INFORME DE VOTO ELECTRÓNICO

Jordi BARRAT ESTEVE / Víctor Manuel MORALES ROCHA

ÍNDICE

I – INTRODUCCIÓN

El Instituto Electoral de Ciudad de México (IECM) es un organismo con larga trayectoria en lo relativo a la utilización de nuevas tecnologías aplicadas a los procesos de participación política. En este sentido, la apuesta por el voto electrónico, tanto en su formato de urnas como de voto remoto, ha situado al Instituto como uno de los principales referentes de esta materia tanto a nivel mexicano como internacional. Baste recordar, en este sentido, la utilización del voto remoto en 2012 para los residentes en el extranjero o el desarrollo de un modelo propio de urnas electrónicas de uso local.

El informe parte de este recorrido histórico para centrarse en el uso del voto electrónico para las votaciones llevadas en cabo entre el 8 y el 15 de marzo de 2020. Se trataba de procesos participativos consistentes en la elección de órganos ciudadanos y en la decisión relativa a los presupuestos participativos tanto de 2020 como de 2021. Tras otras experiencias anteriores, el IECM decidió utilizar el voto digital remoto en un periodo de votación anticipada, entre el 8 y el 12 de marzo. Se previó además el voto por Internet como mecanismo exclusivo de votación en casillas de varias demarcaciones para la jornada del 15 de marzo.

El documento se halla dividido en tres apartados. El primero describe los diversos procesos necesarios para llevar a buen puerto la votación y acompaña tales datos de una valoraciones y recomendaciones a nivel de seguridad informática. Posteriormente, el informe aporta unas recomendaciones de carácter más general en las que figuran áreas de oportunidad donde el IECM podría incidir en futuros usos del voto electrónico. Finalmente, el documento deja constancia de incidentes ocurridos en la aplicación del voto electrónico, determina sus posibles causas y establece qué medidas mitigadoras podrían adoptarse.

El informe aprovecha la recopilación de datos y la articulación tanto de hallazgos como de recomendaciones para determinar aquellos aspectos que puedan ser considerados como fortalezas, pero también plantea elementos susceptibles de desarrollo y mejora. Se destacan asimismo ciertos extremos que requieren atención para no convertirse en amenazas serias para la futura implantación del sistema de voto electrónico.

II – DESCRIPCIÓN DE PROCESOS

El equipo de trabajo ha dividido el proceso en una serie de segmentos que permiten evaluar de forma separada determinadas fases operacionales y de esta forma identificar con mayor facilidad posibles áreas de oportunidad. Los procesos seleccionados no aspiran a verificar de forma exhaustiva todos los trámites necesarios para la puesta en marcha del voto electrónico, pero permiten al menos una disección de determinadas áreas estratégicas y tal aproximación logra rescatar hallazgos de trascendencia para el conjunto del proyecto.

Los procesos seleccionados han sido los siguientes: registro de ciudadanos que eligieron votar por internet; firma del código fuente y configuración del Sistema Electrónico por Internet (SEI); votación por internet; apertura de urna virtual y cómputo de votos; configuración del SEI; voto por internet en mesas electorales y carga de la llave criptográfica del SEI.

A) Proceso: registro de ciudadanos que eligieron votar por internet.

Los ciudadanos residentes en la Ciudad de México tuvieron la opción de votar por internet, de manera remota, a través de la aplicación del Instituto Electoral de la Ciudad de México llamada SEI (Sistema Electrónico por Internet). Para poder votar en esta modalidad, los ciudadanos debieron realizar un proceso de registro como se explica a continuación.

Descripción

- Periodo: 7 de enero al 25 de febrero.

- Requisitos: el ciudadano debe estar en la lista nominal de votantes de Ciudad de México.
- A través de aplicación móvil (iOS y Android), aplicación web y aplicación de escritorio:
    - El votante ingresa datos de su credencial de elector manualmente (clave de elector y OCR), o bien hace una captura de su credencial de elector vía cámara del dispositivo a fin de que se reconozcan automáticamente los datos de la clave de elector y el código OCR. Debido a que actualmente existen tres tipos de credencial de elector vigente, el votante tiene que escoger el tipo de la propia y es apoyado para ello con imágenes de ejemplo de las tres variantes, que son mostradas por la aplicación.
    - Una vez validados los datos de la credencial de elector, el votante escoge si desea recibir la contraseña de acceso al sistema de votación a través de correo postal o por correo electrónico. Si elige la opción de correo electrónico, tiene que hacer una validación adicional que consiste en tomar algunas capturas del rostro en las posiciones que indica la aplicación. Entonces se realiza un proceso de comparación de la fotografía en la credencial, capturada previamente, con las imágenes del rostro del ciudadano. Dichas validaciones consisten en la toma de medidas de ciertos puntos del rostro como, por ejemplo, distancia de oreja a nariz o distancia de oreja a ojo. Si se valida correctamente, la contraseña es enviada al solicitante por correo electrónico; de otra manera, el envío se realiza por correo postal.
- Registro en módulos itinerantes. Son unidades móviles que se colocan en puntos de gran afluencia en la ciudad. El votante se identifica con su credencial de elector y se le envía la contraseña al correo electrónico que proporciona.
- Oficinas de distritos. El votante se identifica con su credencial de elector y se le imprime su contraseña.
- En caso de que un ciudadano pierda su contraseña, se le puede enviar nuevamente la misma contraseña al correo electrónico que se registró en el proceso. En el caso de que la contraseña haya sido enviada a través de correo postal, no se remite nuevamente y el ciudadano pierde, por lo tanto, la oportunidad de votar vía Internet. Sigue contando, no obstante, con la posibilidad de acudir a la mesa electoral correspondiente el día de la jornada electoral.
- Si un ciudadano cambia de número de teléfono después de haber realizado el registro para votar por Internet, pierde la posibilidad de votar a través de este medio. Sigue contando, no obstante, con la posibilidad de acudir a la mesa electoral correspondiente el día de la jornada electoral.

Controles de seguridad en el proceso

- La contraseña es una cadena aleatoria de 8 caracteres alfanuméricos y especiales, lo que constituye un código apropiado en cuanto a robustez y usabilidad.
- Cuando se realiza el registro con aplicación móvil, se guarda la dirección MAC del teléfono para poder detectar prácticas de registro corporativo, es decir, la misma persona o un grupo de ellas realizando registros en lugar de otros.
- Uno de los datos que se captura en el registro es el número de teléfono celular y dicho número no puede ser utilizado para el registro de otra persona. Tal número es importante ya que a dicho terminal llegará el *token* utilizado en la fase de votación como parte del proceso de autenticación. Todo ello ayuda a verificar la legitimidad del votante durante la fase de votación.
- Se lleva a cabo un proceso de comparación de rostro para comprobar que la persona que porta la credencial de elector es realmente quien dice ser y de esa manera poder enviar la contraseña a través de correo electrónico. Este proceso de análisis del rostro se ejecuta a través de un *web service* que provee la empresa *Ho1a*. La aplicación de

registro captura las imágenes del rostro y las envía, junto con la imagen de la fotografía de la credencial de elector, a dicho *web service* que, después de realizar la comparación, devuelve un valor estableciendo si hay o no similitud entre la fotografía de la credencial de elector y las imágenes del rostro del solicitante.

Recomendaciones

- Durante el registro de los votantes se utilizan tres elementos que servirán posteriormente para la identificación a la hora de emitir el voto: credencial de elector, contraseña y número de teléfono. Estos tres elementos, aunque representan una combinación robusta de autenticación, son en cierto sentido vulnerables por ser accesibles por personas cercanas o que compartan el domicilio del votante.

  El caso de la contraseña, que sería el elemento "secreto", puede dejar de serlo al tenerla impresa o conservarla en el correo electrónico en donde se recibió. Tal práctica sucederá además en la mayoría de los casos ya que resulta difícil, al tratarse de una contraseña que él no eligió, que el ciudadano la retenga en su memoria.

  En este sentido, se recomiendan las siguientes acciones:
  - Concientizar al ciudadano del riesgo que representa que otras personas tengan acceso a estos elementos de identificación.
  - Permitir en el proceso de registro que el votante determine su propia contraseña, con ciertas restricciones para que sea robusta. Tal variación aumenta la probabilidad de que la retenga en su memoria y no necesite tenerla por escrito.
  - Explorar opciones adicionales que complementen o sustituyan los mecanismos actuales de identificación del votante, a fin de asegurar con mayor precisión que no exista la suplantación de identidad en el proceso de votación. Dichas opciones podrían ser biométricas, como la huella dactilar, la geometría de la mano, o bien el mismo mecanismo de reconocimiento y validación de rostro que se utiliza en el proceso de registro.
  - Analizar la certificación digital como opción alternativa de autenticación, tal y como sucede en el Sistema de Atención Tributaria en México. Un certificado digital, protegido con NIP, ofrece un mecanismo de autenticación robusto, siempre y cuando el votante le conceda importancia como elemento de seguridad, y para que esto suceda el mismo certificado digital debe tener otros usos. En este sentido, se requeriría una colaboración entre varias dependencias para que el certificado digital tenga un uso más allá de los procesos electorales. El ejemplo de Estonia puede ser particularmente útil a estos efectos.
- Las contraseñas de los votantes deberían ser cifradas con una función hash antes de ser almacenadas en la base de datos, a fin de evitar que puedan ser conocidas, sea de manera legítima o no, por los que tengan acceso a la base de datos. Se recomienda utilizar las funciones SHA1 o SHA2. Si el ciudadano pierde su contraseña y solicita una reposición, el sistema debería generar una diferente. De hecho, ciertos informes previos del propio IECM ya preveían esta opción al señalar que "las claves y *token* que se distribuyen se generan de manera aleatoria y *se cifran* para garantizar la correspondencia única para la emisión del voto/opinión, y solo les conoce la o el ciudadano" (: 33 / Estudio).

B) Procesos: firma del código fuente y configuración del SEI

https://www.youtube.com/watch?v=XTAKWz3f_u4&t=337s

En acto público se realiza la firma digital del código fuente del Sistema Electrónico por Internet que fue previamente auditado por una entidad externa. El código fuente que se firma es del

software que reside en el servidor y el de las aplicaciones móviles, incluyendo las utilizadas para el voto remoto (Android y iOS) y la de las iPad's que se usaron en las mesas electorales seleccionadas para tener voto por internet. Este proceso de firma constituye una prueba de integridad del código fuente, lo que permite verificar, en caso de ser necesario, que el software utilizado en la fase de votación es el mismo que fue auditado y firmado. En el mismo acto se configura la elección en el SEI.

Descripción

- Fecha: 7 de marzo de 2020
- Requisitos: El software debe haber sido auditado.
  Se debe haber generado una clave criptográfica para el secretario ejecutivo del IECM, quien la utilizará para firma.
- El proceso realizado para la firma y resguardo del código fuente se describe a continuación:
    - Se realiza la copia de código fuente de una memoria USB a una computadora personal que no tiene conexión a internet.
    - Haciendo uso del software comercial *Quickhash*, se aplica una función SHA-256 a cada uno de los archivos que componen el código fuente.
    - El secretario ejecutivo provee la clave criptográfica para realizar la firma digital de los archivos. La clave criptográfica se encuentra almacenada en una memoria USB que resguarda el secretario ejecutivo, quien debe ingresar su contraseña para realizar la firma digital. Este proceso de firma digital se realiza utilizando el software comercial llamado *SeguriDoc*.
    - Se realiza una copia del código fuente firmado en la memoria USB.
    - La memoria USB se guarda en su sobre, que es sellado con una cinta de seguridad y posteriormente firmado por el auditor, por el secretario ejecutivo y por el contralor interno del IECM.
    - El sobre queda en posesión del secretario ejecutivo, quien posteriormente lo lleva a una caja fuerte localizada en su oficina.
- Una vez realizado el proceso de firma, se continua con la configuración del SEI, en donde el administrador del sistema realiza las siguientes actividades:
    - Se crea la elección, asignándole un nombre, y se especifican las fechas y los horarios de su inicio y fin.
    - Se realiza la importación de catálogos de la elección: i) ciudadanos que votarán por internet, ii) unidades territoriales, iii) candidaturas y iv) proyectos 2020 y 2021.
    - Después de la carga de los catálogos, se comprueba, a través de la opción del sistema "Avance de la votación", que el sistema se encuentra cerrado, ya que debe abrirse automáticamente para la recepción de los votos el primer minuto del día 8 de marzo.

Controles de seguridad en el proceso

- El código firmado se almacena en la memoria USB y es guardada en un sobre que se cierra con cinta de seguridad, firmado de manera manuscrita por el auditor, el contralor interno del IECM y el secretario ejecutivo del IECM. Finalmente, se resguarda en la caja fuerte de la oficina del secretario ejecutivo del IECM.
- La computadora utilizada para la configuración, así como el servidor de administración de la elección, no tienen conexión a internet. La computadora se conecta al servidor, a través de un enlace ethernet, a fin de realizar la configuración de la elección. Todo ello previene que existan atacantes externos que intervengan la comunicación entre la computadora y el servidor.

- El sistema de configuración solamente es accesible por el administrador del sistema, quien tiene que ingresar cuatro contraseñas alfanuméricas.

Recomendaciones

- Debido a que el sobre que contiene la memoria USB con el código fuente firmado se resguarda en un lugar conocido, a la sazón la caja fuerte de la oficina del secretario ejecutivo, deben articularse las medidas necesarias para que dicho lugar se mantenga seguro contra accesos no autorizados. Alternativamente, puede resguardarse el sobre en un lugar secreto.
- El acto público incluyó la firma del código del sistema web y de las aplicaciones móviles para plataforma Android y iOS, esta última en las versiones de votación remota y de iPad. Cabe destacar que no se realizó para esta elección una auditoría y la consiguiente firma del código correspondiente al módulo de registro de votantes. Se recomienda también auditar, firmar y resguardar esta parte del software.
- La auditoría de los sistemas utilizados es crucial a nivel de transparencia y seguridad, pero algunas de las funciones clave para dotar de seguridad a los procesos se llevan a cabo con software de terceros. Tal es el caso de *Quickhash* y de *SeguriDoc*. Se recomienda auditar dichos programas. Alternativamente, tanto la generación de claves como la firma digital pueden desarrollarse con herramientas propias susceptibles de ser auditadas.
- Se recomienda especial atención en la computadora donde se realiza la firma del código, ya que ahí se ingresa la contraseña y la clave de la elección. Se debería verificar públicamente que la clave de la elección no quedó guardada en la computadora, así como asegurarse que no existe ningún programa malicioso como, por ejemplo, un *keylogger* que pueda grabar la contraseña del secretario ejecutivo una vez que este la captura. Una auditoría de la computadora, previa a la elección, acompañada de una custodia segura de la misma, incrementarían la seguridad. Debe evitarse, en todo caso, que la computadora que se utilice para estos fines sea un dispositivo de uso habitual de los funcionarios del Instituto y contenga, como sucedió en este caso, otros programas ofimáticos ajenos a la tarea de firma, cifrado y configuración de la elección.
- A tenor de los *Lineamientos*, la Llave de apertura "será resguardada conforme a los procedimientos y mecanismos que para tal efecto se determinen" (art. 24). Sería recomendable que esta regulación ya ofreciera mayores detalles sobre el modo de custodia de un elemento tan sensible. Entre otros, podría hacerse referencia al uso de sobres timbrados por varios actores, al lugar en el que se depositará la Llave y sus mecanismos de custodia o qué dispositivos electrónicos pueden utilizarse para su generación.
- Los *Lineamientos* limitan asimismo las garantías explícitas a la presencia de "una tercera persona con fe pública" (art. 23), pero, como es sabido, tales actores se limitan a constatar cuáles son las acciones que se llevan a cabo. No entra dentro de sus labores calificar las actuaciones realizadas o proponer mejoras. Es por ello que, si la normativa no se halla detallada con otro tipo de salvaguardas, la presencia de notarios sirve únicamente para conocer qué es lo que se ha hecho y no para saber si lo realizado era lo conveniente o no. Resulta oportuno, por lo tanto, complementar la labor realizada por la persona con fe pública y también informar sobre el rol de esta persona en las operaciones que se llevan a cabo. Aunque la normativa alude en otros apartados a las funciones tano de la entidad auditora como de observadores electorales, debe enfatizarse explícitamente su intervención en la fase de creación y uso de la Llave criptográfica ya que se trata de una etapa particularmente sensible para la integridad de todo el proceso.

