ARTÍCULO

ISSN 1994-5272

Metodología para la identificación de riesgos en sistemas de votación electrónica

Ana Gómez Oliva
<agomez@diatel.upm.es>
Universidad Politécnica de Madrid

Emilia Pérez Belleboni
<belleboni@dialtel.upm.es>
Universidad Politécnica de Madrid

[Resumen] En la actualidad, no existen parámetros de medida que permitan evaluar la bondad de un sistema de votación electrónica. Este artículo busca dar respuesta a esta necesidad, especificando un conjunto de elementos y criterios que brinden, por una parte, la posibilidad de evaluar la idoneidad de sistemas automatizados de votación, y, por otra, realizar comparaciones entre diversos sistemas. Para ello se ha partido de la propia experiencia, del análisis de la información publicada por los autores y promotores de otros sistemas de votación, así como de las opiniones manifestadas en distintos foros en los que los potenciales votantes han reflejado sus esperanzas, reticencias y temores. El resultado es la presentación organizada de características que permite identificar riesgos y evaluar funcionalidades en estos sistemas de votación.

[Palabras clave] Votación electrónica, identificación de riesgos, criterios de comparación, verificabilidad, clasificación de sistemas de votación

[Title] Methodology for identifying risks in electronic voting systems

[Abstract] There are currently no measurement parameters to evaluate the benefits of an electronic voting system. This paper aims to address this need by specifying a set of elements and criteria achieving two goals: To assess the suitability of automated voting systems and to make comparisons among systems. Proposed criteria area based on the own expertise, along with the deep study of the information offered by authors and sponsors of a number of voting systems as well as the expressed opinions in forums where potential voters state their hopes, fears and reluctance to achieve this target. The result is the presentation of a body of characteristics to identify risks in electronic voting systems.

[Keywords] Electronic voting, risks identification, comparison criteria, verifiability, rating voting systems

Gómez, Ana y Emilia Pérez Belleboni. «Metodología para la identificación de riesgos en sistemas de votación electrónica». En: *Elecciones*, 2014, enero-diciembre, vol. 13, N.º 14, pp. 49-74

[Recibido] 07/09/14 & [Aceptado] 12/11/14

Introducción

Desde hace varios años, los sistemas de votación electrónica han dejado de ser experiencias piloto, no vinculantes, para convertirse en una realidad. Son actualmente numerosos los países, que en mayor o menor medida, han ido automatizando sus procesos electorales para aprovechar las ventajas que brindan las TIC.

No obstante, los resultados obtenidos hasta la fecha indican que un sector importante de la población se muestra receloso y, a menudo, cuestiona la validez de los resultados obtenidos en esta modalidad de votación. Los motivos de estos temores se pueden encontrar en la desconfianza que puede inspirar un nuevo sistema cuyo funcionamiento se desconoce, en el que la ausencia de pruebas físicas tangibles, como las proporcionadas por las papeletas tradicionales, produce en los votantes una sensación de vulnerabilidad ante una posible alteración de los resultados. Con todo, no es este el único temor al que deben enfrentarse los sistemas de votación electrónica. Otra de las dudas más frecuentemente referidas por los votantes afecta a la percepción que tienen sobre la posibilidad, real o no, de que su voto no sea secreto. Mientras que en la votación tradicional aceptamos que, desde el momento en que introducimos el sobre con el voto en la urna nadie puede volver a relacionarnos con él, en las experiencias de votación electrónica antes referidas se puede dudar de si después de identificarnos y emitir el voto queda un rastro que permita determinar cuál es la opción por la que nos hemos decantado.

Como suele ocurrir en el desarrollo de nuevas ideas, en los inicios se carece de parámetros de medida que permitan comparar las distintas soluciones que se plantean con el fin de evaluar ventajas y carencias de cada una. Este artículo busca dar respuesta a esta necesidad, identificando un conjunto de parámetros de medida, que permitan a los responsables de la puesta en marcha de futuros sistemas de votación electrónica discernir qué tipo de sistema es el que mejor se adapta a sus necesidades, con pleno conocimiento del alcance de sus decisiones.

Los criterios y elementos por evaluar han surgido fundamentalmente del convencimiento de que para que merezca la pena afrontar el esfuerzo de cambiar un sistema de votación tradicional por otro electrónico es necesario asegurarse de que el cambio ofrece ventajas sustanciales y disminuye los riesgos,

teniendo siempre en consideración las amenazas que se ciernen tanto sobre los datos y equipos como sobre las personas.

1. Sistemas de votación electrónica: requisitos funcionales y de seguridad

Uno de los aspectos que resulta preciso tener en cuenta antes de hacer una propuesta de evaluación válida es saber qué tipo de modelo de sistema de votación tradicional se tomará como referencia. Los modelos electorales están diseñados conforme con la idiosincrasia de cada país. Así, hay países, como España, donde se enfatiza en la adecuada identificación de los votantes mediante la presentación de un documento oficial en el momento de la votación, mientras que en otros países, como el Reino Unido, los votantes acreditan su identidad sobre la base de la confianza mutua y conocimiento de los vecinos que acuden al colegio electoral.

Los procesos electorales están estrechamente ligados a la idiosincrasia e historia de los pueblos que los utilizan. Muestra de ello es que ciertas características que para algunos resultan irrenunciables, se consideran poco relevantes, innecesarias e incluso peligrosas para otros. En <http://aceproject.org>, se encuentra, entre otra información, enlaces a legislaciones electorales, publicados por instituciones oficiales de distintos países, a partir de los cuales se puede deducir que existen argumentos a favor y en contra para considerar ciertos aspectos de los procedimientos como signos claros de la limpieza del proceso, como ocurre, por ejemplo, con la imposición de urna transparente o no. Con todo, hay algunos principios que parecen ser universalmente aceptados, aunque la forma y el grado en el que alcanzan sus objetivos pueden diferenciarse mucho de una organización social a otra. Como resultado, existe un amplio rango de soluciones sobre la forma en que los sistemas electorales, ya sean tradicionales o electrónicos, velan por la calidad del proceso de votación aunque no puedan ofrecer seguridad total.

