EXIGENCIAS TÉCNICAS DEL VOTO ELECTRÓNICO

Por Joaquín Domínguez Fernández,
Cortes de Aragón

INTRODUCCIÓN

El concepto de voto electrónico es un concepto muy amplio que engloba la utilización total o parcial de dispositivos y sistemas de tecnología de la información y de las comunicaciones (TIC) a todo el proceso electoral o a algunas fases del mismo. Podemos incluir la emisión del voto en una urna electrónica (con o sin impresión inmediata de una papeleta que permita la verificación por parte del ciudadano o de la autoridad), el registro y la verificación de la identidad del elector, el recuento de la mesa electoral en particular o el recuento global consolidado, la transmisión de los datos u otra serie de actividades. Es decir, se trata de emplear las TIC en todas o en algunas fases del proceso electoral.

Las primeras maquinas que trataron de automatizar algunos aspectos de los sistemas de votación datan del siglo XIX, así en 1869 Thomas Alva Edison patentó un sistema de grabación de voto electrónico. El primer uso oficial de una máquina para votar, conocida como cabina automática de votar (Myers Automatic Booth) se desarrolló en Lockport, New York en 1892. Hacia 1930, estas máquinas estaban instaladas en las principales ciudades de Estados Unidos y en 1960 más de la mitad de la población votaba usando estas máquinas.

El empleo de ordenadores en los procesos electorales se remonta a 1964 en Estados Unidos, siendo en los años 80 cuando toma verdadera importancia

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

permitiendo automatizar las bases de datos de los censos electorales y la consolidación en el recuento de votos.

CLASIFICACION DE LOS SISTEMAS DE VOTACIÓN

En función del grado de automatización alcanzado podemos clasificar los sistemas de votación en distintos niveles.

En el primer nivel de esta clasificación encontramos los sistemas "clásicos" de votación: votación mediante urna y papeleta, tarjetas perforadas, lectores ópticos, maquinas de palanca …

1. *Sistemas de votación mediante maquinas de palanca:* Derivan de la maquina original de Myers de 1892. El votante realiza la selección del nombre del candidato de su preferencia haciendo girar una pequeña palanca situada junto a los nombres de los mismos. Los votos se registran al final del proceso, tirando de una palanca mayor. A medida que cada palanca es activada, giran las ruedas dentro de la máquina para indicar o marcar un voto. Al final de la votación, las ruedas de conteo de cada máquina indican el número de votos emitidos por cada candidato. Hace más de 30 años que no se fabrican esas máquinas porque su mantenimiento es muy caro y difícil. En consecuencia, han caído en desuso en forma gradual.

2. *Sistema de votación mediante tarjeta perforada*: La papeleta, en la que figuran todos los candidatos a los diferentes puestos, y todas las opciones sometidas a referéndum, tiene un círculo para cada opción, y el votante debe perforar con un sacabocados el círculo correspondiente a la opción elegida. La máquina tiene un foco de luz, y esta luz pasa a través de las perforaciones e incide sobre una célula fotoeléctrica que actúa sobre un contador, que va

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

contando así los votos. El sacabocados debe cortar la cartulina y el confeti formado debe caer; si no cae, la luz no puede pasar, y la máquina no cuenta el voto.

3. *Sistemas de voto mediante lector óptico:* es la evolución del sistema anterior. Se trata de aparatos capaces de "leer" marcas realizadas por el votante en una papeleta con un bolígrafo. Es el mismo sistema utilizado para el tratamiento de algunas loterías o tests. Actualmente, el aparato lector ha sido desarrollado de manera que ya no solo reconoce cruces o marcas, sino también caracteres como números (que permitirían ordenar opciones) o incluso palabras.

En un segundo nivel de esta clasificación encontramos los sistemas de votación que sustituyen algunos de sus elementos físicos o procedimientos manuales por algún tipo de sistema o proceso electrónico. Que tratan de automatizar mediante sistemas o procesos electrónicos la autenticación del votante, el proceso de la votación propiamente dicho o el proceso de escrutinio. La gran mayoría de las actuaciones para automatizar el proceso de votación que se ha realizado en los diferentes países se encuadra en este segundo nivel.