C) Proceso: votación por internet

https://www.youtube.com/watch?v=-vcRYe31IVo

Los votantes que realizaron su registro en el periodo correspondiente pueden sufragar a través de la aplicación SEI. Se trata de la misma aplicación que permitió realizar el registro de votantes, aunque, a partir de la fecha en que se abre el sistema de votación, la aplicación habilita la opción de votar.

Descripción

- Periodo: 8 al 12 de marzo.
- Requisitos: el votante debe haber realizado el registro en el periodo correspondiente a dicho proceso y debe haber recibido una contraseña.
- Una vez que el votante abre la aplicación, se inicia el proceso para emitir el voto:
    - El votante elige, entre los tres tipos de credencial de elector, el que corresponde a la propia. Cada uno de los tipos de credencial son mostrados con una imagen de ejemplo.
    - Se habilita la cámara del teléfono y el votante captura el frente de la credencial. En dos de los tipos de credencial de elector también se debe capturar el anverso, ya que allí es donde se encuentran los dígitos del OCR. Con la captura de la credencial se llenan automáticamente los campos “clave de elector” y “OCR”.
    - El votante ingresa la contraseña que recibió previamente, ya sea por correo electrónico, correo postal o de manera impresa en una oficina de distrito.
    - El votante selecciona la opción “Generar token”. Al seleccionar esta opción el sistema valida que los datos de los tres campos son correctos (clave de elector, OCR y contraseña). Si es así, el elector recibe un mensaje SMS con el token, que es una clave de 6 dígitos. Si alguno de los datos no es correcto, el votante tiene la posibilidad de corregirlo, seleccionando el campo correspondiente e ingresando el dato de manera manual.
    - El votante ingresa el token y, si este es válido, se continúa con la votación.
    - Se presentan las boletas para que el votante seleccione las opciones deseadas.
    - El votante confirma su selección y se envía el voto.
- En los últimos minutos del día 12 de marzo y en acto público se reúnen funcionarios del IECM para constatar el cierre automático de la recepción de votos por internet. A las 00:00 horas se hace notar que, aun cuando el sistema no acepta la apertura de nuevas sesiones de votación, aun hay algunos votantes con sesión abierta y por ello el sistema les permite emitir sus votos. Finalmente se declara que el sistema ya no permite más votos.

Controles de seguridad en el proceso

- El proceso de autenticación requiere que, al momento de utilizar la aplicación, el votante cuente con tres elementos: credencial de elector, contraseña y teléfono, cuyo número registró previamente y en el que se recibe el token. La combinación de estos elementos conlleva que la autenticación sea robusta, evitando ataques de usurpación por parte de personas no cercanas al votante.
- La sesión de votación caduca en 15 minutos, lo que impide en buena medida ataques de suplantación de identidad causados, por ejemplo, por extravíos del teléfono.
- El voto se firma digitalmente, luego se cifra y es enviado a través de SSL. La firma y el cifrado se realiza con RSA. Finalmente, el voto se vuelve a cifrar con una función del manejador de base de datos Oracle. Asumiendo una correcta implantación del cifrado, el proceso descrito asegura tanto la confidencialidad del voto como su integridad.
- Los votos se almacenan en un servidor ubicado físicamente en las instalaciones del IECM. El centro de datos en donde se encuentra el servidor cuenta con medidas de

control de acceso, de manera que es difícil que una persona no autorizada ingrese al lugar sin advertirlo.

- Los votos se almacenan de manera aleatoria en una de las 7 tablas o "urnas virtuales" disponibles en la base de datos, a fin de confundir el orden en que se recibieron los votos y de esta manera romper la relación voto-votante.
- Tanto la información de la cantidad de votos recibidos como el estatus del sistema se observan desde el módulo de administración, a donde accede el administrador del sistema.

Recomendaciones

- Aun cuando se considera fuerte el uso combinado de diferentes elementos para que se autentique cada votante, no llega a evitarse que una persona cercana, como el cónyuge, suplante al votante legítimo. Una persona que vive en el mismo domicilio, por ejemplo, puede tener acceso a los elementos de autenticación. Se recomienda utilizar un mecanismo biométrico que impida la suplantación durante el proceso de votación, tal como huella dactilar, geometría de la mano, o bien, el mismo mecanismo de reconocimiento y validación de rostro que se utiliza en el proceso de registro.
- Debido a que una sesión iniciada por un votante puede permanecer activa durante 15 minutos, en caso de que el votante deje una sesión abierta y descuide su dispositivo, otra persona podría concluir el proceso de votación con opciones diferentes a las deseadas por el votante legítimo. Debido a tal posibilidad, se recomienda que el votante tenga que ingresar nuevamente la contraseña al momento de confirmar sus opciones de votación, o al menos una parte de la contraseña para así conservar la facilidad de uso. Podría tratarse, por ejemplo, de los últimos tres caracteres.
- A pesar de que el centro de datos del IECM cuenta con control de acceso, se recomienda tener un esquema de redundancia de datos. Los votos recibidos se guardarán en un segundo servidor, que se encontrará además en un lugar físico diferente, es decir, fuera de las instalaciones del IECM.
- Si bien los votos se almacenan de manera aleatoria en diferentes tablas a fin de romper la relación voto-votante, existe aun la posibilidad de que se pueda deducir dicha relación, especialmente teniendo privilegios de acceso al sistema y/o base de datos. Elementos como la hora en que se guardan, además de *logs* de sistema o *logs* del tráfico de red entrante pueden utilizarse para encontrar la relación. Se recomienda, como medida mínima, realizar un proceso de mezclado o permutación de los votos antes de ser descifrados. Alternativamente, puede implantarse otro mecanismo que impida llegar a conocer dicha relación como, por ejemplo, mecanismos de firma ciega y el uso de servidores diferentes, y en diferentes ubicaciones, para autenticar al votante y para recibir el voto.
- En el proceso en donde se verifica que el sistema se cierra automáticamente al concluir el día 12 de marzo, se puede observar en pantalla la dirección de acceso al servidor, tanto la versión intranet como la que se accede a través de Internet (registro.iecm.mx). Aun cuando se requieren credenciales de acceso que solo posee el administrador del sistema, se recomienda no hacer públicas las direcciones de acceso al módulo de administración. Se evita así invitar a intentos de distintos tipos de ataques, incluidos los de denegación de servicio.

D) Proceso: apertura de urna virtual y cómputo de votos

https://www.youtube.com/watch?v=V5v-x65x45k
https://www.youtube.com/watch?v=tD1nxFAObkM&t=3s

En sesión extraordinaria del Consejo General del IECM, se realizó la "Apertura de la urna virtual y cómputo de votos" de la votación por internet realizada del 8 al 12 de marzo.

Descripción

- Fecha: 13 de marzo de 2020
- El proceso transcurrió como sigue:
    - En el sistema de votación se selecciona la opción "Apertura y cómputo de urna virtual". A continuación, el Secretario Ejecutivo del IECM debe insertar la memoria USB en donde se encuentra la clave privada de la elección así como teclear su contraseña.
    - Se realiza el cómputo de total de votos recibidos en la modalidad de votación por internet.
    - Se da apertura a los trabajos de generación de actas de las 1815 unidades territoriales que participaron en la elección a fin de que el día de la votación presencial (15 de marzo) las mesas electorales tengan información de los votantes que ya enviaron su voto a través de internet y no les sea permitido votar nuevamente.

Controles de seguridad en el proceso

- La apertura de la urna en este acto público requiere la clave privada de la elección, así como la contraseña, ambas en posesión del secretario ejecutivo del IECM, lo que previene la apertura de la urna por parte de personas no autorizadas e incluso por el propio Secretario Ejecutivo fuera de la fecha estipulada.

Recomendaciones

- Debido a la importancia de la memoria USB al contener la clave privada de la elección, se recomienda mejorar su seguridad. Si la memoria se dañara o perdiera, resultaría imposible descifrar los votos y se afectaría gravemente la elección. Se recomienda buscar un esquema alternativo de protección de la clave, ya sea realizando una copia, custodiada en lugar diferente, o, mejor aun, implantando un esquema de secreto compartido. Todo ello disminuye la probabilidad de que llegue a ser imposible descifrar los votos por falta de una clave privada o contraseña. En un esquema de secreto compartido como el propuesto por Adi SHAMIR[1], se puede compartir entre varios participantes un secreto, como una contraseña o una clave criptográfica, de modo que con la colaboración de un subconjunto de los participantes se pueda recuperar el secreto.
- Llama la atención asimismo que, como fruto de la apertura anticipada de la urna, se generen resultados parciales cuando aún queda pendiente una jornada entera de votación. Adviértase, en este sentido, que, de acuerdo con la *Guía para la Implementación del Sistema Electrónico de Internet*, las actas de cómputo por mesas son entregadas al inicio de la jornada a los respectivos responsables quienes "sumarán los votos y las opiniones del SEI a la contabilidad de los votos y las opiniones que se recibieron durante la Jornada Electiva Única del 15 de marzo de 2020" (: 113 / Guía). Más allá de las medidas de seguridad y discreción que puedan articularse para prevenir posibles filtraciones, se recomienda buscar fórmulas alternativas que desemboquen en una apertura única y unificada de la base de datos definitiva con la totalidad de sufragios. El hecho de que se disponga de la lista de votantes efectivos por internet durante los días previos debería ser ya suficiente para excluirlos del listado nominal a utilizar durante el domingo. Por otro lado, el escrutinio por mesas, en caso de que se estime pertinente hacerlo de este modo y no de forma centralizada, debería poder

[1]Se puede consultar la teoría del esquema de secreto compartido en:
https://www.histo.cat/1/How-to-share-a-secret.pdf
Existen librerías para facilitar su implementación en diferentes lenguajes de programación.

realizarse al término de la jornada de votación del 15 de marzo incluyendo entonces los sufragios recibidos por las dos modalidades aceptadas de votación.

E) Proceso: configuración del SEI

https://www.youtube.com/watch?v=rPiza3vtISQ

En acto público se realizó la configuración del Sistema Electrónico por Internet (SEI) a fin de poner a punto el sistema para la jornada electoral del día 15 de marzo.

Descripción

- Fecha: 14 de marzo de 2020.
- Durante este proceso se realizó la carga de los siguientes catálogos:
  - Lista nominal de 787,648 votantes.
  - 153 unidades territoriales correspondientes a tres distritos electorales completos (9, 12, 13) y parte de otro (5).
  - 2404 candidaturas.
  - 1463 proyectos para 2020.
  - 1228 proyectos para 2021.

- Una vez cargados los catálogos, se verifica el avance de la votación, en donde se puede constatar que el sistema se encuentra cerrado y que no se han recibido votos. El sistema se abrirá automáticamente para recibir votos a partir de las 9:00 horas del día 15 de marzo.

Controles de seguridad en el proceso

- Los catálogos cargados en el sistema son archivos que han sido previamente validados por la unidad correspondiente, pero no se transparenta el proceso y, por lo tanto, no se puede tener certeza de que dichos archivos se mantienen íntegros hasta su carga en el sistema.

Recomendaciones

- Se recomienda que, una vez que los catálogos son verificados o validados por la entidad correspondiente, sean firmados digitalmente, a fin de que se puedan verificar justo antes de su carga en el sistema. Otra alternativa consistiría en implantar una cadena de custodia segura. Este proceso de verificación de catálogos es muy relevante debido a que cualquier manipulación propiciaría desde negar el derecho de ejercer el voto a un ciudadano, en caso de manipulación de la lista nominal, hasta provocar que las candidaturas o proyectos sean incorrectos o incluso ilegítimos.
- Habida cuenta que la configuración de la votación para el 15 de marzo se lleva cabo sobre la base de la misma Llave criptográfica utilizada para el proceso anterior del 8 al 12 de marzo, existe la posibilidad de que, debido a *malware* o manipulación deliberada por funcionarios del Instituto, la computadora haya retenido la Llave y se hayan incluso realizado copias cuyo control quedaría ya fuera del alcance de los propios gestores de la votación. La integridad de la jornada del día 15 de marzo estaría, por lo tanto, en entredicho. Se recomienda redoblar los controles sobre las computadoras utilizadas en la apertura de urnas y configuración de elecciones para evitar usos fraudulentos de la Llave criptográfica. Se recomienda asimismo analizar la utilización de dos Llaves criptográficas diferentes, para la jornada de votación remota y para la votación en casilla respectivamente.

F) Proceso: voto por internet en mesas electorales

El día 15 de marzo las mesas electorales de cuatro distritos (9, 12, 13 y parte del 5) ofrecieron la modalidad única de voto por internet, de manera supervisada, a través de la aplicación móvil instalada en iPad's.

Descripción

- El operador electoral realiza en la aplicación la apertura de la elección, con las siguientes actividades:
    - Escribe una palabra que se le muestra en pantalla, a manera de captcha.
    - Escanea, con la cámara de la tableta, un código QR que le fue entregado previamente impreso en una tarjeta.
    - Ingresa su NIP, también asignado previamente.
- Una vez abierta la elección, el operador puede iniciar el proceso de votación, realizando las siguientes tareas con cada uno de los votantes:
    - Escanea, con la cámara de la tableta, el código QR de operador.
    - Ingresa su NIP.
    - Selecciona el tipo de credencial del votante y realiza la captura con la cámara de la tableta. Esta captura debe arrojar automáticamente los datos de clave de elector y OCR.
    - El operador verifica que los datos corresponden a los de la credencial de elector y, una vez realizado tal control, franquea el acceso al votante a la mampara en donde se seleccionarán las opciones de voto.
- Se presentan las boletas para que el votante seleccione las opciones deseadas.
- El votante confirma su selección y se envía el voto.
- Cuando un votante envía su voto, el iPad emite un sonido durante 7 segundos, a fin de que el operador advierta que el votante ha concluido el proceso.
- Si hay votantes que necesiten ayuda, un acompañante puede acceder a la mampara para asistir al votante. Un acompañante solamente puede realizar dicha función en dos ocasiones y en cada ocasión se le marca un dedo meñique con tinta indeleble.
- Al finalizar la jornada electoral, el responsable de la mesa realiza en la tableta un proceso de cierre de elección. Tal como en la apertura de la mesa, en el cierre el operador ingresa sus credenciales.
- Después del cierre de la votación, en la aplicación se habilita la opción de cómputo de votos, a realizar de manera local en cada mesa electoral. Esta opción se habilita siempre y cuando se haya realizado el proceso de carga de la llave criptográfica por parte del secretario ejecutivo del IECM, tal como se describe en el siguiente proceso (carga de la llave criptográfica del SEI).
- Para realizar el cómputo, el operador debe nuevamente autenticarse a través del QR y del NIP. Al realizar el cómputo, los votos son descifrados en el servidor y contabilizados. Los resultados se muestran en la pantalla de la tableta y son almacenados en el servidor para su posterior consolidación con los resultados de otras mesas electorales.

Controles de seguridad en el proceso

- La apertura y cierre de la votación, así como el cómputo de los votos, son realizados por el operador responsable de la mesa electoral, comprobando previamente su identidad mediante el escaneo del código QR y el número de identificación personal (NIP) que se le asignaron. Todo ello evita, en cierta medida, que el sistema sea operado por una persona no legítima.
- El proceso de autenticación y elegibilidad de votantes se realiza mediante la credencial de elector, que es capturada con la cámara de la tableta a fin de validar la clave de elector y OCR. La autenticación correcta queda a expensas de la habilidad e interés del

operador de la mesa electoral para validar que la fotografía de la credencial de elector corresponda a la persona que la porta.
- El sonido que emite la tableta al concluir una sesión de voto evita en gran medida que el votante intente manipular el sistema o la tableta.