Por poner ejemplos significativos, podemos destacar que, mientras algunas sociedades entienden que el voto debe ser una obligación, para ofrecer con ello una forma de proteger al ciudadano ante coacciones que le impidan ejercer el derecho, otras sociedades consideran que el ciudadano es libre de abstenerse o votar y no se considera necesario ofrecer control sobre la posibilidad de que el

votante sea impedido de ejercer su derecho a voto. Cuando se establece que es un deber, la penalización por el incumplimiento de la obligación de emitir el voto puede ser tan relajada que se aproxime al reconocimiento del voto como derecho y no como obligación o, por el contrario, puede conllevar a la pérdida de muchos derechos básicos como ciudadanos.

Si bien para unos el voto debe, obligatoriamente, ser marcado en el interior de una cabina e incluso consideran delito penalizado seriamente que el propio votante encuentre formas de probar fehacientemente ante terceros cuál ha sido su opción, para otros el uso de la cabina es una opción tan válida como cualquier otra. Mientras que algunas legislaciones entienden que el voto solo se puede emitir en colegios electorales constituidos especialmente a tal efecto, otras permiten que los buzones, las oficinas de correo u otras entidades asuman la responsabilidad de ser receptores y en consecuencia custodios de los votos.

La combinación con mayor o menor grado de complejidad de los factores como los que se acaban de enunciar, y de otros muchos, busca fundamentalmente ofrecer mecanismos para garantizar que el recuento refleje de manera fiel la voluntad de los votantes que ha sido manifestada libremente. Lo expuesto anteriormente demuestra que la extracción de valores que pudieran considerarse de validez universal para los sistemas de votación es una tarea ardua y proporciona resultados que deben ser sometidos a numerosas matizaciones. Además, la enorme variedad de enfoques planteados por los diversos sistemas de voto propuestos genera una gran dificultad, incluso imposibilidad, de efectuar una comparación nítida.

Por todo ello, antes de pasar a presentar los parámetros de evaluación de los sistemas de votación, seguidamente se recogen algunos conceptos básicos ligados a los sistemas de votación electrónica, proponiendo una clasificación de sus distintos tipos y detallando la problemática específica de seguridad que conlleva su puesta en marcha, junto con las soluciones comúnmente adoptadas para algunos de los problemas planteados.

Según la definición del Consejo de Europa (Directorate of Democratic Institutions, 2010) «voto electrónico» es aquel donde al menos el voto es emitido por medios electrónicos. Esta definición, demasiado amplia, requiere ser matizada para situar el presente estudio, ya que a partir de los procesos que

se automatizan afloran diversas dimensiones sociales y tecnológicas, que será necesario abordar en la definición de parámetros que se proponga.

En función de las tareas automatizadas resulta útil establecer una clasificación de los sistemas de votación en tres niveles como se indica a continuación:

En un nivel básico de automatización de los procesos electorales, consideraremos la automatización de parte del proceso manteniendo el voto mediante papeletas. Incluye la utilización de herramientas informáticas y telemáticas para agilizar tareas necesarias, pero complementarias de un proceso de votación, como el registro de votantes, la generación y publicación del censo electoral, la impresión de las actas de constitución de mesas y actas de recuento final de votos, la impresión de justificantes, la transmisión de resultados de votación, etcétera.

La simpleza de estos sistemas si son comparados con los del siguiente nivel no puede ser una invitación a bajar la guardia puesto que es posible obtener pingües beneficios con ataques adecuados como pueden ser la alteración del censo electoral, el levantamiento de actas con resultados distintos de los obtenidos o el ataque a la transmisión de la información (Carracedo Gallardo, 2004).

En el nivel intermedio consideramos la automatización del proceso de emisión del voto por parte de un votante previamente identificado y autenticado por mecanismos complementarios al del voto. Se incluye también, en este nivel el recuento de votos, la generación de actas y, si procede, la publicación de resultados. En este caso se dispone de máquinas electrónicas ante las cuales se realiza el acto de depositar el voto mediante un procedimiento electrónico. Estos sistemas informáticos, que sustituyen a las antiguas urnas de los procedimientos tradicionales en las que se introducen las papeletas, capturan y almacenan el voto de forma electrónica, en algunos casos generan algún tipo de comprobante, finalmente realizan automáticamente el escrutinio y emiten el acta correspondiente al terminar la votación. Todos y cada uno de los pasos son susceptibles de ser atacados o sufrir accidentalmente problemas que provoquen un mal funcionamiento. Los países que han implementado en todo su territorio el voto electrónico con bastante éxito de crítica (Consejo Nacional Electoral venezolano 2012, Tribunal Superior Eleitoral 2013) disponen ade-

más de redes de comunicación para transmitir de forma segura los resultados del recuento realizado en las distintas urnas electrónicas ubicadas en cada uno de los colegios electorales.

En el nivel avanzado, la votación se lleva a cabo mediante el uso de redes telemáticas y agentes telemáticos específicos, de tal forma que, tanto la autorización para votar tras la exitosa identificación electrónica y autenticación del votante como el voto, son transmitidos por la red con profusas medidas de seguridad. La experiencia por excelencia de este caso es la que se realiza en Estonia (Estonian National Electoral Committee, 2013).

1.1. Requisitos funcionales y de seguridad

Los requisitos funcionales y de seguridad que deben reunir los sistemas de votación electrónica se han determinado habitualmente reproduciendo las garantías proporcionadas por el voto tradicional, por lo que fundamentalmente se ha centrado en la protección del anonimato del votante, en impedir el voto no autorizado, en lograr que se cumpla el principio de «un votante un voto» y en asegurar el recuento correcto de los votos. Además, puesto que se usarán recursos informáticos, estos esquemas de votación incluyen procedimientos criptográficos que minimizan la probabilidad de que el voto emitido por el votante pueda ser alterado o examinado durante su transmisión o almacenamiento.