En este segundo nivel encontramos los sistemas electrónicos de votación: Demotek, Registro Electrónico Directo (RED)…

1. *Demotek:* Diseñado y desarrollado dentro de un proyecto dirigido por la Dirección de Procesos Electorales del Departamento de Interior del Gobierno Vasco. Realiza la lectura automática de la opción de voto de la papeleta mediante el reconocimiento óptico de los caracteres que figuran en ella. Consta de los mismos componentes que un sistema tradicional, es decir, urna y papeletas, además de un equipo electrónico para el reconocimiento y recuento instantáneo del voto en el momento en

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

que es emitido, y un módulo de comunicaciones para la transmisión de los resultados, tras el cierre de las urnas, a una oficina electoral central.

2. *Maquinas de registro electrónico directo*: Se trata de ordenadores modificados, en los que el elector establece sus preferencias gracias a una pantalla táctil o a una pantalla y un teclado. En algunos casos, el propio aparato registra el voto directamente. En otras, el voto se graba en un soporte externo que el votante ha introducido previamente en el aparato (por ejemplo, una tarjeta magnética). Tras emitir su voto, el votante utiliza su tarjeta a modo de una papeleta tradicional, introduciéndola en una urna, que a su vez será un aparato lector de tarjetas magnéticas y que realizará el recuento. Y en otras el aparato registra el voto directamente pero imprime un comprobante de voto o papeleta para el elector, que en algunos casos deberá introducir en una urna al modo tradicional, o lo guarda para una verificación posterior.

En el tercer nivel de la clasificación tenemos los sistemas de votación que emplean las redes telemáticas. Se pueden dar dos situaciones diferentes: el elector se tiene que desplazar hasta un centro de votación (puede ser el colegio electoral o un centro acondicionado para ello) para emitir su voto, o bien el elector puede votar desde su casa a través de Internet.

VENTAJAS DE LA VOTACION ELECTRONICA

Los defensores de la votación electrónica señalan una serie de ventajas que aportan estos sistemas electrónicos frente a los sistemas tradicionales.

- Disminuyen las posibilidades de fraude electoral
- Su implementación aumenta la participación electoral

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

- Ahorro de costes
- Aumento de la velocidad en la presentación de los resultados
- Mejora de la precisión de los resultados
- Incrementa la accesibilidad para discapacitados
- Mayor flexibilidad
- Los equipos se pueden utilizar en otras consultas y no sólo para las elecciones (democracia directa)
- Se podrían eliminar varios materiales electorales, como las papeletas.
- Movilidad y comodidad del votante
- Son una consecuencia natural de la modernización democrática

CONSIDERACIONES SOBRE LA IMPLANTACIÓN DEL VOTO ELECTRÓNICO EN DIFERENTES PAÍSES

La mayoría de los países del mundo han considerado o están considerando la utilización del voto electrónico. Muchos de ellos han realizado pruebas y varios utilizan actualmente el voto electrónico vinculante. Vamos a analizar algunos ejemplos de países que utilizan el voto electrónico vinculante, así como determinados problemas que han surgido.

1. **Bélgica**: Fue el pionero del voto electrónico en Europa. Introdujo el voto electrónico en 1991 para resolver los problemas derivados de la complejidad del sistema electoral belga (voto obligatorio, hasta cinco procesos electorales simultáneos, tres lenguas diferentes, …..). Dicho sistema suponía un enorme gasto de tiempo a causa de los procesos manuales de validación y recuento de votos, que resultaban bastante

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

tediosos y tenían un considerable margen de error. Para superar estas dificultades, Bélgica eligió un sistema simplificado, reemplazando las papeletas por una tarjeta magnética que aunque no modifica el proceso existente sí incorpora aspectos de seguridad física y tecnológica. Emplean el sistema Digivote desarrollado por Steria.