Recomendaciones
- Se recomienda mejorar el proceso de autenticación del votante, a fin de evitar que una persona que porta una credencial de elector de otra persona tenga acceso a la votación. Aun cuando se trata de un problema no exclusivo de la votación electrónica, podría mejorarse tal aspecto aprovechando los avances tecnológicos en materia de autenticación, como los procedimientos biométricos entre otros.

G) Proceso: carga de la llave criptográfica del SEI
https://www.youtube.com/watch?v=Llt5KLVIfNY
En acto público en el IECM, se realizó la carga de la llave criptográfica minutos antes de la conclusión de la jornada electoral. Este proceso se lleva a cabo dentro del sistema de votación, con la clave privada que custodia el secretario ejecutivo del IECM, así como su contraseña. Al momento de concluir este proceso, se habilitó automáticamente la opción de cómputo de votos en las tabletas de las mesas electorales. Es así como las mesas electorales, al concluir la recepción de votos, comienzan con su descifrado y cómputo de los mismos, obteniendo los resultados a nivel local, es decir, de mesa electoral.

Controles de seguridad en el proceso
- El descifrado de los votos se realiza con la clave privada custodiada por el secretario ejecutivo, que a su vez está protegida por la contraseña que él mismo conoce. Por lo tanto, no se pueden descifrar los votos ni obtener resultados sin la aportación de dichos elementos, lo que aporta una seguridad importante al proceso. Por otro lado, en un hipotético escenario en el que no sea posible que el secretario ejecutivo aporte uno de los elementos citados, sería imposible descifrar los votos, lo que tendría un impacto negativo en el proceso electoral.

Recomendaciones
- A fin de disminuir la probabilidad de que suceda una incidencia en el que sea imposible descifrar los votos por falta de clave privada o contraseña, se recomienda explorar la posibilidad de implementar un esquema de secreto compartido como el propuesto por Adi SHAMIR. Dicho esquema permite compartir entre varios participantes un secreto, como una contraseña o una clave criptográfica, de modo que con la colaboración de un subconjunto de los participantes se puede recuperar el secreto.
- El hecho de cargar en el sistema la llave privada de la elección cuando aun se encuentra abierta la recepción de votos presenta el riesgo de que pueda lograrse acceso indebido a la llave, bien a través de internet bien directamente del servidor por personal del IECM. Podrían entonces descifrarse votos anticipadamente, tanto los que ya están almacenados en la base de datos como los que están llegando, siendo este último caso más peligroso ya que se pueden descifrar y ligarlos a la identidad del votante. Se recomienda que la carga de la llave criptográfica se realice cuando la votación haya concluido.

III – CONSIDERACIONES GENERALES
Las siguientes consideraciones no son exclusivas de un proceso en particular, sino del sistema electrónico por internet en general y a los procesos que le acompañan antes, durante y después

de una elección. Se parte, por lo tanto, de un análisis genérico del voto para Internet para entender en toda su dimensión el supuesto práctico de Ciudad de México.

El apartado incluye las siguientes subsecciones: fortalezas, estimación de riesgos, verificabilidad individual y universal, libertad de sufragio, registro de eventos (logs) inmutables, marco legal, normativa sobre auditorías, auditoría / aspectos técnicos, escalabilidad del sistema, diseño de la boleta y del proceso de votación, capacitación, simulacros y logística, apoyo a redes de observaciones electorales y oportunidades.

A) Fortalezas

Iniciamos estas consideraciones generales con algunas aportaciones que destacan fortalezas del sistema electrónico implantado en el IECM. Como ya se indicó al inicio del informe, se trata de una de las experiencias más innovadoras en el campo del voto electrónico tanto a nivel local como internacional. Merece la pena, en este sentido, aportar algunos datos que permitan calibrar en su justa medida esta afirmación.

El voto por Internet es una modalidad de voto electrónico cuya utilización a nivel mundial todavía es bastante limitada y ha sufrido además importantes altibajos en los últimos años. Sin ánimo de ser exhaustivos, pueden citarse países de referencia en el uso del voto por Internet como Estonia, Suiza, Canadá, Panamá, Armenia, Australia, Francia, Países Bajos, Noruega o Finlandia. Cada uno de ellos incluye numerosos matices y en algunos casos se trata de ejemplos que han paralizado su aplicación por causas diversas, como en los Países Bajos o en Finlandia. Además, entre todos estos países, el uso del voto por internet tiene ciertas limitaciones como, por ejemplo, aplicarse exclusivamente en algunas zonas (Suiza o Noruega) o para algunos colectivos, como los expatriados en Francia o Armenia.

Es en este marco internacional en el que debe valorarse la iniciativa del IECM y, si tomamos en consideración tanto su trayectoria histórica desde 2012 como su repercusión demográfica, puede concluirse con facilidad que nos hallamos ante uno de los supuestos de hecho más significativos. Pocos territorios cuentan, por ejemplo, con una línea de progresión sin interrupciones significativas como la que se da en Ciudad de México. También pocos, o incluso quizás ninguno, tienen un impacto demográfico potencial de la magnitud del que se plantea en este caso. Ciertamente, sin embargo, el hecho de que el voto electrónico no llegue a reimplantarse en elecciones constitucionales, posibilidad rechazada por el INE para los comicios de 2018, resta valor y sobre todo visibilidad al proyecto, pero no debe impedir destacar, como aquí se hace, su protagonismo.

Todo ello no habría sido factible sin el enorme esfuerzo institucional desplegado por el IECM al menos desde los inicios de siglo. Es entonces cuando el antiguo IEDF lanza un prototipo de urnas electrónicas y es a partir de esta experiencia por la que el Instituto logra posteriormente utilizar el voto por Internet. Tras adquirirlo a una empresa catalana para su uso en 2012, el Instituto continua su desarrollo e implantación en consultas y elecciones populares de diverso tenor.

Tanto la documentación aportada como las entrevistas con responsables políticos y técnicos del Instituto reflejan gran profesionalidad y conciencia clara sobre el enorme reto que supone lanzar un sistema de voto por Internet. Baste, por ejemplo, con consultar los numerosos estudios de carácter técnico, operativo, social o financiero. Baste también con consultar los informes de los órganos creados al efecto, como el Comité Técnico cuyas recomendaciones han sido atendidas en diversas ocasiones a lo largo de estos últimos años.

El conocimiento especializado del equipo gestor en el IECM no es un factor desdeñable si atendemos a lo que suele suceder en otras latitudes. No es infrecuente, en este sentido, que los

organismos electorales carezcan de capacidad técnica interna y que tales debilidades se suplan con un protagonismo desmesurado de contratistas privados. Es en tales contextos en los que no siempre se vela de la forma más correcta por el interés público, pero en el caso de Ciudad de México las capacidades del propio IECM permiten trazar una línea propia que incluso permite desarrollos informáticos internos y no externalizados.

En definitiva, los antecedentes de uso y la trayectoria continuada en el uso del voto por Internet juntamente con el apoyo institucional que recibe incluso en circunstancias delicadas y la profesionalidad del equipo técnico a su cargo constituyen factores de enorme valor que cabe calificar de fortalezas.

Existe además un contexto social favorable con escasas opiniones críticas al voto electrónico. Se trata de un hecho llamativo que debería ser tomado en consideración tanto en forma positiva, pero también como alerta ante su posible evolución en el futuro. Cabe señalar, en este sentido, que muchos de los países en los que se ha utilizado o se utiliza el voto electrónico deben lidiar con grupos sociales muy activos en su contra, y a veces no carentes de razón en sus argumentos. Es por ello que conviene consolidar la interlocución entre el IECM y aquellos sectores sociales que podrían estar más interesados en involucrarse en el análisis de la democracia digital. La implantación gradual del voto electrónico, que constituye otra de las fortalezas a reseñar en el caso del IECM, favorece esta operación. También merece destacarse, en este sentido, el apoyo ya brindado a las redes de observación electoral.

Desde el plano técnico, el impulso de análisis externos al IECM y el hecho de que el sistema sea "auditable en todas sus etapas" (: 45 / Estudio) contribuyen enormemente a afianzar la plataforma. Se une a ello la transparencia del Instituto a la hora de proporcionar un apoyo documental amplio y detallado sobre el uso del voto electrónico. Finalmente, cabe reconocer una indudable voluntad innovadora en aspectos técnicos como se demuestra, por ejemplo, con el impulso del reconocimiento facial para autenticar a los electores. Se trata de mecanismos de alta sofisticación que demuestran que el IECM no se arredra fácilmente ante determinados retos. En otro orden de cosas, el mantenimiento de un "Centro de Atención Telefónica las 24 horas del día" (art. 22 / Lineamientos) demuestra también un compromiso claro con la participación de los ciudadanos.

B) Estimación de riesgos

De acuerdo con la información recabada para la elaboración de este informe, se puede observar que las medidas de seguridad actuales, tanto a nivel de infraestructura como de software y procedimientos, son, en la mayoría de casos, las adecuadas para el tipo de elecciones y número de votantes que se ha tenido en los últimos años en la Ciudad de México. No obstante, a medida que la relevancia de una elección se eleve, como en el caso de una elección para Jefe de Gobierno de la ciudad, y el número de votantes se incremente, la motivación o intereses para realizar un ataque también aumenta.

Si bien en el seno del IECM, así como por parte de la entidad auditora, se han realizado análisis de riesgos del sistema de elección por internet, en estos se ha contemplado primordialmente la infraestructura de servidores y comunicaciones, con un enfoque del flujo, operación y continuidad del sistema. En cambio, dichos análisis han profundizado poco en otros elementos fundamentales del sistema electrónico por internet, como el propio software, la información sensible y los diversos procesos que sustentan una elección, todo ello orientado a la protección de los principios democráticos y sus consecuentes requisitos de seguridad en un entorno de voto electrónico. Tampoco quedan de manifiesto en dichos análisis los diversos tipos de atacantes y las motivaciones que pudieran tener para atentar contra la integridad de la elección. Estos

aspectos son importantes ya que permiten estimar de una manera más aproximada los posibles riesgos, la probabilidad de ocurrencia y el impacto que tendría cada uno en caso de suceder.

En este sentido, se recomienda realizar un proceso exhaustivo de estimación de riesgos del voto por internet, en donde se considere que hay atacantes que buscarán realizar infiltraciones, manipulaciones o atentar en contra de la integridad de la elección. Dicho análisis de riesgos debe considerar todos los tipos de atacantes, entre los que se pueden incluir votantes, criminales informáticos, partidos políticos, personal del IECM, responsables de mesas electorales o gobiernos extranjeros, entre otros. Al realizar una estimación de riesgos amplia y profunda se podrá determinar, con mayor precisión, los mecanismos técnicos, políticos y procedimentales que deben implantarse para contar con un sistema y un entorno seguro de voto por Internet.

C) Verificabilidad individual y universal

A fin de aumentar la transparencia y percepción de seguridad, se recomienda implantar mecanismos de verificación del voto, que ofrezcan las siguientes garantías:

1. el voto se registró tal como fue la intención del elector (característica conocida en la doctrina como *cast as intended*).
2. el voto fue almacenado tal y como fue emitido (conocido como *recorded as cast*)
3. el voto se contabilizó tal y como fue almacenado (conocido como *counted as recorded*).

Verificación individual / Cast-as-intended y *recorded-as-cast*

La verificación individual es un aspecto muy importante para validar el correcto funcionamiento de un sistema de voto electrónico ya que permite combatir la opacidad inherente a esta tecnología. Su principal objetivo consiste en que el votante pueda estar seguro que su voto se ha registrado correctamente. En sistemas convencionales basados en papel, los ciudadanos pueden verificar que su voto es recibido correctamente ya que son ellos mismos quienes colocan la boleta en la urna física y, sea personalmente como observadores o indirectamente a través de los interventores de partidos políticos, puede garantizarse que la urna permanece cerrada hasta el escrutinio y no se alterna su contenido mediante la sustracción de boletas o la adición de votos indebidos.

En el voto electrónico, por el contrario, un mensaje de mera confirmación de que un voto ha quedado correctamente registrado no proporciona garantía ni de que el voto realmente se haya transmitido conforme a la intención del elector ni de que se haya además almacenado tal y como fue emitido. En este sentido, el programa de voto electrónico puede estar diseñado para ofrecer un mensaje tranquilizador al elector mientras se altera subrepticiamente el contenido de su sufragio. Adviértase además que la posibilidad de que un voto no se registre adecuadamente no se asocia directamente con una falla o manipulación del software. En entornos de votación remota, en donde los dispositivos desde los que se emite el voto no están bajo el control y supervisión de la autoridad electoral, es posible que exista *malware* en el dispositivo del cliente que manipule la intención del voto antes de que este sea cifrado y transmitido.

En el caso del sistema utilizado en Ciudad de México, diversos informes resaltan como dato positivo el hecho de añadir una nueva funcionalidad consistente en la remisión de un comprobante de entrega al elector. En concreto, Comités Técnicos anteriores proponían “el envío de confirmaciones de emisión de voto” y “el SEI del 2017 se actualizó de tal forma que se enviaron notificaciones al votante, vía un número de teléfono celular (: 47 / Opinión).

Es lo que sucede actualmente, aunque con significativas diferencias entre el voto móvil y el emitido en casilla. Si atendemos a la *Guía*, en ambos casos el elector recibe confirmación de la remisión, lo que no equivale a recepción en el servidor, y mensaje de agradecimiento [: 34 y 39

/ Guía; el Manual precisa de todos modos que la comunicación queda reducida a un solo mensaje del siguiente tenor “Gracias por darnos tu opinión” o “Gracias por participar” (: 6)]. Si atendemos, en cambio, al video explicativo en el propio IECM, el mensaje alude a que el voto “se guardó correctamente”, es decir, parece incluir su almacenamiento (*https://www.youtube.com/watch?v=-vcRYe31IVo*; minuto 02:05). Además, en el caso del voto móvil, el ciudadano también recibe un mensaje SMS en su teléfono confirmando la recepción del sufragio (: 34 / Guía), lo que no aparece previsto para el voto en casilla.

Se trata, sin lugar a dudas, de una mejora sustancial respecto a lo que sucedía en versiones anteriores en las que no existían tales mensajes de confirmación, pero tal dato no debe ocultarnos que nos hallamos todavía lejos de lo que la doctrina entiende por verificación individual. El sistema de Ciudad de México dista de lo ya existente en otros casos a nivel comparado, como Estonia, e incluso de otros supuestos en los que, si bien no se produce una verificabilidad individual completa, se ofrece al elector un comprobante con un código personalizado de tal forma que, una vez finalizada la jornada, pueda comprobarse si ese código se halla en la lista publicada por la administración electoral. Tal documento refleja el conjunto de sufragios que han sido almacenados.

Los códigos no incluyen el sentido del voto y no pueden, por lo tanto, calificarse de verificaciones individuales, pero ofrecen al menos una cierta trazabilidad del sufragio. En el caso de Ciudad de México, en cambio, el mensaje se limita a un agradecimiento y a una confirmación genérica sobre el procesamiento del voto, pero sin posibilidad alguna de verificación personal.

Adviértase asimismo que tales comprobantes tienen cierta virtualidad si se remiten a dispositivos diferentes a los utilizados para emitir el sufragio. En caso contrario, los comprobantes no demuestran en realidad nada ya que los vicios del programa informático pueden generarlos para ofrecer tranquilidad al votante. En el caso, por ejemplo, del voto en casilla, mostrar un comprobante en la misma pantalla que se ha utilizado para votar no añade en realidad ninguna garantía real y puede servir a lo sumo como un mecanismo psicológico, no técnico, que aumenta la confiabilidad del sistema.