Una dificultad que presenta el diseño adecuado de un sistema de votación es que, entre los requisitos, se presentan exigencias que son, en principio, opuestas:

- El sistema debe garantizar que solo las personas con derecho a voto pueden emitir un voto, a la vez que debe garantizar que es imposible relacionar a esta persona, fehacientemente identificada, con el voto que ha emitido. Es decir, hay que combinar (aunque en fases distintas) dos servicios de seguridad habitualmente contrapuestos: autenticación y anonimato.
- El sistema de votación electrónica debería aportar, como valor añadido, mecanismos para que los votantes verifiquen el tratamiento que se le ha dado a su voto, pero que con ello no le exponga a la coacción y venta de votos.

1.2. Amenazas que surgen por el uso de redes y sistemas informáticos

Las amenazas que se ciernen sobre un sistema de votación habitualmente se orientan a quebrantar las garantías que este debe ofrecer. La forma de materializar las amenazas en ataques, su probabilidad de éxito, y la recompensa que puede obtener un atacante son propias de cada sistema usado. En el caso de votación electrónica, los sistemas que lo componen deben enfrentarse a amenazas específicas originadas, por una parte, por la utilización de sistemas informáticos para emitir y recibir el voto, ejecutar los procedimientos de recuento, etcétera, y, por otra, por el hecho de emplear redes de comunicación necesarias para interconectar los dispositivos que forman parte del sistema de votación (puntos de identificación de votantes, puntos de emisión de voto, urna remota, etcétera). Por tanto, el sistema deberá abordar medidas para protegerse fundamentalmente de los siguientes ataques:

1. Ataques sobre la información, haciendo factible que un atacante pudiera modificar o eliminar los votos legítimamente emitidos o averiguar su contenido y relacionarlo con el votante. Estos ataques a la integridad y a la confidencialidad se pueden realizar, por ejemplo, mediante la introducción de programas maliciosos en los ordenadores personales de los votantes o de los lugares públicos donde se pudiera votar, consiguiendo cambiar el voto emitido por el votante o impedirle votar introduciendo dispositivos que alteren la comunicación. Para contrarrestar los citados ataques a los sistemas informáticos y a las redes telemáticas, los sistemas de votación más avanzados incluyen procedimientos criptográficos que permiten garantizar la confidencialidad e integridad de la información, así como proporcionar una prueba sobre el verdadero origen de esta.

2. Ataques sobre la infraestructura de comunicaciones cuyos servidores son proclives a sufrir un ataque de denegación de servicio el día de la votación, buscando impedir a los votantes el legítimo derecho a ejercer su voto. Una de las maneras habituales en que se presenta este tipo de ataques consiste en que, previamente a la celebración del evento señalado, se hayan introducido troyanos en una cantidad elevada de computadoras, y que el día en que este evento se lleva a cabo el troyano se active, ocasionando que los ordenadores generen tráfico suficiente para inutilizar la infraestructura de

comunicaciones. Es este problema de muy difícil solución y muy atractivo para colectivos atacantes organizados por diversos motivos, por lo que es de prever que se vayan desarrollando tecnologías de protección. Mientras se alcanza esta situación, el sistema está más expuesto si la votación se realiza desde cualquier computadora, por medio de Internet, que si se restringe el ámbito de actuación de los votantes a un entorno controlado como el que se da cuando la votación solo se puede realizar desde lugares específicos y empleando redes privadas virtuales. Otros ataques a la infraestructura física exigen la redundancia de servidores y de sistemas de alimentación eléctrica.

3. La alteración de resultados de la votación es una amenaza que afecta a cualquier sistema de votación, tradicional o no. Se trata de una amenaza que puede materializar un atacante desde dentro del propio sistema con gran probabilidad de éxito, consiguiendo que los resultados que se publiquen como definitivos no se correspondan verdaderamente con los votos emitidos. En los sistemas tradicionales, este riesgo es contrarrestado por la existencia física del papel de los votos emitidos, y por la incorporación de supervisores y observadores que vigilan tanto el proceso de votación como el de recuento. Sin embargo, en la votación electrónica esta amenaza, con frecuencia, es descuidada o su riesgo infravalorado, a pesar de que los estudios al respecto indican que uno de los factores que impiden la aceptación social de estos sistemas es la percepción por parte de los ciudadanos de que existe una gran facilidad para modificar los datos almacenados electrónicamente.

   Una de las soluciones planteadas para enfrentarse a este problema consiste en generar un comprobante, que desde ciertos sectores se insiste en que sea en papel, que permita al votante asegurarse de que el voto ha sido contabilizado conforme con sus deseos. Sin embargo, la existencia de un comprobante en el que figure de alguna forma más o menos velada el voto emitido por el ciudadano plantea la posibilidad de que pudiera utilizarse como elemento de coacción o venta de votos, por lo que es conveniente buscar soluciones alternativas.

2. Propuesta de elementos y criterios evaluables

Para la elaboración de la propuesta recogida en este apartado se ha partido de los estudios de importantes sistemas de votación y de la propia experien-

cia adquirida en el diseño de un sistema de votación electrónica (Tribunal Superior Eleitoral 2013, Estonian National Electoral Committee 2013, Ministry of Local Government and Regional Development 2011, Scytl Secure Electronic Voting, S.A. 2013, Ben Adida 2006, James Heathe 2006, Gómez Oliva 2005).

En los siguientes apartados se procura dar una visión extensa de los aspectos en los cuales es conveniente poner una atención crítica a la hora de comparar aspectos de seguridad y pulcritud de funcionamiento de los sistemas de votación. Se enumeran y comentan diversos elementos agrupados en cuatro categorías: protección del entorno, protección interna, verificación del proceso y auditores y elementos por auditar.