2. **Holanda**: Holanda ha retirado de manera preventiva las máquinas de voto electrónico (el 1 de octubre de 2007, la corte de Alkmaar anuló la certificación de las maquinas de votación NEDAP). Esto es consecuencia directa de la inseguridad de estas máquinas. Un estudio realizado por expertos holandeses, agrupados en la "We don't trust in the Voting Computers Foundation" ("Fundación Nosotros no Confiamos en las Maquinas de Voto") - sobre la maquina Nedap ES3B , utilizada en un 90% en Holanda, y en menor porcentaje y con mínimas modificaciones en Francia, Alemania, Irlanda, Dinamarca y Gran Bretaña, muestra como "con un breve acceso a los dispositivos antes de la elección, pudieron hacerse del control total y virtualmente imperceptible de los resultados de la votación", así como también descubrieron que las emanaciones de radio de una ES3B se pueden recibir en varios metros de distancia y utilizar para averiguar quién vota a quien.

3. **Estonia**: País pionero en el uso vinculante y flexible del voto por Internet. En 2.005 realizó una prueba piloto en unas elecciones locales, utilizando smart cards con firma electrónica. En las elecciones parlamentarias del 2.007, 30.275 personas votaron por Internet (3,5% de la población). Quienes desearon emitir su voto de forma electrónica contaron con la posibilidad de realizarlo durante los tres días previos al inicio de los comicios y la legislación electoral de este país establece la supremacía del voto tradicional (papel) sobre el electrónico. De esta forma, aun habiendo emitido un voto electrónico, los electores cuentan con la posibilidad de votar nuevamente en

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

papel. Este último anula el primero. Se precisa de una tarjeta de identidad electrónica (6 €) con criptografía asimétrica.

4. **Brasil**: hasta 1996 las elecciones eran realizadas con urnas de lona previamente selladas que recibían las papeletas de votación de los electores, las cuales eran escrutadas de manera manual lo que producía prácticas fraudulentas de dos tipos, en el escrutinio de los votos o en los registros de cada urna. Preocupados por este problema, el Tribunal Supremo Electoral constituyó en 1995 una Comisión del Voto Informatizado en consideración a las experiencias pioneras de voto automatizado. Esta comisión debió definir el equipo que tuviera en cuenta la complejidad del proceso electoral, la modesta infraestructura del país, con un gran número de electores analfabetos, grandes zonas del país con una geografía compleja y muchas veces inaccesible, donde no hay las mínimas condiciones como la energía eléctrica, recintos seguros, etc.

   El resultado concreto fue la creación del prototipo de la urna electrónica con características propias para utilizarse en el país. Reúne en la mesa receptora las funciones de lista nominal, urna y papeleta, funciona con energía eléctrica o bien con una batería común externa de automóvil, con teclado similar al del teléfono digital para el tecleo del número del candidato, pantalla líquida para la colocación de la fotografía del candidato y sobre todo, componentes producidos en el mercado brasileño, factor clave para el mantenimiento y soporte de las elecciones en todo el país.

   Su primera utilización fue en las elecciones de 1996 en las ciudades capitales y municipios con más de 100 mil personas. Para esta elección se usaron 75 mil urnas electrónicas para 32 millones de personas, es decir el 30% del electorado y 75 mil mesas electorales automatizadas. En las Elecciones Generales de 1998, se dio continuidad a la automatización del proceso en las que se incremento

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

el uso de la urna electrónica; 68 millones de ciudadanos utilizaron esta urna, es decir el 60% del total del electorado, se automatizaron 152 mil mesas electorales (50%). La urna electrónica fue el único método de votación en las elecciones a Presidente de la República en octubre de 2002 y fue empleado por 115 millones de votantes. El Tribunal Superior Electoral está estudiando cambiar Windows CE por Linux en las urnas electrónicas.

5. **Venezuela:** Cuenta con un sistema electoral tecnológicamente muy avanzado. El sistema consta de dos elementos electrónicos: la máquina de votación electrónica, con la que se emite el voto, y el dispositivo "captahuellas", que apoya el proceso de identificación.

   En las elecciones parlamentarias de 2005 las maquinas de votación empleadas fueron las Smartmatic modelos SAES3000 y SAES3300 (23.000 unidades). Corren el S.O. Windows XP y la aplicación de votación desarrollada en C+.