En cambio, en el caso del voto móvil, todo dependerá de los dispositivos que se utilicen para emitir el voto ya que, si bien puede replicarse lo que ya sucede en el voto en casilla, es decir, que el votante utilice para votar el teléfono al que después se recibirá el comprobante, también puede suceder que se utilice otro dispositivo, sea otro teléfono o computadora. Es en este último caso donde el comprobante despliega toda su potencialidad ya que resulta más difícil que un mismo programa pueda estar funcionando al mismo tiempo en dos dispositivos alejados físicamente entre sí.

Cabe señalar, en definitiva, que el sistema de votación experimentaría una mejora sustancial si implantara sistemas de verificabilidad individual que, utilizando dispositivos informáticos diferentes, remitieran al elector un comprobante en el que se plasmara cuál ha sido su intención de voto.

Tal funcionalidad mitiga enormemente la opacidad inherente a todo sistema de voto electrónico, pero genera simultáneamente otro reto consistente en preservar tanto el secreto del sufragio como la libertad del elector. En efecto, si el ciudadano recibe un comprobante en el que conste qué ha votado, se alimenta la posibilidad de que otra persona pueda exigirle ese documento para comprobar que realmente ha votado de acuerdo con las instrucciones recibidas. Se trata de un factor nada desdeñable que merece un análisis pormenorizado. Véase, en este sentido, el apartado posterior de este informe relativo a la libertad de sufragio.

Por último, también podría pensarse, en el caso del voto en casilla, en la incorporación de comprobantes en papel que, al igual de lo que sucede en otros casos de urnas electrónicas mexicanas, quedaran resguardados en la propia casilla a efectos de un eventual recuento posterior. El ciudadano dispondría de un sistema para comprobar la correcta emisión de su sufragio y se posibilitarían además revisiones posteriores, aunque también es cierto que tal novedad supondría modificaciones importantes a nivel logístico y de infraestructura. Es por ello que parece más conveniente contemplar, como medida inicial, la incorporación de comprobantes digitales como los descritos en párrafos anteriores.

Verificabilidad universal / Tallied as recorded

Por otro lado, si se desea lograr una plena auditabilidad del proceso, es decir, lo que se conoce como *End-to-End (E2E) Verifiability*, la verificación individual debe ir acompañada de otros mecanismos que permitan validar que todos los sufragios han sido escrutados tal y como fueron almacenados. Aun cuando un voto se haya registrado correctamente en el servidor, no cabe descartar manipulaciones previas al conteo de los votos que escaparían, por lo tanto, de las dos verificaciones individuales ya descritas, cuyo alcance se detiene cuando el sufragio ha sido almacenado y no van más allá, es decir, hasta el momento del escrutinio.

La solución propuesta en algunos países, como Noruega, Estonia o Suiza, consiste en articular esta última fase de tal forma que pueda ser verificada por cualquier actor interesado. Debido a su complejidad criptográfica, tal etapa ya no está al alcance de cualquier ciudadano, pero pueden preverse sistemas para que cualquier técnico pueda verificar por sí mismo si la apertura de la urna digital, el filtrado de los votos y el escrutinio se realizan de forma correcta. Se trataría, en definitiva, de ofrecer un método de verificación neutro e independiente disponible para todo aquél con suficiente capacidad técnica. Todo ello contrasta con lo que sucede hoy en día en el escrutinio ya que se halla sometido únicamente al control de una entidad auditora contratada por el propio IECM.

D) Libertad de sufragio

Como se ha indicado en la sección precedente, la verificabilidad individual entraña ciertos riesgos ya que, al proporcionar al votante un comprobante del contenido de su voto, permite que terceros puedan ejercer presión sobre el ciudadano para que desvele el sentido de su sufragio. Se trata lógicamente de una consecuencia indeseable e inaceptable en un procedimiento originalmente diseñado para fortalecer y no para aminorar las garantías del sistema de voto electrónico.

Es por ello que toda verificación individual deberá incluir mecanismos que permitan tener certeza de que el voto ha sido almacenado sin que simultáneamente se indique cuál ha sido la elección del votante. Se trata de algo aparentemente incompatible entre sí, pero diversos sistemas han logrado alcanzar ambos propósitos, es decir, mantener el secreto del voto y permitir su verificación por parte de cada ciudadano. En términos generales, existen dos opciones: confiar en la responsabilidad individual de cada ciudadano y en un contexto social que no contemple coacciones a la libertad de los votantes o establecer un sistema de voto múltiple que impida conocer qué sufragio ha sido tomado en cuenta durante el escrutinio.

En relación con la primera posibilidad, el procedimiento electoral delegaría en la propia sociedad la carga de evitar malas praxis con los comprobantes. A la vista del contexto en el que se aplica el sistema de voto electrónico, se partiría de la premisa de que los casos de coacción acabarían no produciéndose o lo harían en unos porcentajes residuales. Tal entorno permitiría implantar una verificabilidad individual con comprobantes sin mayores candados para garantizar el secreto del voto.

Existen países, como Suiza, en los que tradicionalmente se ha admitido el voto remoto, sea postal o por Internet, sin que se articulen mecanismos especiales de protección de la libertad del ciudadano. Una vez recibida en casa la documentación electoral, se puede emitir el sufragio de forma extraordinariamente sencilla, como depositando el sobre con la boleta en cualquier buzón de correos. Y la misma práctica se ha trasladado al voto por internet. Si bien es cierto que Suiza no contaba con verificación individual, el sistema de emisión del voto refleja el tipo de entorno social que debería existir para admitir sin reparos los comprobantes.

Cabe preguntarse lógicamente en qué situación se halla México, es decir, si en este caso la remisión de comprobantes a cada ciudadano con el sentido de su voto pudiera ir en detrimento de la libertad del votante y, en consecuencia, del secreto del voto. Sin perjuicio de los correspondientes informes sociológicos al respecto, que no se han llevado a cabo en el marco del presente informe, no parece aventurado afirmar que el caso mexicano dista mucho del suizo y la admisión de comprobantes de voto debe contemplarse con suma prudencia.

Sea como sea, existen ciertos elementos que enriquecen este debate y uno de ellos consiste en cómo se ha evaluado hasta la fecha en México el riesgo que supone la admisión del voto por internet en sí mismo, es decir, no solamente la verificabilidad individual mediante comprobantes, sino el conjunto del sistema de voto electrónico remoto utilizado en Ciudad de México.

Tal análisis cobra suma relevancia si tenemos en cuenta que los riesgos antes descritos sobre los comprobantes de voto también existen, en mayor o menor grado, durante la emisión del sufragio. Nada impide, por ejemplo, que la coacción se produzca en el mismo momento del voto y no deba esperarse, por lo tanto, a una eventual recepción posterior de un comprobante. Se trata de la misma amenaza consistente en la presencia de terceros capaces de ejercer presión sobre un votante para que le muestre el comprobante recibido, en caso de admitir la verificabilidad individual, o para que les muestre la pantalla de votación inmediatamente antes de emitir el sufragio. En este sentido, el sistema implantado en Ciudad de México incluye sistemas altamente complejos para evitar suplantaciones de identidad, pero no disuade ante una eventual coacción directa al votante en el momento de emitir su sufragio.

Todo ello debe además considerarse a la luz de antecedentes de la propia Ciudad de México en los que el voto clientelar ha sido detectado como mala praxis consolidada especialmente en ciertas colonias de la Ciudad. Es lo que motivó, entre otros motivos, el esfuerzo del IECM en implantar un sistema de reconocimiento biométrico que mitigara, en la medida de lo posible, los casos de suplantación. Obsérvese, en este sentido, que la identificación ha sido un importante caballo de batalla tradicional para el IECM como se demuestra, por ejemplo, con la reseña del Comité Técnico creado en 2019 en el que da cuenta de las “quejas de la ciudadanía, durante el desarrollo de la jornada electiva en su modalidad presencial ordinaria, sobre que aparecen en el listado de Voto Electrónico, cuando no han ejercido su voto/emitido su opinión de manera electrónica” (: 43 / Opinión).

El reconocimiento biométrico constituye una medida encomiable que ha logrado sus frutos, pero que también refleja la existencia de un sustrato social en el que la confianza social mutua y en las instituciones es todavía incipiente como para proponer medidas basadas en la auto-responsabilidad. Destacan, en este sentido, las verificaciones muestrales que lleva a cabo el IECM sobre la entrega de Claves de Voto por Internet por correo certificado para evitar fraudes en este proceso.

Sea como sea, debe recordarse que la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación (TEPJF) ya tuvo ocasión de pronunciarse sobre la relevancia de la libertad del

votante y su impacto sobre un mecanismo de voto electrónico. Aludimos, en concreto, a la sentencia que validó el sistema implantado en 2012 para los vecinos del Distrito Federal residentes en aquel momento en el extranjero. Tras un análisis de las garantías técnicas del sistema de voto electrónico propuesto, a la sazón parecido al actual salvando las innovaciones técnicas añadidas posteriormente, el Tribunal concluye que corresponde a los propios ciudadanos la salvaguarda de las claves de votación que les han sido proporcionadas y, en este sentido, cabe deducir que las eventuales suplantaciones quedan ya fuera del radio de acción de la administración electoral:

> "esta Sala Superior, a partir de las reglas de la experiencia y la lógica, estima que el sistema cumple con estándares suficientes de seguridad, ya que su funcionamiento es similar al que se utiliza en otros sistemas de internet para accesar a sitios electrónicos que requieren altos niveles de seguridad y confianza, como es la banca en línea o el procesamiento de compra de diversos productos, en el cual se proporcionan los datos de una cuenta de banco o una tarjeta de internet, en cuyos casos, las claves de acceso son personales y de responsabilidad de su titular*, como sucede en el caso que se analiza*" [SUP-JRC-306/2011, cursiva añadida; el Comité Técnico creado en 2019 recuerda este argumento (: 40 / Opinión), aunque también utiliza una cita parcialmente errónea de la sentencia que además se refiere a los argumentos planteados por el recurrente, a la sazón el Partido de la Revolución Democrática, y no la propia Sala Superior del Tribunal: "al implementarse la modalidad de voto electrónico por internet ... el Instituto Electoral del Distrito Federal privilegió el derecho a votar y confió en la responsabilidad y formación cívica del ciudadano ..." (: 37 / Opinión)]

Llegados a este punto y más allá de la equiparación como mínimo discutible entre voto electrónico y otros servicios digitales como los financieros, cabe preguntarse si el mismo razonamiento sería aplicable a los comprobantes de votación. Si el Tribunal no veía ningún inconveniente en confiar en la responsabilidad de cada ciudadano para gestionar las claves de acceso, lo mismo podría llegar a afirmarse en cómo gestionar documentos en los que se plasme qué opción de voto se ha escogido. Aunque a primera vista los segundos parecen más problemáticos al contener el contenido del voto, lo cierto es que los primeros pueden igualmente derivar en fraudes electorales, sea por suplantación, algo muy mitigado con el novedoso reconocimiento facial, sea por coacción. Además, no cabe banalizar este último riesgo a la vista de los comportamientos clientelares detectados en ciertas zonas de la Ciudad.

Es por ello que, siguiendo el criterio del propio Tribunal, una primera opción consistiría en contemplar la posibilidad de implantar la mencionada verificabilidad individual para las fases de emisión y almacenamiento de los sufragios. Además, los ejemplos comparados también nos muestran opciones que anudan tal verificabilidad individual con el combate a las presiones recibidas por el elector. Diversos países han implantado, en este sentido, el voto múltiple, es decir, atribuir al elector la facultad de emitir diversos sufragios, entre los que finalmente solo se retiene uno, sea el último llevado a cabo remotamente desde entornos no controlados sea el realizado en la propia casilla de votación y, por lo tanto, con las garantías habituales en lo relativo a la garantía del secreto del sufragio y la libertad del votante.

El voto múltiple genera habitualmente un cierto escepticismo e incluso rechazo ya que a primera vista puede aparecer como algo contradictorio con el principio "una persona, un voto". Tal reacción se fundamenta, sin embargo, en una comprensión incompleta de las funcionalidades de esa práctica ya que, si se contempla en todas sus dimensiones, puede concluirse que nos hallamos ante una técnica muy efectiva para combatir cualquier amenaza que se cierna sobre el elector, sea la suplantación, la coacción en el momento de la propia votación e incluso la presión para desvelar el contenido de los comprobantes de voto. Todo ello queda enormemente mitigado ante la realidad de que el elector, tras haber sufrido estas coacciones, puede volver a emitir otro sufragio privando de razón de ser a las mencionadas amenazas.

Además, los sistemas de voto múltiple presentan diversas variantes ya que algunos prevén la combinación de voto electrónico y en papel, en cuyo caso prima siempre el segundo, o también un posible voto anticipado en papel antes del emitido en formato electrónico. En este caso, la coacción perderá todo sentido ya que el sufragio finalmente escrutado no será ni el llevado a cabo durante la coacción ni tampoco ninguno posterior, sino uno que ya se habría emitido con anticipación y con desconocimiento del atacante.

Debe reconocerse que todas estas opciones aumentan la complejidad de la logística electoral, pero también es cierto que solamente son necesarias en la medida de que la coacción al votante, y no la responsabilidad individual a la que se aferraba el Tribunal, sea una amenaza real. El IECM puede ir modulando las diversas variantes de voto múltiple llegando incluso a su supresión, pero siempre se mantendrá como resultado positivo la presencia de comprobantes fruto de la verificabilidad individual ya analizada.

E) Registro de eventos (logs) inmutables

Una de las ventajas más importantes del voto electrónico, respecto al voto tradicional en papel, consiste en que toda acción deja una huella que posteriormente puede ser útil para analizar y descubrir los motivos de fallas, las intrusiones, las manipulaciones y cualquier transacción que haya sido realizada dentro del entorno del sistema. Existen herramientas que realizan el registro de cada transacción (logs), indicando fecha, hora, usuario y acción realizada. Tales herramientas generalmente están incluidas en los propios sistemas operativos de las computadoras y servidores, así como en los dispositivos de red.

Pese a las ventajas que ofrece la generación de *logs* a nivel de sistema o red*,* no se puede garantizar solo con ellos un mecanismo certero para una auditoría post-electoral, ya que puede haber casos de atacantes con privilegios de acceso, por lo que también podrían modificar los *logs* a fin de eliminar cualquier prueba de la manipulación.

Se recomienda diseñar un mecanismo de registro y protección de *logs* que se adapte al sistema electrónico de votación del IECM. Los *logs* pueden ser generados y protegidos a través de técnicas criptográficas simples tales como funciones hash o firmas digitales y con el encadenamiento de los mismos, lo que ayuda a saber con más precisión en donde se llevó a cabo alguna manipulación. Una vez que se ha usado alguna técnica de inmutabilidad, deben ser almacenados en un entorno seguro.

F) *Marco legal*

El 16 de noviembre de 2019 el IECM aprueba los denominados *Lineamientos Generales del Sistema Electrónico por Internet* (IECM/ ACU-CG-077 /2019). Se trata de un documento en el que, a través de 53 artículos, se describe el funcionamiento del sistema de votación con mecanismos informáticos. El mismo día, por acuerdo IECM/ ACU-CG-078/2019, se decide utilizar el voto electrónico para recabar votos y opiniones para la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021. Finalmente, el mismo día y por acuerdo IECM/ ACU-CG-079/2019, se publica la convocatoria general para la Elección de las Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021.

Sin perjuicio del análisis en detalle de aspectos concretos de tales textos, interesa ahora llamar la atención sobre el lapso de tiempo entre la aprobación y su implantación efectiva. Entre la fecha indicada y el inicio de la votación transcurren unos escasos cuatro meses, lo que se antoja insuficiente.

Debe señalarse, en primer lugar, que el canon internacional más habitual al respecto desaconseja modificaciones sustanciales del marco normativo electoral que tengan lugar en los últimos doce meses antes de las elecciones. Pueden consultarse, en este sentido, las directrices de la Comisión de Venecia al respecto (Código de Buenas Prácticas en Materia Electoral / § II.2.b). En nuestro caso, habida cuenta que en algunos distritos no existía modalidad alternativa al voto electrónico, la aprobación de los lineamientos debe ser considerada como un cambio sustancial en el que debería aplicarse la directriz temporal reseñada.