2.1. Protección del entorno

El conocimiento del entorno con el que interactúa el sistema de votación electrónica o telemática es primordial puesto que allí se puede encontrar el eslabón débil por el que se rompa una cadena de protecciones del propio sistema de votación automatizado. Un sistema de votación debe seguir las pautas de funcionamiento que le impone la sociedad en la que se va a aplicar, y estar sometido a las decisiones humanas de las personas que tengan a su alcance la configuración, gestión y operación de los equipos que lo componen. Además, en casi todos los casos, este sistema de votación debe interactuar con elementos que resultan ajenos a su control. A continuación, se identifica requisitos del entorno que determinan el comportamiento del sistema de votación (tabla 1).

Tabla 1

Elementos para la protección del entorno

Confección, actualización y consulta del censo electoral
Identificación de los votantes
Información que se debe proporcionar sobre el ciudadano
Formato, soporte físico y protecciones de seguridad
Emplazamiento y equipos
Necesidades de elementos de identificación de personas autorizadas
Cualificación necesaria de los votantes para ejercer su derecho a voto

2.1.1. Confección, actualización y consulta del censo electoral

El censo electoral es una pieza clave en la limpieza del proceso, ya que desde la manipulación de sus datos se podría incluir ciudadanos inexistentes, mantener ciudadanos que deberían haber sido dados de baja por cualquier motivo legal de pérdida de la condición de votante (cambio de residencia, dictamen judicial, defunción) y excluir ciudadanos aplicando criterios ilegítimos.

Además, es necesario conocer los procedimientos por los cuales el sistema de votación y el de gestión del censo asumen las condiciones de interfaz y participan de los mecanismos comunes de seguridad, dado que la comunicación en este caso requeriría de al menos ofrecer garantías de integridad y prueba de origen.

Un mal funcionamiento accidental o fraudulento del censo o de la comunicación de la entidad que identifica y autentica a los votantes con dicho censo no puede modificar votos legítimamente emitidos, pero puede impedir la emisión de votos legítimos y puede también amparar la adición de votos ilegítimamente.

2.1.2. Identificación de los votantes

El sistema de votación necesitará interactuar de alguna forma con el ciudadano que se identifica aportando físicamente un documento o alguna pieza de información propia. La adecuada gestión de la identificación de los ciudadanos es un paso de crucial importancia hacia la limpieza de todo el proceso electoral y adquiere dimensiones importantes cuando se pretende aplicar identificación electrónica a la votación telemática. Recae sobre el ciudadano la obligación de aportar la documentación que se le requiere para votar y sobre el sistema la obligación de no producir falsos negativos ni falsos positivos.

Es necesario conocer la forma en la que el sistema se protege ante la suplantación de personas, así como la protección existente para garantizar la integridad y la confidencialidad de la información en las comunicaciones.

2.1.3. Información que se debe proporcionar sobre el ciudadano

Entre la información que proporciona el votante al identificarse y la que proporciona el censo, se debe generar toda la información que requiera el sistema de votación para ejecutar correctamente sus procesos. La seguridad de que se está comunicando con el ciudadano que dice ser es proporcionada por los procedimientos electrónicos o manuales de identificación, y los datos de la elección en la que este ciudadano puede tomar parte puede ser suministrada por el sistema de gestión del censo electoral.

Es necesario conocer los procedimientos que facilitan esta comunicación, y evaluar sus amenazas y riesgos. Habrá también que comprobar que el sistema no obtiene ni genera nada más que la información necesaria para operar adecuadamente.

2.1.4. Formato, soporte físico y protecciones de seguridad

Además de conocer el formato de la información que se intercambia, es importante conocer con detalle cuáles son las protecciones de seguridad a las que se somete tanto la información almacenada como la transmitida, cuáles son los medios físicos usados para la transmisión y para el almacenamiento de la información. A partir de este conocimiento se puede evaluar la eficacia u obsolescencia de los métodos de protección usados e identificar el riesgo residual.

Es también importante conocer si esta protección está apoyada, además, por la penalización judicial a las personas que puedan tener responsabilidad en algún mal uso de esta información.

2.1.5. Emplazamiento y equipos

Por lo habitual, los equipos que dan servicio a los sistemas de votación electrónica deben ser situados en recintos sometidos a normas de protección física de inmuebles de acuerdo con la valoración de los riesgos de sufrir accidentes, ataques o cualquier otro tipo de daños que se prevea. Aun sabiendo que las decisiones técnicas estarán condicionadas por las voluntades políticas, será recomendable prever redundancia (adecuadamente protegida) de equipos, de dispositivos de almacenamiento de datos, de suministro de energía eléctrica y

de comunicaciones en cantidad suficiente para hacer frente a ataques, accidentes, averías, etcétera.

2.1.6. Necesidades de elementos de identificación de personas autorizadas

Será muy recomendable realizar una identificación integral de todas y cada una de las personas que tiene acceso a los locales donde se sitúan las diversas partes de la infraestructura, determinando cuáles son los roles de cada una, y sus necesidades y posibilidades de acceso físico a los recintos. Estas condiciones adquieren aun mayor importancia en el caso de acceso a los servidores de sistemas de voto del nivel avanzado.

2.1.7. Cualificación necesaria de los votantes para ejercer su derecho a voto

Es conveniente identificar con claridad la capacitación mínima que permita a las personas emitir libremente un voto que refleje su voluntad y desglosar los beneficios que obtendría con una capacitación más elevada. Por ejemplo, en votaciones tradicionales, una persona que desconozca el idioma local en el que está escrita la mayor parte de la información o que carezca de habilidades aritméticas tendrá evidentes problemas para entender la documentación que forma parte de las actas del colegio electoral, aunque en general, está capacitado para emitir su voto libre y secreto.

La información sobre el sistema diseñado debería estipular en qué medida las nuevas tecnologías podrían, por ejemplo, permitir con reducido incremento de costo ofrecer a los votantes la información en diversos idiomas, y en diversos soportes (fundamentalmente, visual o auditivo) y recibir el voto desde un teclado, pantalla táctil o por medio de reconocimiento de voz, aportando así una ampliación del espectro de ciudadanos a cuyo alcance se pone el nuevo sistema de votación.

2.2. Protección interna

El sistema de votación debe realizar tareas críticas cuya protección es necesario establecer ante agresiones procedentes tanto desde el exterior del sistema como desde el interior de este. A continuación se identifican estas tareas (tabla 2).