   Dispositivo "captahuellas": se escanea la huella dactilar del votante (ordenador independiente), se conecta a la Universidad Bolivariana en Caracas, donde se ubica una base de datos con las huellas de los votantes, si la huella se capturo en un proceso previo se coteja, y si no se almacena (emplean bases de datos locales de replica). En 2005 la base de datos contenía 6,8 millones de registros de un electorado de aproximadamente 14,4 millones.

   Proceso de votación: Cada votante tiene tres minutos para emitir su voto. Puede solicitar un nuevo periodo de 3 minutos y si durante este segundo periodo no vota, pierde su voto. Después de emitir el voto, la maquina imprime un resguardo que el votante puede comprobar antes de introducirlo en la urna. Esto sirve de backup y para la realización de auditorías manuales de determinadas urnas.

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

6. **India**: En 1989 se puso en marcha el voto electrónico, aumentándose desde entonces de forma gradual el número de maquinas. En las elecciones al Parlamento indio de 2004 se emplearon más de un millón de maquinas electrónicas distribuidas en 700.000 colegios electorales de 543 distritos. Las cifras en las que se mueve el país indio - 675 millones de electores, presentándose a las elecciones casi 800 partidos, miles de agrupaciones electorales y miles de candidatos independientes- hace conveniente sino imprescindible el uso de maquinas de votar electrónicas. Las maquinas de votar electrónicas fueron suministradas por dos empresas del país, con un coste reducido y un manejo simple.

7. **EE.UU**.: Los Estados Unidos tienen un sistema electoral complejo en el que cada Estado e incluso cada Condado determina la forma y los recursos electorales a utilizar. En las elecciones presidenciales de noviembre de 2.000, casi el 70% de los votantes utilizó la vía electrónica para emitir su voto. En el año 2.004, la mayor parte de los votantes emplearon sistemas automatizados; 13,7% empleó tarjetas perforadas; 14% empleó sistemas de palanca; 34,9% lectura óptica y 29,3% empleó equipos RED.

   Estados Unidos es el país que lleva más tiempo utilizando estos sistemas de votación electrónica y donde se han realizado estudios sobre su seguridad, sobre todo por parte de las universidades americanas.

   Uno de los fallos más destacables de estos sistemas es el que tuvo lugar en el estado de Florida, donde la falta de normativa y control, unido a una tecnología obsoleta (tarjeta perforada), propició que muchos votantes no pudieran saber con certeza qué opción era la que habían marcado.

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

La Universidad de Princeton hace público un estudio sobre la seguridad de la máquina Diebold AccuVote-TS. El documento concluye que la máquina es vulnerable a varios ataques extremadamente serios, que minan la precisión y la credibilidad de los recuentos de votos con ella realizados.

En un informe de la Universidad de Berkeley -California-, se llega a la conclusión de que las máquinas de votación (Diebold Election Systems Inc.) de la empresa Diebold no son lo bastante seguras para garantizar una elección fiable, y que el ataque de virus podría, a través de una sóla máquina, interrumpir o cambiar el resultado de todas las elecciones.

Universidad de Pensilvania: El informe EVEREST (Evaluation and Validation of Election-Related Equipment, Standards and Testing), que estudia sistemas de votación electrónicos de las empresas "Election Systems and Software (ES&S)" y "Hart InterCivic and Premier Election Solutions" antes conocido como "Diebold", pone en evidencia el sistema de voto electrónico de Estados Unidos (el 80% del voto en Estados Unidos es manejado por máquinas fabricadas por estas empresas). Se han detectado fallos de todo tipo, como por ejemplo, fallos debidos a "buffer overflows", cifrado insuficiente (inexistente en algunos casos) y fallos de firmware, que posibilitan alterar el resultado de unas elecciones.

Para resumir el estado de la votación electrónica en Estados Unidos nada mejor que citar al profesor Rubin que en el año 2006 publicó un libro titulado "*Brave new ballot" en* el que dice literalmente*: "Imagine* por un momento que usted vive en un país donde nadie está seguro de cómo se cuentan los votos y no existen registros fiables para realizar un recuento. Imagine que las máquinas cuentan los votos pero nadie sabe como lo hacen. Ahora imagine que alguien descubre que estas máquinas son vulnerables a ataques, pero las agencias

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

responsables no toman las medidas necesarias para hacerlas seguras. Si usted vive en U.S.A. no necesita imaginárselo. Esta es la realidad del voto electrónico en este país".