En este sentido, conviene anticiparse a una posible objeción que enfatizara el componente puramente técnico de los lineamientos en contraste con otras regulaciones que establecen los derechos de participación política de los ciudadanos. Siguiendo este razonamiento, los lineamientos no alterarían de hecho la forma de participación de los electores, sino que se limitarían a establecer ciertas cautelas técnicas y, como tales, se trataría de cuestiones neutrales que podrían escapar del citado marco temporal establecido a nivel internacional.

Lo cierto, sin embargo, es que una de las aportaciones del voto electrónico consiste precisamente en difuminar esa barrera entre lo meramente técnico u organizativo y las decisiones jurídicas relevantes a efectos de garantías electorales. Con el voto electrónico, lo técnico adquiere también suma trascendencia. Es útil aquí, por ejemplo, referirnos a la multicitada sentencia del Tribunal Constitucional Federal germano en la que se enfatiza el carácter público y el necesario control ciudadano de todo lo técnico, al menos en el ámbito electoral.

Todo ello es si cabe más paradójico si tomamos en consideración que el programa de voto electrónico en Ciudad de México tiene, como ya se ha relatado, una larga trayectoria. No habría, por lo tanto, razón alguna para que los lineamientos no pudieran ser aprobados, o actualizados, con una anticipación mayor a la jornada electoral. No nos hallamos, en definitiva, ante una precipitación técnica, sino ante una práctica quizás habitual en otros ámbitos organizativos que debería mejorarse en ocasiones futuras.

Debe señalarse, en todo caso, que la Ciudad de México ha vivido una profunda transformación constitucional en los años más recientes. Tal cambio ha propiciado una cadena de adaptaciones normativas, con las consiguientes demoras, y todo ello acabó afectando la labor del IECM ya que se hallaba a expensas de las regulaciones aprobadas a nivel legislativo.

Tal factor puede explicar el escaso lapso de tiempo para la preparación del marco normativo del voto electrónico, con sus correspondientes desarrollos y controles, pero debería evitarse en el futuro que los imponderables políticos o constitucionales acaben perjudicando cuestiones que pueden resolverse en planos diferentes. En este sentido, la aprobación de lineamientos, los desarrollos informáticos y las auditorías deberían articularse como proyectos de larga trayectoria. El voto electrónico debe, en definitiva, desarrollarse en paralelo a la organización de consultas populares concretas de tal forma que, cuando éstas se convoquen, su normativa se limite a recoger lo que ya haya estado validado a nivel técnico con suficiente anticipación.

G) Normativa sobre auditorías

Según la propia documentación del IECM, la transparencia constituye uno de los tres factores que rigen el sistema juntamente con la autenticación del elector y las cuestiones de seguridad física y lógica de la infraestructura.

El programa de voto electrónico incluye la realización de una auditoría externa, lo que merece una valoración muy positiva. Como es sabido, la cadena de confianza en los casos de voto electrónico no puede reposar únicamente en los procedimientos tradicionales. Si en el voto en

papel se hace preciso incluir elementos externos a la administración que aporten confianza, lo que en México ha venido en llamarse la ciudadanización del procedimiento electoral, el uso del voto electrónico exige enfatizar este componente, es decir, requiere controles e intervenciones suplementarias por parte de actores ajenos a los poderes públicos.

De forma más concreta, a la vista de las particularidades técnicas del voto electrónico, la presencia de ciudadanos anónimos en la administración electoral es necesaria, pero no suficiente dado que no tendrán los conocimientos apropiados para valorar si lo realizado a nivel técnico es apropiado o no. Es por ello que las auditorías externas deben ser aplaudidas.

Sea como sea, constatar que se ha llevado a cabo una auditoría externa, como en nuestro supuesto de análisis, constituye solo un primer paso que debe ir acompañado de la valoración de otros parámetros. Resultará relevante, por ejemplo, conocer cómo se ha seleccionado al auditor, de qué tiempo ha dispuesto para llevar a cabo el análisis técnico, qué información le ha sido proporcionada, cuáles han sido las cláusulas de confidencialidad pactadas, cuál es el alcance real del análisis y, sobre todo, qué régimen de publicidad se aplicará al informe final de la auditoría.

Es absurdo, por lo tanto, contentarse con el mero hecho de que exista una auditoría ya que tal iniciativa podría quedar seriamente sesgada si los parámetros enunciados en el párrafo anterior no satisfacen lo que se espera de estos estudios técnicos. En este sentido, conviene recordar que el motivo por el que se contrata una auditoría en este campo difiere de las razones por las que análisis similares se llevan a cabo en otras áreas. Normalmente, muchas aplicaciones técnicas necesitan ser auditadas, o certificadas u homologadas, antes de su puesta en marcha. Se trata de procedimientos de armonización y control de calidad ampliamente implantados en todo proceso productivo.

En el caso del voto electrónico, las auditorías persiguen también tal armonización y calidad contrastadas, pero incluyen asimismo otros objetivos, como la generación de confianza entre los ciudadanos. La auditoría deberá verificar que el sistema funciona, pero también hacerlo de tal forma que los ciudadanos queden convencidos que no ha habido ningún fraude. Este segundo objetivo es más difícil de lograr dado que, teniendo en cuenta la naturaleza propia del voto electrónico, los ciudadanos no tendrán otros elementos en qué apoyarse para comprobar la funcionalidad del nuevo instrumento. Mientras que cualquiera puede detectar si un tren alcanza o no la velocidad programada, el voto electrónico no ofrece tal facilidad para ser controlado y entonces la auditoría constituye un instrumento de gran ayuda, aunque su tenor literal será incomprensible para la mayoría de ciudadanos. Se trata de un gesto de transparencia que, si bien no será comprensible para todos, sí podrá ser evaluado por expertos independientes e inyectar de este modo confianza suficiente en el conjunto de la ciudadanía.

Es por ello que, más allá de su contenido, el procedimiento seguido para auditar, que sí podrá ser evaluado por cualquier ciudadano, se erige como un factor primordial para generar confianza.

Marco temporal

En el caso sometido a nuestro análisis, existe de entrada un primer elemento susceptible de mejora. Se trata del marco temporal disponible para la ejecución del conjunto de la auditoría. Si el marco normativo, como ya se ha referido, se aprueba ya con mucho retraso en comparación a lo que hubiera sido deseable, la auditoría arranca incluso después y dispone, por lo tanto, de un lapso temporal muy ajustado para realizar sus labores.

Se trata de un elemento que la propia auditoría pone de relieve, aunque lamentablemente lo hace una vez ya completada la votación. El informe reza, en sus párrafos finales, como sigue:

> "Se recomienda que para posteriores versiones se cuente con el *tiempo* y recursos *suficientes* para que se realicen pruebas exhaustivas y que los simulacros se realicen con parámetros muy cercanos a los que se manejarán durante la jornada.
>
> Se recomienda en la medida de lo posible tener los requerimientos con *suficiente tiempo de anticipación* y congelar el diseño a partir del 1er simulacro, a partir del cual los únicos cambios que debería haber son los relacionados con la corrección de errores" [: 8 / Informe I; cursiva añadida]

Llama la atención que el informe no reclame *mayor* tiempo de anticipación, sino *suficiente* lapso temporal. Se trata de un matiz relevante ya que, mientras que en la primera opción puede presumirse que las labores de supervisión se han llevado cabo de forma completa, la segunda despierta dudas sobre las propias tareas auditoras. Es al menos lo que cabe deducir al constatar que no se ha dispuesto de tiempo suficiente para analizar los requerimientos normativos y técnicos relativos al voto electrónico.

Todo ello se agrava además si prestamos atención a la cadena de disposiciones normativas que se inicia con los acuerdos del Consejo ya reseñados. Si bien es cierto que en el acuerdo IECM/ ACU-CG-077 /2019 se plasman lineamientos que el sistema de voto electrónico deberá respetar, nos hallamos todavía ante un cuadro incompleto ya que los alcances totales de ciertas actuaciones, entre las que se halla singularmente la propia auditoría, no se determinarán hasta que se complete un "instrumento jurídico" entre IECM y la auditora en el que se establecerán:

> "I. Los alcances mínimos de la auditoría, establecidos en los presentes Lineamientos y el plan de trabajo asociado al mismo [sic];
> II. La información que la autoridad electoral administrativa pondrá a disposición del ente auditor, salvaguardando en todo memento los derechos de la propiedad intelectual y la protección de los datos personales de las y los ciudadanos" (art. 50 / Lineamientos)

Tal instrumento jurídico no se concreta hasta el 24 de febrero de 2020 mediante acuerdo en el IECM y la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México (UNAM). Restaban, por lo tanto, menos de dos semanas para el inicio de la votación y para el desarrollo de la auditoría, al menos si atendemos a las fechas en las que se formalizaron los documentos. Además, el acuerdo contiene un *Anexo técnico para la auditoría al sistema informático y a la infraestructura tecnológica del Sistema Electrónico por Internet (SIE 2020)*. Dado que algunos incisos de este anexo desarrollan y amplían lo dispuesto en los Lineamientos aprobados en noviembre de 2019 y teniendo en cuenta que los informes posteriores de la firma auditora se refieren de forma explícita a tal *Anexo* [: 3 / Informe I; cursiva añadida], debe concluirse que el marco normativo específico para la implantación del SIE no queda realmente definitivamente asentado hasta finales de febrero de 2020. Se trata de un factor que podrían experimentar claras mejoras en futuras ocasiones redundando de este modo en un renovado flujo interno de adopción de decisiones en el seno del IECM.

Selección de la entidad auditoria

Determinar quién o quiénes van a realizar la auditoría no es un factor baladí ya que puede influir decisivamente en la percepción de la ciudadanía sobre la labor de evaluación que se lleve a cabo. Sin perjuicio de la calidad técnica que pueda ofrecer la auditoría en sí misma, los resultados globales pueden ser insatisfactorios si no se logra forjar una confianza suficiente en los propios electores. Recuérdese, en este sentido, que las auditorías de voto electrónico no aspiran únicamente a comprobar la fiabilidad técnica de la herramienta, sino también a consolidar la confianza de todos los interesados.

Deberán considerarse, entre otros elementos, la disponibilidad del sistema para que cualquier solicitante pueda realizar su correspondiente auditoría y, en caso de que no se permita tal apertura, los criterios utilizados por la administración electoral para identificar a la entidad auditora, el sistema de retribución establecido y los acuerdos de confidencialidad que se hayan podido alcanzar entre las partes contratantes.

Cabe empezar señalando que el sistema utilizado por el IECM no prevé, por el momento, una apertura que permita realizar una auditoría técnica a cualquier persona interesada en hacerlo. Ni el código fuente ni otros componentes esenciales del sistema de voto electrónico se ponen a disposición del público a tales efectos.

Pese a que tal opción suscita obvios interrogantes, en su mayor parte relativos a las brechas de seguridad que pudieran ocasionarse con la publicación de elementos técnicos altamente sensibles del sistema, debe recordarse que existen ya casos a nivel comparado que han aceptado tal grado de apertura y, entre todos ellos, el noruego merece especial atención ya que la apertura se promovió con especial intensidad y desde la propia administración electoral. Nos referimos al uso de voto por internet en las elecciones celebradas en 2011 y 2013. Supusieron entonces un salto cualitativo en lo relativo al análisis externo e independiente de los sistemas de voto electrónico. Se trata además de mecanismos que, en mayor o menor medida, han sido replicados después en otros países. Los tests realizados en Suiza en 2019 y la normativa estonia sobre supervisión del voto electrónico se nutren en parte de la anterior experiencia noruega.

Si todo ello ha sido posible en estos países, el IECM podría plantearse un esquema de auditoría técnica que no quedara reducido a las entidades seleccionadas por el propio Instituto, sino que instaura una plataforma a la que diversos interesados pudieran acceder para realizar su supervisión. Se trata lógicamente de protocolos que requieren mayor detalle y precisión, pero debe retenerse como mínimo el principio aperturista a diversas entidades.

Cabe añadir a todo ello que, a nivel estrictamente técnico, las preocupaciones por la seguridad del sistema son habitualmente rebatidas por gran parte de la comunidad académica al entender que la oscuridad nunca es la mejor forma de alcanzar la mayor seguridad en una aplicación informática. *Security by obscurity* no es, en este sentido, un patrón de comportamiento recomendable y el IECM es consciente de ello ya que por eso se admite la participación de una firma auditora, aunque se hace de forma limitada y con un aperturismo menos ambicioso del hallado en otros países.

En relación con los criterios utilizados para seleccionar a la entidad auditora, cabe señalar que los datos disponibles son por el momento escasos. Partimos de lo señalado en los propios *Lineamientos* al prever “una auditoría pública en cada una de sus etapas de desarrollo e implementación, a través de instituciones o empresas con prestigio internacional” (art. 48). A tenor de esta formulación, cabe indicar, en primer lugar, que no se excluye la posibilidad de que entidades de lucro participen en la auditoría pública. Se emplea, por otro lado, una formulación difusa y genérica como la de “prestigio internacional”, que, salvo que se concrete en algún otro tipo de disposición, pierde casi toda eficacia real. Quedan excluidos entes de dimensión únicamente local, pero el abanico de otras Instituciones susceptibles de encajar en esa definición de prestigio internacional es demasiado amplio. Sería recomendable, en este sentido, que el IECM estableciera criterios más rigurosos para poder acotar el perfil de entidades susceptibles de llevar a cabo la auditoría.

Del mismo modo, tampoco se determina el procedimiento de selección. Los *Lineamientos* no aclaran si existirá una convocatoria pública a la que puedan presentarse diversas entidades y si el IECM estará obligado a tomar en consideración diversas opciones con la baremación

correspondiente. Se trata de nuevo de factores nada baladíes. Puede darse el caso que el IECM identifique con claridad una firma auditora de comprobada excelencia y reputación, pero, si la selección no va acompañada de un procedimiento competitivo, público y transparente, lo ganado con la auditoría puede perderse por los déficits en su selección.

En el caso de estudio, la Facultad de Estudios Superiores (FES) Aragón de la UNAM ha llevado a cabo la auditoría. Se trata de la misma entidad que ha venido colaborando con el IECM en los últimos años y que, entre otras tareas, también desarrolló la auditoría externa encargada en julio de 2017 con la perspectiva de uso del voto electrónico en las elecciones de 2018. En aquella ocasión, otra entidad –*Scanda Kimat*— también llevo a cabo una segunda auditoría.

A tenor de los datos recabados del propio IECM, no se realizó licitación pública para la auditoría, sino que se remitieron invitaciones directas a siete instituciones académicas con representación en la Ciudad de México. Las invitaciones se cursaron a principios de febrero otorgando un plazo breve de tiempo para la respuesta de los potenciales interesados. Se trata de una restricción temporal que daña la credibilidad del proceso ya que, más allá de sus causas reales, quizás justificadas por el calendario ajustado al que ya se ha hecho mención, puede ser percibida como una maniobra para excluir determinados candidatos.

En relación con los criterios específicos para determinar la presencia o no de prestigio internacional y para calibrar la solvencia de los candidatos, el IECM llevó a cabo una evaluación técnica en la que se concluye que FES Aragón cumple con los requisitos establecidos (Acuerdo COEG-09-20, de 17 de febrero). El análisis se sustenta en un *Anexo técnico para la contratación de los servicios de auditoría al sistema informático y a la infraestructura tecnológica del Sistema Electrónico por Internet (SEI 2020).* Se trata de una tabla en la que, a partir de un listado detallado de requisitos, el Instituto concluye, de forma escueta y concisa, que la propuesta cumple con lo solicitado, pero no se aportan mayores detalles o comentarios al respecto. El *Anexo* se adjuntó en las invitaciones antes mencionadas, pero se desconoce si obtuvo mayor difusión antes de la adjudicación de las tareas auditoría.