Tabla 2

Elementos para la protección interna

Personas que intervienen en el proceso
Cualificación necesaria para ejercer su derecho a verificar voto propio
Equipos y las conexiones entre ellos
Funciones y claves criptográficas utilizadas
Medidas de protección frente a ataques externos
Identificación y autenticación de personas
Autorización para votar
Emisión de los votos
Recuento y publicación

2.2.1. Personas que intervienen en el proceso

En el diseño completo del esquema de votación tendrá que existir una relación clara de los roles de las personas responsables del correcto funcionamiento del sistema y de la capacitación técnica mínima que deberán poseer las personas que ejerzan cada rol.

Será necesario conocer los procedimientos usados para identificar a las personas que asumen la gestión, la administración y la operación de los sistemas, así como el tipo de credenciales que necesitan estas personas, y las medidas previstas para evidenciar suplantaciones y falsificaciones.

2.2.2. Cualificación necesaria para ejercer su derecho a verificar voto propio

Al ser la verificación del voto un requisito que debe destacarse entre las propiedades de los sistemas de voto automatizados, la información sobre el sistema debería incluir la mención sobre la preparación necesaria que debe tener una persona para obtener las pertinentes pruebas y la preparación necesaria para comprender, por sí misma, esas pruebas que aporta el sistema.

El ejercicio del derecho a llevar a cabo la verificación individual del voto típicamente pone en peligro el voto secreto, por lo que deben establecerse con

claridad los mecanismos de acceso a la verificación y aportación de pruebas para evaluar en qué medida evitan convertir este derecho de verificación en un riesgo para el votante que debería poder ejercer de forma segura, fiable y voluntaria su prerrogativa de verificar el tratamiento de su voto.

2.2.3. Equipos y las conexiones entre ellos

Es necesario establecer previamente las características básicas que deben poseer el *software* y el *hardware* que interviene en el proceso electoral, así como las características físicas y lógicas de las comunicaciones, determinando sus procedimientos de uso y la política tanto de verificación como de auditoría. La tendencia a incorporar mecanismos de identificación biométrica en las máquinas de votación es una decisión que debería estar pulcramente identificada, informada y verificada la imposibilidad de romper el secreto del voto.

En este punto, es también importante conocer el nivel de compromiso de los usuarios con los fabricantes, y en general con los titulares de licencias y patentes. A partir de ese conocimiento, se podrá valorar su seguridad y evaluar los riesgos remanentes para la información.

2.2.4. Funciones y claves criptográficas utilizadas

Los sistemas de votación automatizada se apoyan en procesos criptográficos para establecer las garantías que le son propias. La información intercambiada está protegida por mecanismos criptográficos que garantizan la integridad, prueba de origen y confidencialidad de dicha información. Los sistemas de votación electrónica, aunque mantengan como aspecto fundamental la existencia del voto en papel, manifiestan apoyarse en procesos criptográficos.

Es necesario establecer con claridad (y relacionarlo con el estado de la tecnología en el momento de ser usada) lo siguiente:

- cuáles son las protecciones que se aplican a cada pieza de información
- qué algoritmos criptográficos se usarán en cada caso y con qué fin
- cómo se generarán las claves y cuáles son las características básicas de estas: longitud, tiempo de vida, etcétera.

- qué procedimientos se usarán para la distribución y conservación de las claves
- qué procedimientos se aplicarán en la custodia de cada clave desde su generación hasta el momento en que su compromiso no comporte riesgo
- qué riesgos se han identificado ante el posible compromiso de cada una de las claves en las diferentes fases del proceso de votación
- cuáles son las contramedidas previstas para minimizar o anular el daño producido por el compromiso de cada clave.

2.2.5. Medidas de protección frente a ataques externos

Un sistema de votación es susceptible de recibir ataques por variados motivos, que pueden incluir tanto el divertimento o reto científico-técnico para una parte de la población, como la obtención de beneficio político, económico o social para otros. Un importante punto débil de estos sistemas es el acceso a sus recursos con limitaciones laxas de distancia, de horarios y de fronteras. Será útil indicar las medidas destinadas a impedir que un atacante pueda actuar sobre información sensible en las distintas fases del proceso, obteniendo, modificando o destruyendo su contenido. Otro ataque de especial importancia dada la apertura geográfica y limitación temporal del proceso electoral es el de denegación de servicio (DoS) para el cual es previsible una rápida «evolución sincronizada» en las técnicas de ataque y de defensa, como se está poniendo de manifiesto con las actuaciones del colectivo Anonymous.

2.2.6. Identificación y autenticación de personas

Una de las premisas que se puede considerar como universal en los sistemas de votación es que se debe garantizar a todas las personas que pertenecen al cuerpo electoral el derecho a entregar un voto para que sea correctamente contabilizado. Además, se debe garantizar que no se contabilizará ningún voto que provenga de persona alguna que no pertenezca a este cuerpo o provenga de alguna entidad extraña. Debe estar clara la forma en la que los procedimientos que dan soporte a esta garantía no cometen errores, accidentales o intencionados, en la identificación ni en la autenticación de votantes.

Estrechamente vinculado con la adecuada identificación del ciudadano está la autenticación de este como potencial votante. Mientras que para lo primero se requiere la aportación de la credencial adecuada, para lo segundo es ineludible la correcta gestión de los registros del sistema. En esta parte del proceso, es importante identificar las posibilidades de que se produzca suplantación de personas o negación indebida de la autenticación.