VOTO TELEMÁTICO

Este tipo de sistemas de votación electrónica prevé que el votante no deba desplazarse hasta el colegio electoral y pueda emitir su voto a través de las redes telemáticas. Puede tratarse de una red interna y controlada por la propia institución que organiza la convocatoria, o puede realizarse la votación desde cualquier plataforma conectada a Internet (generalmente un ordenador).

Las redes informáticas o telemáticas son un objetivo para los ataques y operaciones no autorizadas, afectando tanto a la seguridad de los sistemas como a la validez de la información que se almacena o transfiere. Entendemos por ataque cualquier uso malicioso de la red, realizado de forma intencionada.

Para hacer frente a los ataques se definen una serie de propiedades básicas de seguridad que debe de satisfacer cualquier sistema de voto telemático:

- *autenticación*: garantiza que una persona o una maquina es quien dice ser. Este servicio protege contra un ataque frecuente en la red, por el cual una entidad remota se hace pasar por quien no es (suplantación de personalidad). En este caso no existe ninguna persona que acredite la identidad de los votantes, tal y como ocurre en la votación tradicional con los miembros de las Mesa Electoral.

- *confidencialidad de los datos*: garantiza que los datos tan solo serán entendibles por el destinatario o destinatarios del mensaje. Protege contra el típico "pinchazo" de la comunicación (sniffer).

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

- *integridad de los datos*: Este servicio garantiza al receptor del mensaje que los datos recibidos coinciden exactamente con los envidados por el emisor de los mismos, es decir, el receptor detectará si se ha producido o no un ataque de modificación de mensaje, lo que le permitirá dar por buenos o no los datos recibidos.
- *no repudio*: sirve para evitar que alguno de los participantes en la comunicación niegue haber formado parte de ella.
- *Unicidad*: Cada votante sólo puede votar una vez.
- *Verificabilidad individual*: Cada votante deberá poder asegurarse de que su voto ha sido considerado adecuadamente, tanto en lo referente al contenido del voto emitido como si este ha sido tenido en cuenta adecuadamente.
- *Compra de votos o imposibilidad de coacción*: ningún votante debe ser capaz de demostrar ante terceros qué voto ha emitido.
- *Anonimato*: Se trata de conseguir que la identidad de la persona que realiza una determinada operación telemática (en este caso el voto) permanezca oculta ante alguno de los actores presentes en la operación.

El voto electrónico por Internet o voto telemático añade la complejidad de combinar la autenticación de los votantes con el mantenimiento del anonimato en relación con los datos depositados (voto). Pero además el votante debe disponer de mecanismos que le permitan comprobar que su voto ha sido contabilizado adecuadamente en la opción que eligió (*Verificabilidad*).

La mayoría de los servicios o mecanismos de seguridad se basan en técnicas criptográficas.

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

Criptografía:

La palabra criptografía proviene en un sentido etimológico del griego Kriptos=ocultar, Graphos=escritura, lo que significaría ocultar la escritura, o en un sentido más amplio sería aplicar alguna técnica para hacer ininteligible un mensaje. La criptografía es la ciencia de ocultar mensajes.

La criptografía se puede clasificar históricamente en dos: La criptografía clásica y la criptografía moderna.

- Criptografía clásica o simétrica: se utiliza la misma clave para cifrar y descifrar mensajes.
- Criptografía moderna, asimétrica o de clave pública: cada usuario posee dos claves, una privada que debe mantener secreta, y la otra publica que podrá conocer todo el mundo. El algoritmo más extendido y usado que implementa esta solución es el RSA.

La criptografía simétrica actúa de la siguiente manera:

- A quiere enviar un mensaje confidencial a B --> A cifra el mensaje con la clave publica de B, y solo B lo podrá descifrar con su clave privada.
- A cifra un mensaje con su clave privada. Cualquier usuario lo puede leer utilizando la clave pública de A. Pero como solo A tiene su clave privada, sólo él lo pudo cifrar (Autenticación).