A la vista de lo señalado, cabe señalar que el actual proceso de selección de entidades auditoras es susceptible de ser perfeccionado incorporando, por un lado, criterios que estén directamente vinculados con el prestigio internacional que se menciona en los *Lineamientos.* Ahora mismo, por ejemplo, el *Anexo técnico* no incluye parámetros de este tipo.

Por otro lado, sería oportuno tomar en consideración criterios de excelencia institucional que guarden relación con la capacidad de la auditora en términos generales y no únicamente sobre las tareas específicas a realizar sobre el voto electrónico. Se trataría de calibrar el *status* de la auditora como tal y no solamente su capacidad para desarrollar aspectos técnicos concretos. En Francia, por ejemplo, se exige que las auditoras cuenten con determinados sellos de calidad.

Por último, conviene dotar de mayor publicidad al anexo técnico que se utiliza para valorar la solvencia de cada propuesta.

Por otro lado, debe señalarse que la retribución es sufragada por el propio IECM, lo que resulta congruente con el hecho de contar con una plataforma de voto electrónico desarrollada internamente en el Instituto. Se trata de un esquema diferente al existente en otros países en los que, al existir empresas con soluciones privadas de voto electrónico, las auditorías requeridas por la administración son financiadas por las propias empresas. Tal solución no es factible en el caso del IECM, pero no debe olvidarse que identificar quién financia la auditoría constituye también un factor primordial para valorar la confiabilidad del producto resultante y todo ello sin

perjuicio de la calidad intrínseca que puedan tener los informes aportados, extremo que escapa al análisis que se lleva a cabo en este apartado.

Para terminar con el análisis del procedimiento de selección de una firma auditora, conviene hacer referencia a la existencia de acuerdos de confidencialidad entre la auditora y la entidad propietaria del producto. Tales documentos o *Non-Disclosure Agreements (NDA)* son de suma importancia ya que pueden contener cláusulas que comprometan la fiabilidad de todo el análisis. Puede suceder, por ejemplo, que ambas partes acuerden excluir ciertos aspectos de la auditoría o que acuerden llevarla a cabo sin consultar determinada documentación. Ambos pactos pueden ser razonables, pero, al estar incluidos en un acuerdo de confidencialidad, los lectores desconocerán que están consultando un análisis realmente incompleto y ninguna de las partes podrá informarles al respecto ya que estarán ligadas al NDA que hayan suscrito. Es por todo ello que los acuerdos de confidencialidad son de vital importancia. No olvidemos además que son moneda de uso corriente en las labores de auditoría.

En el caso que nos ocupa, el marco normativo establecido por el IECM no alude a ningún acuerdo de este tipo. Como ya se ha señalado, los *Lineamientos* prevén un instrumento jurídico acordado entre IECM y la entidad auditora en el que se detallarán las labores a realizar y la documentación a recibir, pero no se incluye ninguna mención a la confidencialidad. Si se consulta el mencionado acuerdo, cuya publicidad no viene impuesta en los *Lineamientos*, interesa destacar la décima cláusula en la que, tras aludir a las obligaciones de confidencialidad de ambas partes y a la sumisión al ordenamiento jurídico, también se prevé la firma "de un acuerdo de confidencialidad o de No divulgación" entre la UNAM y el IECM. Se trata, por lo tanto, de un nuevo acuerdo diferente al contrato en el que se incluye esta décima cláusula.

Este documento no ha sido consultado para la realización de este informe y resulta imposible, por lo tanto, aventurar su contenido. Sea como sea, conviene alertar sobre su importancia en los casos de voto electrónico. Ya se ha mencionado que tales NDA son habituales en este tipo de tareas y su presencia no debería causar extrañeza, pero tampoco debe olvidarse que la finalidad de las auditorías de voto electrónico va más allá de la comprobación técnica y persigue afianzar la confianza ciudadana. En este sentido, cualquier pieza que escape al control ciudadano es susceptible de crear dudas que empañen el conjunto del proceso. Es por ello que conviene evaluar la necesidad de contar con un acuerdo de este tipo y suprimirlo en caso de que no sea estrictamente preciso.

Debe analizarse también la opción de hacerlo público. Obsérvese, en este sentido, que el acuerdo determina qué es lo confidencial, pero no señala que el documento en sí mismo sea de acceso reservado. Se trata de dos componentes que no deben confundirse.

Criterios de evaluación

Las plataformas de voto electrónico son herramientas informáticas de gran sofisticación técnica y deben cumplir por ello unos parámetros exigentes de funcionalidad, seguridad o integridad, pero, al tratarse de aplicaciones a utilizar en procesos de representación democrática, existen también otros criterios que conviene tener en cuenta.

La lectura de la documentación aportada por el IECM nos permite destacar diversos aspectos relacionados con los criterios a utilizar durante la auditoría. En primer lugar, el marco normativo establecido incluye parámetros singularizados a los que firma auditora deberá acomodarse al efectuar su análisis. Entre otros documentos, ya se ha mencionado que tanto los *Lineamientos* como el *Anexo* incluido en el acuerdo con la firma auditora especifican ciertos criterios de análisis. Por otro lado, los informes del *Comité Técnico* o el *Estudio de viabilidad* efectuado por

las unidades correspondientes del IECM también suelen hacer referencia a diversos principios que el sistema de voto electrónico debe respetar.

Nos hallamos, por lo tanto, ante un escenario positivo en el que la firma auditora no tendrá plena libertad para obrar de la forma que considere más conveniente, pero se han identificado determinadas áreas de oportunidad en las que el Instituto podría fortalecer y clarificar el marco en el que se ejecuta la auditoría.

Se ha detectado, en primer lugar, un cierto desequilibrio en lo atinente a los criterios técnicos o democráticos del voto electrónico. Los documentos antes reseñados, y especialmente los *Lineamientos* y el acuerdo con la firma auditora, se esfuerzan por dejar constancia de los diversos tests técnicos que se espera llevar a cabo, tales como los de funcionalidad o seguridad, con especificaciones incluso más detalladas que llevan a mencionar, entre otras, las pruebas de denegación de servicio, los test de penetración, los análisis de vulnerabilidades o las pruebas de estrés.

Se trata de elementos necesarios en todo producto informático, pero llama la atención cómo lo que podríamos denominar criterios democráticos merecen menos atención. Así, por ejemplo, en el apartado dedicado a la auditoría dentro de los *Lineamientos*, existe únicamente una apelación final cuando, al describir el dictamen que deberá hacerse público, se alude al principio de elegibilidad del votante, al secreto, a la vinculación de un solo voto por elector y a la "efectiva emisión, transmisión, recepción y cómputo del sufragio emitido" (art. 52).

Además, si repasamos la totalidad de la documentación obrante sobre el sistema de voto electrónico, deduciremos con facilidad que, en términos generales, las apelaciones a los criterios democráticos de toda votación no rebasan alusiones genéricas como las señaladas en el párrafo anterior y que en diversas ocasiones los informes parecen conceder más importancia a unos principios sobre otros. No son pocos, por ejemplo, los casos en los que los documentos aluden, incluso en su propio título, al principio de "un votante, un voto", pero no sitúan al mismo nivel otros principios de igual rango.

Debe señalarse, en este sentido, que los criterios enunciados tanto en el artículo 52 de los *Lineamientos* como en otros documentos no agotan los principios por los que debe regirse una elección democrática, sobre todo si tenemos en cuenta las características enormemente especiales que rodean a una votación por Internet. Existen esfuerzos a nivel internacional que han intentado acomodar al voto electrónico las garantías tradicionales presentes en cualquier convocatoria electoral y, entre todos ellos, destaca por su trascendencia la labor desarrollada por el Consejo de Europa tempranamente desde 2004. En este sentido, la Recomendación 2017(5), sobre estándares del voto electrónico, supone la actualización de la antigua Recomendación 2004(11) sobre el mismo ámbito y aporta una lista sistematizada de criterios detallados que singularizan para el voto electrónico el significado de los principios de universalidad, libertad, secreto e igualdad del sufragio.

Una lectura somera de tales documentos permite descubrir con facilidad cómo los requisitos establecidos por la regulación mexicana son demasiado genéricos y tienden a orillar los parámetros democráticos en beneficio de elementos de análisis puramente informáticos.

No se trata, por otro lado, de un hecho infrecuente ya que lo mismo sucede en otros países y es fruto del desequilibrio entre el protagonismo de los técnicos informáticos, cuya presencia y labor es indispensable, y las aportaciones de otros analistas de carácter más social, como juristas o politólogos. Una combinación más intensa de ambas perspectivas aunada con una consulta de los documentos internacionales ya mencionados generaría un área de oportunidad en la que el

IECM podría establecer un listado de requerimientos sistemático y más detallado para la auditoría de cualquier sistema de voto electrónico. Adviértase, en este sentido, que, pese a la profusa y variada documentación generada por el IECM, no se dispone aun de un listado con las características reseñadas. Los *Lineamientos* aspiran a ejercer ese rol, per su contenido actual debe ser actualizado y ampliado.

Publicidad

En relación con el marco jurídico aprobado para la realización de la auditoría, ya conocemos que los propios lineamientos determinan tanto el alcance como algunas de las pruebas que la entidad auditora deberá obligatoriamente llevar a cabo (art. 49). Sea como sea, ciertos detalles se delegan a otro "instrumento jurídico" (art. 50) a convenir entre el Instituto y el ente auditor. No se precisa, sin embargo, la publicidad de tal acuerdo. Nótese que, según la propia auditoría, tal instrumento contiene un Anexo técnico donde se detallan los parámetros a analizar. Se trata, por lo tanto, de una documentación del máximo interés que debería estar a disposición de los analistas, aunque ello requiriera mantener en secreto ciertos elementos del acuerdo contractual.

Cabe repetir además aquí lo señalado en relación tanto con los acuerdos de confidencialidad como con el anexo técnico utilizado por el propio Instituto para evaluar la solvencia de las diferentes candidaturas de entidades auditoras.

En la misma línea, los *Lineamientos* establecen una distinción en la documentación a entregar por la auditora al Instituto. Existen tanto "informes parciales" como un "dictamen", pero solamente en el segundo se detalla su carácter público (art. 52). Tal documento deberá constatar tanto la restricción del sistema a las personas elegibles para emitir un solo sufragio secreto como la integridad en la custodia de tal voto. Nos hallamos ante un equilibrio delicado entre informes parciales de publicidad limitada y un documento final cuyo contenido puede acabar siendo muy genérico, es decir, que recoja conclusiones y datos estadísticos, pero no profundice en aspectos de fondo. Retomando lo ya señalado, se recomienda favorecer la publicidad de la totalidad de la documentación aportada por la entidad auditora. Si se entiende que tal criterio puede perjudicar la propia seguridad del sistema, cabe contemplar la publicación completa *a posteriori* de los informes correspondientes. Nótese, en este sentido, que el acuerdo firmado entre el IECM y la entidad auditora señala que los informes parciales tienen "calidad de reservados en términos de las disposiciones aplicables en materia de transparencia y acceso a la información" (: VII).

Debe señalarse finalmente que el IECM ha publicado en su página web tanto un informe sobre el software como dos documentos posteriores a los días de votación, todos ellos elaborados por los responsables de FES Aragón de la UNAM. Dejando a un lado el primer dictamen sobre el software, los otros dos consisten, por un lado, en un informe de la auditoría informática abarcando del 7 al 15 de marzo y, por otro, un "informe de Evaluación de la Auditoría Informática" abarcando solamente entre el 15 y 17 de marzo de 2020.

El segundo documento revisa la operatividad del sistema de voto electrónico, identifica los errores detectados en las dos modalidades de sufragio y extrae tanto conclusiones como recomendaciones para futuros usos. Sin perjuicio de las observaciones sobre estos documentos que se aportarán en secciones posteriores, interesa ahora destacar que el segundo informe se refiere a un "análisis forense para verificar las causas del incidente, las cuales fueron informadas al IECM para que las tome en consideración para el futuro" (: 7 / Informe I). Habida cuenta de que nos hallamos ya en el periodo posterior a la propia votación, cabe preguntarse por la posibilidad de que estos análisis también se hagan públicos, lo que contribuiría a afianzar la confianza y transparencia del proceso de voto electrónico en su conjunto.

Finalmente, existe asimismo un *Comité Técnico* que, de acuerdo con los *Lineamientos*, se activa entre dos y seis meses antes de la convocatoria respectiva, dependiendo del tipo de consulta o elección que esté prevista, y puede alargar sus labores hasta haberse realizado la jornada respectiva (art. 15). Sus tareas consisten, entre otras, en "proponer mejoras y opinar sobre el desarrollo del Sistema" [art. 16 b)], que se recibirán como muy tarde tres meses antes de la jornada correspondiente, y sobre todo "validar los esquemas de seguridad para la protección e integridad del Sistema" [art. 16 d)]. El Comité estará compuesto por cinco especialistas designados por el Consejo General.

Se trata de una medida muy valiosa que fortalece el sistema de seguimiento de la implantación del voto electrónico. Cabe destacar asimismo la voluntad del regulador de asegurar una intervención temprana de este organismo para permitir posibles modificaciones.

H) Auditoría / Aspectos técnicos

Habiendo revisado el informe de Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IEC, realizado por personal de la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México, se puede observar que la metodología empleada es adecuada, al seguir estándares internacionales. Más allá de tal constatación, se recomiendan las siguientes acciones para futuras auditorías:

a) Realizar una mayor cantidad de pruebas de caja negra para cada caso de prueba. Es importante en estos supuestos contemplar diversas variables para realizar la misma prueba: varias personas, diversos equipos de cómputo con diferentes versiones de sistema operativo, días y horarios diferentes, etcétera. Todo ello asegura con mayor probabilidad acercarse a los escenarios reales.
b) Incluir en la auditoría de código fuente la funcionalidad de registro de votantes en las aplicaciones móviles, considerando que la fase de registro es tan relevante como las posteriores del proceso de elección.
c) Realizar pruebas de estrés bajo diferentes escenarios como, por ejemplo, en días y horarios diferentes, ya que puede haber una variación en el tráfico de red y, por lo tanto, en la capacidad de respuesta del proveedor del servicio de internet.
d) En esta elección se detectaron dos computadoras diferentes que fueron utilizadas en los diversos procesos de la elección, aparentemente una de ellas propiedad del IECM y otra del administrador del sistema. Sabiendo la importancia que tienen dichos equipos en la configuración y seguridad del sistema, se recomienda que todas las computadoras utilizadas en dichos procesos sean incluidas como parte de la auditoría realizada por la entidad externa. Se corroborará así que no tengan ningún tipo de malware u otras herramientas que pudieran afectar su correcto funcionamiento.
e) En el informe se describe que se siguió el estándar OSSTMM y que una de las áreas que se prueban es la "robustez de los controles implementados para la seguridad de la información y de datos" (: 4 / Informe II). Se puede observar que se realizaron pruebas a nivel de infraestructura de redes, pero, en el informe de auditoría, no hay pruebas de que se haya analizado la seguridad de los protocolos criptográficos utilizados y su correcta aplicación. Es probable que estos mecanismos de seguridad hayan sido verificados a nivel de funcionalidad como parte de las pruebas de caja negra, pero la auditoría de este tipo de sistemas debería analizar la seguridad de dichos protocolos con dos enfoques: a nivel conceptual y a nivel de ejecución.

I) Escalabilidad del sistema

La usabilidad y accesibilidad de todo sistema informático constituyen parámetros para medir su utilidad a nivel práctico. Debe notarse, en este sentido, que la propia normativa local recuerda la existencia de "parámetros internacionales de accesibilidad con el objeto de garantizar la

participación de todas las personas" (art. 8 / Ley de Participación de la Ciudad de México). Además, en el acuerdo por el que se aprueban los *Lineamientos* para el uso del sistema electrónico de votación, el considerando 19 también resalta de forma genérica estos factores de accesibilidad y el considerando 24 atiende de forma más específica a personas con diferentes tipos de discapacidad.