2.2.7. Autorización para votar

La identificación y autenticación de las personas está orientada a otorgar el permiso para que, si esta persona pertenece al cuerpo electoral (dicho de otra forma, está incluida en el censo electoral) pueda entregar el voto que será adecuadamente contabilizado. La documentación del sistema debe incluir la enumeración clara de la información que contiene la autorización para votar, las garantías de que no se otorga autorizaciones indebidas ni se deniega autorizaciones a personas legitimadas para votar, así como los mecanismos existentes para detectar y evitar posibles intentos de suplantación de votantes. Como aspecto destacado, es también necesario comprobar que esta autorización es condición no solo suficiente para emitir el voto sino que es una condición de obligado cumplimiento que nadie puede saltarse. Tan importante es este aspecto en sistemas en los que la autorización es gestionada por personas cuya honradez debe ser ejemplar (que abren una puerta, levantan una barrera o vigilan visualmente) como en sistemas en los cuales estas autorizaciones son piezas de información cuya dificultad de falsificación debe ser alta.

2.2.8. Emisión de los votos

La aceptación de un documento en papel o de una pieza de información como voto válido es un paso crítico del sistema. Es oportuno conocer el uso que el sistema hace de la autorización para votar, las garantías que evitan que puedan votar personas sin la autorización debida, realizando, entre otras, acciones como la falsificación o reutilización de autorizaciones, o bien suplantando a votantes autorizados o, incluso, saltándose el paso de aportación de la autorización. Habrá que evaluar la posibilidad de burlar las protecciones del sistema de forma que se llegue a aceptar como válido un voto emitido por personas no autorizadas o por entidades fraudulentas que podrían estar dentro del propio

sistema. Tampoco se debe descuidar el análisis de las posibilidades de que el sistema ponga impedimentos, accidentales o fraudulentos, que provoquen que personas autorizadas no puedan votar o que votos válidos no sean adecuadamente contabilizados.

Uno de los puntos especialmente delicados, que ha de estar suficientemente justificado y documentado, es la forma en la que el sistema combina la garantía de que el voto es secreto, con la existencia de mecanismos fuertes de identificación y autorización de votantes.

2.2.9. Recuento y publicación

Una de las razones que surgen con más fuerza entre los detractores de los sistemas automatizados de votación es la escasez de pruebas tangibles que permitan a los ciudadanos tener la certeza de que el recuento no ha sido manipulado por accidente, ataque o por voluntad de cometer fraude, y que los resultados publicados son fieles al recuento realizado. En cada sistema se requiere saber cuáles son los mecanismos robustos que permiten a las autoridades, a los candidatos y a los colectivos ciudadanos confiar que los votos han sido no solo correctamente recibidos y almacenados por el sistema sino que además fueron tenidos en cuenta de modo adecuado en el recuento y publicación de resultados. Se deben identificar las garantías aportadas de que no se ha producido inserción ilegítima de votos ni destrucción o modificación de votos válidos.

2.3. Verificación del proceso

Los sistemas de votación tienen previsto ofrecer habitualmente diversos aspectos de verificación del proceso como valor añadido sobre los métodos de votación tradicional, además de las auditorías que deben contar con personas preparadas para ello (tabla 3).

Tabla 3
Elementos para la verificación del proceso

Provisión de pruebas para procesos de verificación/reclamación
Detección de eventos anómalos
Verificación resultados versus coerción

Es necesario conocer claramente cuáles son las pruebas que los candidatos, colectivos de la sociedad civil y ciudadanos actuando en nombre propio pueden obtener a partir del proceso de verificación, y cuáles son las que pueden aportar en caso de disconformidad con los resultados (o con alguna otra parte del proceso) y en qué grado estas pruebas son robustas. Es decir, que no han podido ser falsificadas, tienen el valor que se les atribuye y no ponen en riesgo a la persona que efectúa la reclamación. Son igualmente importantes las medidas que otorgan argumentos de defensa del sistema ante acusaciones equivocadas o mal intencionadas. Es conveniente conocer cuáles son los eventos anómalos que pueden ser detectados, y una vez ocurrido tal suceso, interesará saber, por una parte, qué posibilidad existe de rectificar, y por otra, si se puede identificar a los responsables. Sería también un aporte positivo que se evalúe cuantitativa y cualitativamente si la facilidad de verificación se asocia con algún riesgo, por ejemplo, con el de violación del secreto del voto. La verificación de las distintas etapas del proceso electoral alcanza desde los aspectos más triviales, como son los detectables por inspección visual, a los más específicos que exigen conocimientos especializados y equipamiento apropiado, como puede ser la detección de comunicaciones inalámbricas, el cifrado y descifrado correcto de una pieza de información, etcétera.

Los candidatos, colectivos de la sociedad civil y ciudadanos actuando en nombre propio están en contacto directo con el sistema electoral mientras dura la jornada en la cual tienen interés directo. Son ellos los que deben poseer herramientas suficientes para detectar la autenticidad de los recursos físicos y lógicos con los que se inicia la interacción de votantes con el sistema, descubrir anomalías en el funcionamiento y denunciarlas rápidamente. Estas anomalías deberán ser corregidas si es viable y, en la medida de lo posible, identificar las causas. Además, es deseable que las herramientas y procedimientos de verificación sean poco intrusivos y en lo posible nada destructivos.

Es necesario establecer cuáles son los mecanismos al alcance de quienes tengan la posibilidad de contrastar los resultados que les permitan obtener pruebas fehacientes para conocer con completa garantía cómo ha sido tenido en consideración cada voto verificado. Además, deben fijarse los mecanismos que protegen al sistema ante la posibilidad de otorgar legitimidad a reclamaciones erróneas o fraudulentas. Si quien ejerce la verificación es el votante, debe estar clara la forma en la que está protegido ante una posible coerción en la que se le obligue a realizar el paso de verificación con el objetivo de que revele el contenido de su voto.

2.4. Auditores y elementos por auditar

La auditoría interna o externa de los sistemas es habitualmente la herramienta que los sistemas de votación electrónica o telemática esgrimen como garantes fundamentales de su buen hacer. Será conveniente, por una parte, conocer cuáles son las medidas orientadas a avalar la honradez de los auditores, y, por otra, identificar los eventos que podrán ser detectados por los procesos de auditoría y, si ocurre, las características de la información privilegiada que si cayera en manos inadecuadas pudiera poner en riesgo la limpieza del proceso electoral. Es necesario evaluar la incidencia de la auditoría que se realiza en distintos momentos del proceso de votación con el fin de prevenir que esta interfiera en este, ralentizando las comunicaciones, obteniendo más información de la necesaria o alterando la información (tabla 4).