Y esto es la base de la firma digital, sólo que en el caso de la firma digital A no cifra todo el mensaje sino una muestra, resumen o hash de tamaño fijo (128 o 160 bits, según el algoritmo que se emplee) y este es independiente de la longitud del mensaje original. La firma electrónica nos proporciona los servicios de autenticación, integridad y no repudio.

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

Para garantizar la confidencialidad podemos emplear el sobre digital, el sobre digital usa criptografía simétrica y asimétrica. Un sobre digital se genera a partir de un documento y una clave secreta que se genera de forma aleatoria, se cifra simétricamente el documento con la clave secreta, luego la llave secreta se cifra asimétricamente con la clave pública de la persona a la que le vamos a enviar el sobre y finalmente se concatenan dando origen al sobre digital.

Se pueden combinar los sobres digitales con las firmas digitales dando lugar a un sobre digital firmado y así se garantizan las propiedades de integridad, confidencialidad y autenticación.

Proceso de votación telemática:

El votante se identifica ante una mesa electoral virtual –MEV- (una dirección de Internet) mediante un certificado electrónico que incorpora una firma digital reconocida que se encuentra guardado en una tarjeta inteligente. Esta MEV le identifica ante el sistema y comprueba que está censado, permitiendo al votante continuar para emitir su voto. El votante escoge su voto y lo envía a la urna electrónica. Cuando finaliza la votación, se descifran los votos, se cuentan y se hace público el resultado.

La firma digital proporciona autenticación y el voto debe ser secreto o anónimo.

Para los servicios de anonimato son de utilidad los mecanismos criptográficos antes referidos además de otros específicos, donde el más importante es la firma opaca o firma ciega (ideada por el criptógrafo estadounidense David Chaum).

Aparte de las anteriores surgen nuevas complicaciones por el hecho de estar conectados a Internet. Los atacantes maliciosos son una amenaza importante en las votaciones telemáticas. Ataques que pueden alterar o

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

destruir el voto sin rastro de que se haya producido un ataque, el cifrado deja de tener sentido cuando virus, gusanos o troyanos actúan antes de que el usuario cifre su voto. Los ataques de denegación de servicio pueden dejar el sitio web de la elección inutilizable, virus cada vez más sofisticados pueden infectar los ordenadores de los usuarios el día de las elecciones impidiendo la votación o manipulando los resultados. El problema es que el protocolo TCP/IP sobre el que funciona Internet no se pensó desde el punto de vista de la seguridad y por tanto Internet no es una red segura.

CONCLUSIONES

1. La votación electrónica entraña riesgos de seguridad y fiabilidad. La maquinas de votación electrónica deberían poder ser auditadas hasta la última línea de código, para ello es necesario utilizar software libre o de código abierto y no software propietario como ocurre en la actualidad. El principal problema es que el análisis de código es complejo y es imposible garantizar su fiabilidad al 100%. Por tanto la utilización del software libre es condición necesaria pero no suficiente.

   > *En la "FAQ about the GNU GPL" aparece: "Fíjense, sin embargo, en que votar es un caso muy especial. Sólo porque el software dentro de un ordenador sea libre no significa que se pueda confiar en el ordenador para votar. Nosotros creemos que no se puede confiar en los ordenadores para votar. Votar debería hacerse en papel."*

2. La votación a través de redes telemáticas aporta mas complejidad al sistema electoral y por lo tanto mas riesgos, además de crear

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es

desigualdades sociales. Pero es necesario desarrollar este tipo de tecnologías por que son necesarias si queremos avanzar en el modelo de participación ciudadana a través de Internet.

3. El sistema de voto perfecto no existe, pero si se quiere implementar un sistema de voto electrónico, debe de existir una colaboración entre la Administración, los fabricantes, los expertos en informática, en derecho e incluso los propios ciudadanos, para entre todos delimitar los riesgos contra los que sería necesario protegernos, y crear unos estándares que permitan certificar los sistemas de voto electrónico.

Zaragoza, 22 de enero de 2008.

Palacio de la Aljafería – Calle de los Diputados, s/n– 50004 ZARAGOZA
Teléfono 976 28 97 15 - Fax 976 28 96 65
fundacion@fundacionmgimenezabad.es