El sistema de voto electrónico promovido en Ciudad de México persigue con ahínco eliminar algunas de las críticas que se formulan de modo recurrente a estos sistemas de decisión. Destaca de modo particular el desarrollo tecnológico relativo a los procesos de autentificación del votante, tanto en la fase de registro como posteriormente a la hora de acceder al sistema de votación en sentido estricto. El Instituto ofrece una plataforma de reconocimiento biométrico que incluye, entre otros elementos, reconocimiento facial y lectura de las claves de la credencial de elector.

Se trata de un mecanismo de alta sofisticación técnica que ha logrado evitar eventuales suplantaciones y sobre todo ha conseguido aplacar críticas sobre la posible existencia de estas prácticas. Como ocurre en tantos otros aspectos del procedimiento electoral mexicano, la suspicacia, la desconfianza y lógicamente la existencia real de fraudes desemboca en sistemas de protección de gran complejidad. En nuestro caso, por ejemplo, denuncias de suplantaciones o acarreos en anteriores convocatorias motivaron, entre otros factores, una fuerte inversión en nuevos mecanismos de autenticación.

Como toda medida antifraude, tales esfuerzos deben aplaudirse, pero también es cierto que en algunos casos generan efectos colaterales quizás no tan beneficiosos. A veces, lo óptimo es enemigo de lo bueno y, en el plano informático, tal regla suele traducirse en que la mejor aplicación digital desde una óptica de seguridad puede ser realmente incompatible con su implantación práctica dado que la usabilidad iría en contra de la seguridad. Serían tantos los candados ideados y aplicados a nivel informático que el usuario se vería desorientado y en cierto momento incapaz de seguir utilizando la aplicación.

Aunque el sistema ideado por el IECM se puso en práctica sin quejas o denuncias significativas, lo cierto es que su nivel de usabilidad despierta interrogantes. Se trata de un mecanismo sofisticado que comporta el uso, entre otros elementos, de herramientas de reconocimiento facial juntamente con la necesidad de procesar la imagen y datos de la credencial de elector. Si todo ello acaba con un resultado positivo, el elector recibirá los códigos y contraseñas correspondientes. No se trata, por lo tanto, de un proceso fácil y, si incluso un usuario avezado en estas lides puede hallar trabas importantes, huelga señalar que sectores importantes de la población se revelarán incapaces de culminar con éxito todas las etapas.

El número de usuarios actuales se antoja bajo para poder extraer conclusiones definitivas al respecto ya que la cifra, a la vista del censo total, representa un porcentaje escaso, pero cabe advertir, como dato quizás más revelador, de los bajos registros de votantes reales entre aquellos que ya habían procedido a todo el proceso de pre-registro y estaban ya autorizados a emitir su sufragio de voto remoto. Se contabilizaron un total de "3,159 votos y opiniones ..., lo cual corresponde al 31.52% de participación respecto del total de ciudadanas y ciudadanos que obtuvieron la clave de votación y opinión" (: 22 / Informe III).

Tal dato no es, sin embargo, negativo. Todas las innovaciones tecnológicas necesitan un cierto recorrido temporal para ser aceptadas por los usuarios y resulta razonable, por tanto, que el voto electrónico también respete tales pautas. De hecho, en caso de habernos encontrado con una utilización masiva de esta tecnología, los riesgos no serían menores ya que entonces nos

enfrentaríamos a su posible banalización. Es mejor, en definitiva, un crecimiento sostenido y lento que tasas altísimas que reflejen un relato social frágil.

Sea como sea, convendría analizar las razones por las que la cifra final de usuarios no fue más elevada, sobre todo entre los que ya habían hecho el esfuerzo de identificarse. Puede tratarse, como advertíamos, de un ritmo normal de consolidación tecnológica, pero también podríamos hallarnos ante ciertas barreras de usabilidad que desembocarían en una escalabilidad limitada de la plataforma. En esta segunda hipótesis, el transcurso del tiempo no supondría un crecimiento sostenido del voto electrónico, sino que, una vez alcanzada una cierta tasa de participación, el mecanismo ya no podría escalar más posiciones. Todo ello sería cierto incluso en el supuesto de contar con un aplauso ciudadano generalizado. En definitiva, el sistema sería tan difícil de utilizar, es decir, tan poco usable, que acabaría disuadiendo hasta a los más convencidos.

Una vez expuestas las dos opciones, cabe preguntarse qué es lo que realmente ha sucedido en Ciudad de México. ¿Nos hallamos ante un supuesto de introducción progresiva de un sistema informático o nos enfrentamos a una aplicación cuya usabilidad limitada socava sus enormes ventajas? Los datos disponibles ahora mismo impiden alcanzar una conclusión definitiva al respecto ya que, entre otros elementos, sería necesario proceder a un análisis sociológico en profundidad que midiera el comportamiento y las reacciones de los ciudadanos, tanto a los que utilizaron la aplicación como a los que no lo hicieron y sobre todo a aquellos que, aun estando inicialmente interesados en hacerlo, acabaron desistiendo.

Tal estudio aportará información valiosísima y, partir de esta base, podrá entenderse con mayor precisión qué obstáculo debe superarse, si uno meramente social, consistente en la progresiva aceptación de una tecnología incipiente, y/o uno también tecnológico, que destaca la necesidad de conjugar adecuadamente usabilidad con seguridad. Se trata, en todo caso, de una ecuación cuyo resultado es seguramente susceptible de mejoras importantes con respecto a la situación actual.

En este sentido, debe aplaudirse la previsión ya contenida en el Estudio de viabilidad donde el propio IECM sugiere incluir indicadores sobre “la percepción ciudadana sobre el trámite electrónico de la Clave de Voto por Internet con el uso de la técnica biométrica implementada en el caso de la aplicación para dispositivos móviles” (: 56 / Estudio).

Del mismo modo, determinadas apreciaciones sustentadas hasta la fecha deben ser reconfirmadas a partir de los datos de participación obtenidos en la consulta de 2020. Se trata, por lo tanto, de proceder a una nueva validación de ciertas premisas con el apoyo de mayores instrumentos demoscópicos.

Es lo que puede ocurrir, por ejemplo, cuando el estudio de viabilidad señala, entre otras cosas, “lo fácil y dinámico que resulta el uso del SEI, ya que es similar al que actualmente utiliza la mayor parte de la ciudadanía en otros sistemas de internet que ofrecen diversos servicios, como la banca en línea, el procesamiento de compras o comercio electrónico y la realización de trámites ante diversas instancias, entre otros” (: 29 / Estudio). En el mismo sentido, el Comité Técnico creado en 2019 precisaba que “la aplicación desarrollada por el Instituto Electoral es un facilitador confiable y de uso intuitivo para que la ciudadanía cumpla los propósitos de identificación para la emisión de su voto/opinión” (: 33 / Opinión). Finalmente, el Tribunal Electoral del Distrito Federal también destacó en su momento que el voto electrónico se lleva a cabo “a través de la utilización de un mecanismo que en la actualidad se considera de fácil uso para todos los ciudadanos, como es el acceso a una computadora con conexión a Internet” (TEDF-JEL-017/2013; tomado de : 20 / Estudio).

Todas estas apreciaciones son excesivamente generales y necesitan ser corroboradas o matizadas con estudios sociológicos detallados que midan el grado de aceptación tanto de los instrumentos digitales en general como sobre todo de la aplicación de voto electrónico en particular. El hecho, por ejemplo, de que la ciudadanía esté habituada al uso de Internet para ciertos servicios públicos o privados no implica que acepte tales herramientas en mecanismos de participación ciudadana. Del mismo modo, afirmar que todos los ciudadanos tienen fácil acceso a una computadora con conexión a Internet puede hacernos olvidar que el analfabetismo digital, sea total o funcional, sigue presente en determinadas capas de la población, que pueden tener además dificultades económicas para acceder a estos canales. Finalmente, el uso intuitivo que se atribuye al mecanismo de votación por Internet contrasta con el hecho de que, durante la jornada del día 15 de marzo, siguió existiendo un grado elevado de asistencia a los votantes.

Es por todo ello que un estudio sociológico sobre la aceptación y uso real del voto por Internet permitirá afinar sus desarrollos futuros haciendo especial hincapié en las barreras de usabilidad y escalabilidad que puedan presentarse. Puede alcanzarse así un uso más extendido e incluso mayoritario de esta herramienta.

Finalizamos esta sección con una apelación a las labores de formación del votante ya que una planificación sistemática y a largo plazo en esta dirección permitirá contar con una imagen mucho más fidedigna de la percepción ciudadana sobre el voto electrónico. Se conseguirá asimismo detectar con anticipación deficiencias en usabilidad y se aumentará, en consecuencia, la escalabilidad del sistema.

Se trata de un campo en el que el IECM puede dedicar más recursos. Más allá de campañas de sensibilización ciudadana a través de medios de comunicación o redes sociales, conviene que los propios votantes conozcan de primera mano los dispositivos informáticos y puedan interactuar con ellos en sesiones simuladas. Las actividades registradas en estos ámbitos para la consulta de marzo de 2020 son susceptibles de incrementarse considerablemente en futuras ocasiones. En este sentido, resulta llamativo que, en la distribución de tabletas a utilizar durante la jornada del 15 de marzo, solamente ocho de un total de 239 se destinaran a “simulacros y capacitaciones” (: 10 / Informe III).

J) Diseño de la boleta y del proceso de votación

La documentación electoral fue aprobada por el IECM el mismo día de la convocatoria por acuerdo IECM/ ACU-CG-082/2019 y, en lo relativo al sistema electrónico por Internet, se validan los modelos de boletas virtuales. Se trata de un elemento al que hay que conceder la importancia que merece ya que un diseño deficiente puede arruinar todo un proceso.

Interesa llamar la atención sobre dos aspectos del proceso de votación. En primer lugar, la votación en casilla de cada ciudadano arranca con la entrega de la credencial de elector a la persona responsable de la casilla, quien será la encargada de validar la identidad del votante ante el dispositivo informático habilitado al efecto. Es lo que se señala, por ejemplo, en el *Manual para el uso del Sistema Electrónico por Internet (SEI) en Mesas Receptoras de Votación y Opinión (MRVyO)* (: 4-6), pero contrasta con lo previsto en la *Guía para la implantación*, donde se preveía que, “en caso de ser necesario y a solicitud de la persona votante, las personas responsables de la Mesa podrán brindarle apoyo para acceder al SEI” (: 38 / Guía).

Se trata de un dato importante ya que permite medir el grado de autonomía a disposición del votante en el proceso de elección. Del mismo modo, no es aconsejable que la persona responsable manipule su credencial y lo haga en una cabina de votación que impida al votante observar realmente lo que está ocurriendo. No puede equipararse, en este sentido, la votación

tradicional, en la que la credencial se manipula siempre a la vista del propio elector, con lo que sucede en este caso.

Igualmente, tampoco resulta aconsejable que las personas responsables de casilla deban adentrarse en la cabina para cada votante que acuda a la casilla. Pueden despertarse legítimas suspicacias. Adviértase, en este sentido, que, de acuerdo con lo establecido en el *Manual*, la persona responsable de la casilla abandona la cabina cuando la pantalla ya muestra la boleta que deberá rellenar el elector. Nada impide, por lo tanto, que la persona responsable de casilla marque una determinada opción en la pantalla y que tal acción predetermine de alguna forma la actuación del elector. Puede suceder asimismo, como ya se recordó al inicio del informe, que la persona responsable de la casilla añada trabas inexistentes en el proceso de identificación del votante ante el dispositivo informático.

Todo ello se halla además vinculado a lo señalado en la sección anterior sobre la usabilidad y correspondiente escalabilidad del sistema. Ni el intervencionismo del personal responsable de casilla ni porcentajes bajos de utilización como los registrados en el voto remoto ayudan a plantear un tránsito cómodo entre voto tradicional y sufragio electrónico, al menos si concebimos el segundo con una dimensión mayor que la actual. El proceso se antoja ahora mismo demasiado complejo y deberían buscarse, por lo tanto, vías de simplificación.

Por otro lado, la comparación entre el *Manual* y la *Guía* permite identificar otra discrepancia en lo relativo a la finalización de la sesión de votación. Mientras que la *Guía* señala que, "al presionar 'Salir del Sistema', se cerrará la sesión y de esa forma se concluirá el registro" (: 34 y 39 / Guía, para voto remoto y en casilla respectivamente), el *Manual* de voto en casilla prevé que "la aplicación emitirá un sonido que indicará que el proceso finalizó [y] [l]a aplicación se redirigirá a la pantalla inicial de **Votación**" (: 6 / Manual).

Se trata de nuevo de un dato aparentemente inocuo, pero que puede comportar en realidad graves problemas. Si atendemos, por ejemplo, a lo ocurrido hace unos años en Finlandia, comprobaremos como cada paso del proceso es relevante dado que las elecciones municipales en ciertas localidades tuvieron que repetirse debido a que algunos votantes creyeron haber culminado el proceso de votación cuando realizaron la primera selección de candidaturas. El diseño de la pantalla no era lo suficientemente claro como para indicarles que debían también confirmar y votar. Como resultado de estos fallos, tales electores no quedaron registrados en la urna y el escrutinio electrónico arrojó menos sufragios que el número de votantes anotados por los responsables de casilla.

Ciertamente, nuestro caso no es equiparable ya que la discrepancia sobre la última pantalla no impide que el elector ya haya confirmado sus opciones, haya emitido su sufragio e incluso se le haya enviado un mensaje de agradecimiento. Sea como sea, resulta aconsejable seguir lo indicado en el *Manual* y proceder a una transición automática hacia una nueva sesión de votación.

Adviértase, en este sentido, que no resulta claro qué sucede cuando el elector abandona la casilla sin apretar el botón final de salida de la aplicación y sobre todo si en este caso el siguiente usuario, sea la persona responsable de la casilla u otro votante, puede regresar a pantallas anteriores y visualizar o incluso alterar el sufragio del elector precedente.

K) Capacitación, simulacros y logística

Las reflexiones realizadas tanto sobre la normatividad como sobre la auditoría ya han hecho hincapié en las limitaciones temporales con las que se impulsaron las consultas a celebrar en marzo de 2020. También se indicó que, entre otras razones, el retraso en la aprobación de

regulaciones más genéricas sobre participación ciudadana impidió disponer de más tiempo para la preparación de la consulta.

Sea como sea, conviene llamar la atención sobre las consecuencias que esta premura haya podido tener en el desarrollo de las jornadas de votación. Como se analizará más adelante, tanto el voto remoto como sobre todo la jornada del 15 de marzo se vieron afectadas por ciertos contratiempos que, aunque no lograron anular por completo la votación, tuvieron un impacto nada desdeñable. Sin perjuicio de los comentarios sobre cada contratiempo, interesa ahora destacar que un planteamiento mejorado, y seguramente más holgado en el tiempo, en las tareas de capacitación, planeamiento y ejecución de simulacros y logística en general hubiera logrado detectar y subsanar a tiempo los problemas que después se presentaron.

En relación con los simulacros, conviene preverlos a carga real, desde los lugares en los que se utilizarán los dispositivos y con la participación de todo el personal que estará cargo de la votación durante la jornada electoral. En realidad, sin embargo, los tres simulacros llevados a cabo no cumplían tales requisitos. Se realizaron desde las oficinas centrales del IECM o desde la sede de los órganos desconcentrados, pero no desde la ubicación de las casillas. Además, en el segundo caso, el simulacro no replicaba las condiciones reales que se darían en la jornada electoral ya que, "debido a que los Órganos Desconcentrados no contaban con el personal suficiente para la realización de la prueba simultánea, ésta se realizó de forma escalonada sin permitir conocer el volumen de transacciones real para el día de la Jornada" (: 14 / Informe III).

Existen igualmente otros datos que reflejan la necesidad de fortalecer la programación tanto de simulacros como de capacitaciones. Así se expone, por ejemplo, en el mismo Informe cuando, a raíz del simulacro del 6 de marzo, se observa la necesidad de reforzar la capacitación y significativamente debe realizarse por videoconferencia (: 14 / Informe III), lo que refleja una capacidad institucional de reacción insuficiente para cubrir las necesidades de todo el territorio en lo referido a la implantación del Sistema Electrónico por Internet.