Tabla 4

Auditores y elementos por auditar

Auditoría de registros de personas
Auditorías sobre equipos terminales, servicios y comunicaciones
Verificación de plan de contingencia en caso de desastre
Auditoría sobre las protecciones de seguridad de la información en las redes
Auditorías sobre la generación de claves
Auditorías sobre las protecciones de los datos
Auditoría del escrutinio y de los datos publicados
Otros aspectos identificados por los usuarios y auditores

Si bien es cierto que probablemente los objetos por auditar serán decididos por los responsables de la puesta en funcionamiento del sistema y de los propios auditores, es conveniente que la información de diseño del sistema de voto telemático proporcione la identificación de los registros y procedimientos especialmente destinados a ofrecer elementos que faciliten la auditoría. Asimismo, resultará beneficioso que el diseño del sistema indique la relación de auditorías previstas, especificando claramente el tipo de auditoría y momento del proceso en el que se realiza, así como el evento que resultará avalado o cuestionado.

Podría ser oportuno detallar en qué grado la auditoría puede medir la honestidad con la que se ha realizado la selección, nombramiento, y capacitación de las personas responsables de las labores de administración, montaje, configuración, puesta a punto y mantenimiento de los sistemas. Deberían también ser objeto de evaluación tanto la accesibilidad y disponibilidad de los puntos de votación como la cobertura de las comunicaciones entre los puntos de votación y los servidores.

Un paso más adelante sería que la ciudadanía, esto es electores y candidatos, puedan proponer auditorías específicas y conocer sus resultados.

2.4.1. Auditoría de registros de personas

Un punto crucial, como ya se ha expuesto, es el comportamiento del censo y su interfaz con el sistema electoral. Con anterioridad a la jornada electoral hará falta conocer en qué medida la auditoría puede aseverar que ninguna persona ha sido incluida ni excluida con criterios arbitrarios. Además, habrá que auditar la comunicación entre el censo y el sistema electoral. Resultará de gran utilidad disponer de los criterios con los que se elige la muestra que es auditada y de la descripción del índice de gravedad (con los criterios que se establezcan) de los resultados que se aparten de los que se consideran normales.

2.4.2. Auditorías sobre equipos terminales, servidores y comunicaciones

El equipo auditor debería disponer del personal técnico con la cualificación adecuada y recursos materiales que le permita dar fe de que todos los dispositivos, tanto en su *software* como en su *hardware*, realizan todas las tareas establecidas

en el documento de diseño, y que no lleven a cabo ninguna tarea que no esté indicada en dicho documento. En su defecto, si llevan a cabo tareas no indicadas como necesarias para la elección a la que se aplica (puede ser efecto poco deseado de la reutilización de recursos) debe quedar claramente indicado qué tareas son y los mecanismos que se establecen para que no interfieran con las tareas encomendadas en una elección determinada. La gran cantidad de equipos que interactúan directamente con los votantes puede ser razón para que no se sometan al proceso de auditoría todos ellos, ya que sería poco eficaz una auditoría realizada con mucha antelación a su uso. En este caso, resultará de gran utilidad disponer de los criterios con los que se elige la muestra y de la descripción del índice de gravedad (con los criterios que se establezcan) de los resultados que se aparten de los normales. Los sistemas que están fuera de la vista de los ciudadanos, cuyo funcionamiento complejo deja fuera del alcance de su comprensión a muchos de ellos, son objeto de desconfianza para colectivos que se oponen a la utilización de los sistemas de votación electrónica o telemática. Los informes de auditoría son especialmente importantes cuando hacen referencia a los sistemas que autorizan a votar, que reciben y almacenan los votos, los que calculan los resultados, y los que hacen públicos los resultados definitivos.

2.4.3. Verificación de plan de contingencia en caso de desastre

Un plan de contingencia de seguridad informática debe definir los pasos por seguir para minimizar el efecto negativo de un desastre. La interrupción de suministro eléctrico, interrupción de comunicaciones, el fallo técnico de algunos de los servidores, etcétera, pueden ocasionar pérdidas irreparables si se conjugan de determinada manera. La auditoría tendría que verificar en qué grado resulta ser eficaz el plan de contingencia previsto o, en su caso, la gravedad de su inexistencia.

2.4.4. Auditoría sobre las protecciones de seguridad de la información en las redes telemáticas por medio de las que se enviarán los datos

A medida que evoluciona la tecnología y los conocimientos en criptoanálisis, van perdiendo efectividad las protecciones criptográficas por lo que es necesario auditar en cada momento el grado de validez, eficacia y actualización de los

mecanismos y protocolos de seguridad aplicados a la información en tránsito y almacenada en las distintas fases.

2.4.5. Auditorías sobre la generación de claves

El método, el lugar, el momento de generación de claves y su distribución son aspectos especialmente críticos en lo que afecta a la seguridad del sistema de votación. La auditoría debería establecer la probabilidad de compromiso de dichas claves en esta fase inicial y en todo el ciclo de vida de la clave, así como el grado en que el riesgo puede comprometer el buen hacer del sistema.

2.4.6. Auditorías sobre las protecciones de los datos

Una vez identificados los datos o combinación de ellos, que pudieran poner en riesgo de incumplimiento las garantías que el sistema de votación debe ofrecer, hará falta que la auditoría indique la forma de custodia y en qué grado esta información (claves, censo, resultados, etcétera) está protegida. Asimismo, la auditoría establecerá el grado de cumplimiento del compromiso de tratamiento de la información en los momentos establecidos una vez finalizado el proceso.

2.4.7. Auditoría del escrutinio y de los datos publicados

El objetivo principal de todo el despliegue del sistema de votación es que los resultados publicados sean fiel reflejo del resultado del escrutinio de votos correctamente registrados. La auditoría podrá evidenciar diferencias aparecidas entre los resultados reales y los publicados o respaldar la exactitud de estos. Además, revisará previamente los registros que refrenden el recuento de votos válidos y votos anulados. Si la revisión se hace sobre una muestra de los votos, indicará los criterios con los que se elige dicha muestra.

2.4.8. Otros aspectos identificados por los usuarios y auditores

Una vez conocidas las especificaciones del sistema, será muy útil que los usuarios y los auditores preparen su propia relación de auditorías pedidas, ampliando o reduciendo de forma razonada la lista anteriormente expuesta, de acuerdo con las necesidades específicas de la sociedad.

3. Conclusiones

La implantación de sistemas informáticos y telemáticos para automatizar en todo o en parte los procesos electorales suele ser vista como una «modernización» o como una «agresión». Es conveniente mantener algún grado de alerta ante una cierta presión social que tienda a apoyar este tipo de cambios sin pararse a pensar en la conveniencia o no de su implantación. A estos movimientos tecnofílicos no son ajenos los fabricantes de tecnología, que ven en estos cambios una oportunidad de negocio. Por la parte casi tecnofóbica, los argumentos esgrimidos en detrimento de la aplicación de tecnologías a los procesos de votación suelen omitir cualquier evaluación sobre los riesgos que la aparición de estas y otras tecnologías se ciernen no solo sobre el voto electrónico sino también sobre el voto tradicional.

A la fecha, pocos esquemas de votación abordan de forma eficiente la problemática de vulnerabilidad de los electores y alteración de resultados inherente a la votación en urna electrónica o mediante las redes telemáticas. Se hace necesario, por una parte, introducir sólidas herramientas de verificación para garantizar la veracidad de los resultados, incluso ante posibles confabulaciones entre agentes del sistema. Por otra parte, obliga a añadir eficaces elementos de control que supervisen el correcto desarrollo de todo el proceso de votación y que, en caso de producirse un mal funcionamiento, accidental o malintencionado, permita detectarlo, identificar a los responsables y, en lo posible, corregir la desviación.

El cuerpo formado por la caracterización de los sistemas y variables de evaluación conforman la propuesta de este artículo que recoge todos los aspectos que deben ser cuidadosamente analizados y solucionados antes de la puesta en marcha de un sistema de votación electrónica, a la vez que permite un análisis objetivo y riguroso de los sistemas ya en marcha. De esta manera, se pretende facilitar una paulatina evolución de los sistemas de votación electrónica actuales hacia otros con mayores niveles de transparencia, que conlleven un mayor nivel de confianza y aceptación por parte de los ciudadanos y demás agentes implicados.

Referencias bibliográficas

Adida, Ben y Ronald L. Rivest

2006 «Scratch & Vote: self-contained paper-based cryptographic voting». WPES 2006-ACM Workshop on Privacy in the Electronic Society. New York (pp. 29-40).

Carracedo Gallardo, J.

2004 *Seguridad en redes telemáticas*. McGraw-Hill. Madrid. Mc Graw-Hill

CONSEJO NACIONAL ELECTORAL VENEZOLANO

2012 «Tecnología Electoral en Venezuela». Portal del Consejo Nacional Electoral venezolano. Revisado el 6 de septiembre de 2014, de <www.cne.gov.ve/web/sistema_electoral/tecnologia_electoral_descripcion.php>.

DIRECTORATE OF DEMOCRATIC INSTITUTIONS

2010 *E-voting handbook*. Estrasburgo: Council of Europe Publishing.

ESTONIAN NATIONAL ELECTORAL COMMITTEE

2013 Internet Voting in Estonia. Recuperado el 6 de septiembre de 2014, de <www.vvk.ee/voting-methods-in-estonia/engindex/?tpl=1062>.

Gómez Oliva, A., *et al*.

2005 *Votescript: Telematic voting system designed to enable final count verification. Proceedings of Collaborative Electronic Commerce Technology and Research*. Talca, Chile: CollecterLatam.

Heather, James, *et al*.

2006 *Prêt à Voter*. Revisado el 6 de septiembre de 2014, de <www.pretavoter.com>.

MINISTRY OF LOCAL GOVERNMENT AND REGIONAL DEVELOPMENT

2011 «El pliego de condiciones límite para la obtención de la solución de voto electrónico». Revisado el 6 de septiembre de 2014, de <www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/news-about-the-e-vote-2011-project/year/2009/the-final-tender-documentation-for-procu.html?id=598213>.

SCYTL SECURE ELECTRONIC VOTING, S.A.

2013 <www.scytl.com>. Revisado el 6 de septiembre de 2014, de Secure Electronic Voting. Remote e-voting (Internet voting) and Poll-site e-voting. Scytl: <http://vimeo.com/51684209>.

TRIBUNAL SUPERIOR ELEITORAL

2013 *O Tribunal da Democracia*. Revisado el 6 de septiembre de 2014, de <www.tse.jus.br/hotSites/CatalogoPublicacoes/pdf/codigo_eleitoral/codigo-eleitoral-anotado-e-legislacao-complementar-11-edicao.pdf>.

[Sobre las autoras]

Ana Gómez Oliva

Pertenece al Departamento de Ingeniería y Arquitecturas Telemáticas de la Universidad Politécnica de Madrid (UPM). Se ha especializado en desarrollo de sistema de voto electrónico por Internet, y en voto y participación ciudadana por medio de Internet. Cuenta con dos tesis doctorales: *Solución para la delegación de identidad en sistemas de gestión de identidad paneuropeos basada en infraestructuras de certificación y lenguajes formales de asertos de seguridad* (2010) y *Aplicación de documentos de identificación electrónica a un esquema de voto telemático a escala paneuropea, seguro, auditable y verificable.*

Emilia Pérez Belleboni

Doctora en Telecomunicación por la Universidad Politécnica de Madrid (UPM). Pertenece al Departamento de Ingeniería y Arquitecturas Telemáticas de la UPM. Su tesis doctoral se denomina *Aplicación de documentos de identificación electrónica a un esquema de voto telemático a escala paneuropea, seguro, auditable y verificable.*