Del mismo modo, si el simulacro realizado desde los Órganos Desconcentrados ya detectó problemas de conexión "por mala recepción" (: 14 / Informe III), fallos parecidos podrían ocurrir en las ubicaciones reales de las casillas y hubiera sido recomendable un simulacro desde ellas.

En relación con la logística de distribución de materiales en la jornada del 15 de marzo, el IECM previó un plan de contingencia en el caso de falla en el sistema electrónico y tal planteamiento funcionó de forma razonable, aunque la magnitud del problema, con la práctica totalidad de casillas paralizadas, impidió que la reacción tuviera la agilidad que hubiera sido deseable. Se encuentra buena prueba del reto planteado en el hecho de que, pese a que existía una reserva de contingencia de un 5% de boletas (: 11 / Informe IV), tuvo que pedirse material suplementario a las demarcaciones en las que no había voto electrónico.

El informe elaborado por el IECM cifra en una hora el promedio de tiempo requerido para hacer llegar las boletas en papel a las casillas problemáticas, lo que se antoja como un valor muy positivo a la vista de los retos a superar en las horas más críticas del 15 de marzo, pero tal resultado no puede ocultar algunos pocos casos en los que las casillas esperaron más de dos horas (: 16 / Informe III). La habilitación de mayores vehículos de apoyo o la identificación de ciertas casillas como sub-centros de recogida podría haber facilitado la labor en circunstancias tan extremas. En este segundo supuesto, el responsable del reparto no se vería obligado a ir casilla por casilla, sino que depositaría en ciertas casillas estratégicamente ubicadas la documentación tanto para esa casilla en particular como para otras cercanas, cuya documentación sería recogida, con la adecuada supervisión, por las personas responsables de cada una de ellas.

Llaman la atención asimismo supuestos en los que se inicia la votación en papel pasadas las cuatro de la tarde pese a haber recibido las boletas bastante antes (: 22 / Informe III). Se desconocen las causas de este fenómeno, aunque quizás obedezcan a intentos repetidos, y finalmente vanos, de reactivar el voto electrónico, algo que pudo lograrse en ciertas casillas, pero no en todas.

L) Apoyo a redes de observaciones electorales

El IECM demuestra tener voluntad de apertura al incorporar actores externos en calidad de observadores. Entre otros momentos, la apertura y configuración del sistema prevé la presencia de "representantes de los partidos políticos, candidatos sin partido y en su caso, personas observadoras de la Sociedad Civil" (art. 25 / Lineamientos). Se trata de una medida positiva, pero, como en tantos otros casos relativos al voto electrónico, la mera presencia de observadores puede carecer de sentido si lo que se contempla, dada su complejidad técnica, realmente no puede verificarse.

Es lo que sucede, por ejemplo, cuando se alude a inicialización en cero del sistema o a otros aspectos técnicos similares (art. 26 / Lineamientos). Celebrar una sesión solemne en la que se emitan certificados de este tipo no supone valor añadido alguno a los mecanismos de seguridad ya que tanto la pantalla en la que se observa el contador a cero como los certificados en papel pueden no corresponder a lo que realmente está sucediendo a nivel técnico en el seno de las computadoras.

No se trata, en todo caso, de suprimir tales actos, pero sería conveniente informar sobre su alcance real a nivel de supervisión. No hacerlo transmite un mensaje engañoso a la opinión pública y puede llegar a ser un riesgo ya que se abre un flanco para críticas fundamentadas sobre la verdadera razón de ser de estas presentaciones públicas.

Entre los mecanismos que se prevén en los Lineamientos y que pueden cumplir esta labor suplementaria, merece destacarse la apertura prevista de los "módulos para el monitoreo del estado de operación" (art. 31) del sistema, que se hallan a disposición de representantes de partidos, candidatos y observadores (art. 32).

M) Oportunidades

Culminamos esta sección del informe con una referencia a las oportunidades que el voto electrónico ofrece al IECM a corto y medio plazo. Como anticipábamos al inicio, el Instituto cuenta con una dilatada trayectoria en lo relativo al uso del sistema de voto electrónico. El esfuerzo aplicado durante estos años ha logrado implantar una herramienta apta para mejorar los mecanismos de participación ciudadana y para ello conviene explotar al máximo su potencialidad. Además de atender a los diversos aspectos que se han ido resaltando a lo largo del texto, algo indispensable para que el sistema pueda crecer en confianza técnica y ciudadana, el IECM puede explorar otros caminos que hasta ahora han sido poco trabajados. Existen, en este sentido, tres áreas donde podrían producirse claros avances:

a) Diálogo institucional permanente con otros casos de voto por Internet activos como, por ejemplo, Estonia, Panamá, Armenia o Canadá. Asimismo, debe prestarse atención a países pioneros en este ámbito como Francia y Suiza. El IECM se halla en una posición privilegiada para impulsar un punto de encuentro de experiencias que hoy por hoy se están desarrollando sin demasiadas conexiones entre sí. Se trata de países que afrontan problemas similares y sería muy útil contar con un intercambio permanente de buenas prácticas.
b) La documentación generada por el IECM hasta la fecha trata con solvencia diversos aspectos relativos a la implantación del voto electrónico, pero existen ciertos elementos

que podrían desarrollarse con mayor profundidad. Uno de ellos consiste en la relación entre voto electrónico e igualdad y, de forma más concreta, la forma en la que debe superarse la brecha digital en los casos de mecanismos digitales de participación ciudadana. Existen aquí múltiples flancos en los que profundizar, pero todos ellos pueden reconducirse a procurar un mayor énfasis en análisis de ciencias sociales, sean legales o politológicos.

c) El IECM cuenta con una potente infraestructura tecnológica que utiliza de forma recurrente para consultas locales y aspira a recibir autorización para reimplantar el voto electrónico en las elecciones oficiales. Existe, sin embargo, un campo en el que el voto electrónico podría contar con más desarrollo y cuya aplicación no ha sido todavía explotada con total intensidad. Nos referimos a los procedimientos de decisión internos en otras instituciones, públicas o privadas, que puedan valorar positivamente la utilidad del voto electrónico. Otros países han avanzado bastante en esta línea destacando la admisión de mecanismos electrónicos de votación por partidos políticos, organizaciones civiles de gran tamaño, universidades o colegios profesionales.

IV – Incidentes del sistema durante la jornada electoral

Se expone a continuación una valoración preliminar del desarrollo a nivel técnico de las dos etapas de votación, es decir, la desarrollada entre el 8 y el 12 de marzo, por un lado, y la del domingo 15 de marzo por otro. Los hallazgos, conclusiones y recomendaciones de este apartado necesitan, en todo caso, una auditoría forense completa para poder ser confirmados.

En relación con la votación remota del 8 al 12 de marzo, cabe destacar, como primer hallazgo, un *error en plataforma Android*. Se presentó un error en la aplicación para sistema operativo Android desde el momento en que se inició el período de recepción de votos. Se impedía la votación ya que, al desplegar la boleta, de inmediato se redirigía a la pantalla principal de la aplicación. A pesar de que se solucionó en las primeras horas del día 8 de marzo, y se dio seguimiento a los votantes que informaron que no podían enviar su sufragio, es probable que este error de disponibilidad haya impedido ejercer el voto a otros ciudadanos que simplemente optaron por no volver a intentarlo. Este tipo de fallos, que impactan directamente en el uso del sistema de votación, minan la confianza de los ciudadanos.

El error pone de manifiesto deficiencias en las pruebas de caja negra, tanto internamente en el IECM como las que llevó a cabo el ente auditor. Llama la atención, en este sentido, que el Comité Técnico creado en 2019 hubiera comprobado la funcionalidad de pre-registro en ambos sistemas operativos (: 18 / Opinión), pero que esta prueba no se llevara a cabo posteriormente de manera correcta para la votación. El informe posterior de la entidad auditora deja constancia del error y de los pasos realizados para subsanarlo, pero no valora la suficiencia de la propia auditoría realizada previamente.

Cabe señalar igualmente que la reparación se llevó a cabo “en presencia del Ente auditor” (: 20 / Informe III) y que, según su informe, “se resolvió realizando unos ajustes en el código” [: 5 / Informe I]. Sin perjuicio de considerar la intervención como técnicamente razonable para poder salvar el escollo planteado por el sistema operativo Android, interesa destacar que se modifica un código que había sido previamente cifrado y sellado para así evitar manipulaciones posteriores. Sería deseable, en este sentido, que cualquier ajuste en el código condujera a la repetición de las mismas garantías que se habían dispuesto para garantizar la integridad del código. La mera presencia del Ente auditor, tal y como se recoge en el informe aludido, se estima insuficiente. Los informes no llegan a precisar, sin embargo, si se realizó un nuevo cifrado.

Por otro lado, en relación con la jornada electoral del 15 de marzo, cabe aludir a un *error de conectividad tableta – servidor*, según información recibida de diversas mesas electorales. Los

Responsables de Mesa iniciaban el proceso de autenticación, mas muchos no lograban respuesta del servidor. Otros sí lograron realizar la autenticación, pero a partir de allí la respuesta del servidor era intermitente. Al descartar que se tratara de una falla de internet generalizada, personal de redes del IECM detectó un problema de respuesta del servidor debido a la cantidad de conexiones simultáneas.

Este error tuvo como consecuencia directa la privación del ejercicio del voto para muchos ciudadanos ya que, si bien algunos probablemente regresaron a votar más tarde, otros ya no lo hicieron. Tanto la reputación del sistema y/o del IECM como la desconfianza que todo ello genera para futuros procesos debe ser tenida en cuenta.

Este error presenta una disparidad importante con las pruebas de denegación de servicio realizadas durante la auditoría, donde se generó, según el informe, un pico de tráfico de hasta 21.62 Gbps ocasionado por peticiones legítimas al servidor (: 19 / Informe II). Dicha cantidad de tráfico sería el equivalente a recibir en un segundo alrededor de 2,500 peticiones simultáneas de conexión, asumiendo un tamaño del paquete de conexión de 10 Megabytes, lo que es bastante grande para los datos que se envían en una autenticación. Las solicitudes de conexión al servidor el día de la elección fueron mucho menos que las 2,500 por segundo del escenario de pruebas.

Todo ello nos lleva a dos posibles causas de la no disponibilidad del sistema:

- Pruebas de conectividad deficientes en la auditoría, al no contemplar la realidad del tráfico hacia el servidor que se generaría al inicio de la elección. El informe del IECM afirmaba, como conclusión de los simulacros llevados a cabo, que “la infraestructura web que presta servicio al sistema SEI cuenta con una configuración de balanceo de cargas y una arquitectura de protección de 3 niveles que permite el buen funcionamiento a pesar de un ataque DDoS de alto volumen. La infraestructura SEI no requiere mejoras adicionales por lo cual se recomienda mantener estas políticas de implementación para futuros sistemas” (: 16 / Informe III). Se trataba de una conclusión que se reveló falsa durante la jornada de votación.
- Una modificación en la configuración del servidor o dispositivos de red, respecto a la que se tenía durante la auditoría.

Por otro lado, se detectó un *error de inicio de aplicación*. De acuerdo con la información recibida del IECM y a raíz de las propias observaciones de los autores, otro de los incidentes presentados el día 15 de marzo en que, cuando los responsables de la mesa abrieron la aplicación de votación en la tableta, en lugar de aparecer la pantalla inicial de la aplicación, se mostraba la pantalla de “cómputo de votos”, que solo debería aparecer una vez que se ha cerrado el módulo de votación. Según el informe del IECM, hubo solamente dos supuestos de este tipo (: 25 / Informe III).

Todo indica que la razón de esta incidencia fue que el día anterior se había llevado a cabo un simulacro en el cual se había realizado todo el proceso hasta llegar a la opción de cómputo de votos. La aplicación se abrió al día siguiente precisamente en donde se había dejado el día anterior. A pesar de que este problema tenia fácil remedio ya que, al tocar una parte de la pantalla, la aplicación volvía a la pantalla inicial, lo cierto es que causó demoras y desorientación en los operadores.

Este tipo de errores se atribuye a una o más de las siguientes causas:

- Al diseño de la aplicación, en este caso específico al no contemplar esta posibilidad en el flujo de la aplicación al pasar de un estado de simulacro al estado del escenario real.

- Al diseño del simulacro, al no contemplar llevar la aplicación al estado inicial después de haber recorrido todo el proceso.
- A las instrucciones dadas a los operadores durante el simulacro, al no indicarles apropiadamente cómo regresar la aplicación a la pantalla inicial.
- A la verificación del estado de la aplicación al concluir el simulacro o bien, durante la mañana del día 15 de marzo, con suficiente tiempo antes de empezar a operar la mesa electoral. En las casillas observadas no hubo, en este sentido, prueba de funcionamiento previa al inicio de la votación, lo que sería un elemento de fácil subsanación en futuros usos del voto electrónico.

Como complemento a este diagnóstico técnico, debe señalarse que el IECM articuló un sistema adecuado de seguimiento de las incidencias y es por ello que los informes posteriores pueden dar cuenta de lo que ocurrió de forma pormenorizada y segmentada. Sea como sea, en ciertos casos las observaciones de incidentes reflejadas en el informe final son demasiado genéricas e impiden valoraciones subsiguientes. Es lo que sucede, por ejemplo, en el Distrito 9 (: 7-13 / Reporte), donde se señala únicamente que hubo errores que no pudieron subsanarse, o también en el Distrito 12 (: 14-18 / Reporte).

Cabe mencionar asimismo la disparidad de situaciones que se produjeron en las zonas elegidas para utilizar el voto electrónico. Mientras que ciertas casillas parecen no haber tenido problema alguno con esta herramienta, singularmente en el Distrito 12 (: 19 / Informe IV), otras son clausuradas por la presión de los propios ciudadanos al comprobar que el sistema propuesto no funcionaba (: 18 / Reporte). Mientras que el Distrito 5 no comunica ninguna problemática (: 12 / Informe IV), ciertas casillas consiguen revertir la falla inicial y activar el voto electrónico. En su conjunto, resulta ilustrativo revisar la recopilación de casos aportada por el informe del IECM ya que así se capta con mayor facilidad la pluralidad de situaciones y entornos con los que tuvieron que lidiar los gestores del Instituto durante la jornada electoral.

V – REFERENCIAS

Estudio / *Estudio de viabilidad técnica, operativa y financiera para proponer el uso del SEI, como una modalidad adicional para recabar votos y opiniones en la Elección y la Consulta*

Guía / *Guía para la implementación del Sistema Electrónico por Internet en la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021*

Informe I / *Informe de Evaluación de la Auditoría Informática (informe posterior a la jornada). Período de evaluación: Del 15 al 17 de marzo de 2020*

Informe II / *Informe final de la Auditoría de Software previo a la jornada de votación y opinión. Período de evaluación: Del 24 de febrero al 30 de marzo de 2020*

Informe III / Informe sobre la operación de sistema electrónico por internet del Instituto Electoral de Ciudad de México, 9 de abril de 2020, Versión 2

Informe IV / Informe sobre las actividades realizadas por la Dirección Ejecutiva de Organización Electoral y Geoestadística, y la Unidad Técnica de Archivo, Logística y Apoyo a Órganos Desconcentrados durante la jornada única de la elección de comisiones de participación comunitaria 2020 y la consulta de presupuesto participativo 2020 y 2021, del 15 de marzo de 2020.

Lineamientos / Lineamientos Generales del Sistema Electrónico por Internet

Manual / Manual para el uso del Sistema Electrónico por Internet (SEI) en Mesas Receptoras de Votación y Opinión (MRVyO)

Opinión / *Opinión del Comité Técnico sobre el estado actual del Sistema Electrónico por Internet y recomendación de su utilización en la Elección de Comités Ciudadanos y Consejos de los Pueblos 2019 y la Consulta Ciudadana sobre Presupuesto Participativo 2020*

Reporte / *Reporte concentrado de incidentes (MRVyO)*