Voto Electrónico y Software Libre

Juan Antonio Martínez Castaño
E-mail: *jonsito@teleline.es*
Web: *http://www.dit.upm.es/~jantonio*
v1.2, Agosto 2000

Internet ya forma parte de nuestro mundo. Comunicaciones, Negocios, Documentación, Revistas, Trámites bancarios, y gestión administrativa, poco a poco van siendo proporcionados a través de la red. En este ensayo vamos a tratar un nuevo aspecto del *e-world*: la democracia electrónica y los sistemas de votación a través de la red

Índice General

Índice de Figuras

1 Copyright. Registro de cambios

1.1 Registro de cambios del documento

18-Octubre-2000

Revisión final

24-Agosto-2000

Inclusión de capítulos sobre estructura de los servidores de voto

27-Julio-2000

Reelaboración para envío al CFP del Congreso Hispalinux 2000

10-Julio-2000

Traslación a SGML y conversión a ensayo

7-Julio-2000

Versión original. Artículo Enviado a Prensa Técnica para su publicación

2 Introducción

En un primer momento pudiera pensarse que en el mundo electrónico la toma de decisiones es de lo más sencillo: no es sino una lista de votantes , una lista de opciones y un contador... nada más fácil. Cualquier alumno de primero de Informática sabría realizar un programa de voto electrónico

En cierto modo tienen razón. Un programa de voto no es sino dos arrays, uno de opciones, y otro de votantes, y un mecanismo para incrementar en uno el contador asociado a cada opción. Pero como casi siempre, la sencillez es sólo aparente. Si buscamos en Internet programas de voto electrónico, nos encontraremos con una sorpresa: Sólo existen programas de encuestas, no existiendo casi ninguno sobre votaciones

Porque el código del contador es el menor de los problemas. En este ensayo vamos a tratar la problemática asociada al voto electrónico, analizando punto por punto los diversos aspectos, viendo cómo el software libre puede ser una herramienta imprescidible para el voto electrónico. Por último analizaremos diversos programas de encuestas y de votación basados en software libre, haciendo especial hincapié en el programa ***Free-Vote***, desarrollado por el autor de este ensayo

Y para tratar un tema como la democracia electrónica no hay mejor camino que partír de nuestra Constitución Española, donde se describe el mecanismo de votación como "*Sufragio Universal, Libre, Directo, Igual y Secreto*"

3 Universal

3.1 Tipos de votación en funcion del universo de votantes

Al decir *Sufragio Universal* estamos indicando que todos aquellos implicados en la toma de una decisión tienen voz y parte en la toma de la decisión. Universal se toma en el sentido sociológico de la palabra: aquellas personas que se ven implicadas. Esto ilustra una primera división en la tipología de las votaciones:

Votación pública

Es aquella en la que todo el mundo puede -si quiere- participar.

Votación privada

Aquella en la que el universo de votantes está definido de antemano

3.2 Problemática asociada a la elaboración del censo

¿Cómo se define el universo de votantes?. Entramos en el primer punto conflictivo de la Democracia Electrónica: La elaboración del Censo Electoral. En efecto. La elaboración de una lista de votantes conlleva una serie de problemas legales, que detallamos a continuación:

- No es posible recurrir a sistemas de *cookies* para elaborar listas de votantes: en el caso de una votación pública, el sistema no nos garantiza la unicidad y autenticidad del voto, ni del votante, y en el caso de una votación privada sigue siendo necesario tener una lista de votantes
- Por consiguiente no tenemos más remedio que acudir a un sistema de bases de datos. Esta base de datos debe tener suficientes elementos como para definir de forma unívoca al votante. Al menos serán necesarios:
  - Nombre, apellidos
  - Dirección, E-mail
  - Número de identificación, contraseña
- La reglamentación española obliga a que una base de datos de estas características esté registrada en la Agencia de Protección de Datos, y que cumpla con la reglamentación correspondiente al nivel Básico. La primera condición legal para un sistema de voto Electrónico es pues su inscripción y reconocimiento oficial
- El criterio de universalidad se cumple en el caso de una votación privada: en ella es el organizador quien define a priori la lista de votantes. En el caso de consultas públicas deben proporcionarse:
  - Información y publicidad para que la consulta sea conocida
  - Medios para que aquellas personas que deseen participar puedan inscribirse en dicha consulta
  - Adicionalmente, la *Ley Orgánica sobre Tratamiento Automatizado de Datos*, (LORTAD) obliga a que el sistema provea diversos medios para que los particulares puedan conocer, modificar y cancelar los datos, y conlleva una serie de reglamentaciones y procedimientos sobre la cesión de los datos

3.3 Implicaciones legales del mantenimiento del censo electoral

De lo escrito anteriormente, deducimos que de una simple lista de votantes, hemos acabado en un sistema completo de bases de datos, con una serie de requerimientos legales !y esto no es más que el comienzo!. Vamos a extendernos un momento en este tema:

Podemos entender el derecho a la intimidad (privacidad) como un derecho a ser "dejado solo o en paz" en la esfera personal y privada. En el ámbito informático, debido a la capacidad de los ordenadores para almacenar y procesar datos, es necesario redefinir este derecho, de la siguiente manera:

1. Derecho a recibir información sobre la existencia de las bases de datos que hayan sido creadas, o se vayan a crear, su finalidad, contenidos, responsables, posibles cesiones, y por supuesto; a conocer los datos relativos a la persona y la posibilidad de rectificarlos en caso de error
2. Derecho de acceso a los datos referidos a la persona, para verificar, subsanar o suprimir los datos erróneos, inexactos o caducados
3. Derecho a impedir y prohibir la recogida, registro o grabación, conservación, extracción, utilización, comunicación, manipulación y procesamiento de los datos considerados sensibles: ideologías, creencias, salud, vida sexual, y demás datos que deben permanecer secretos. Del mismo modo , derecho a impedir la recogida de datos que no cumpla las prescripciones legales, o sin consentimiento libre, expreso y consciente del interesado
4. Derecho a la protección frente al uso indebido de estos datos
5. Derecho a la irrenunciabilidad sobre estos derechos

El derecho a la intimidad es un derecho fundamental reconocido en nuestra constitución. En su artículo 18, recoge dicho derecho así como sienta la base legal para la protección de datos personales del tratamiento informáticos. En su artículo 20 marca los límites de la libertad de información, y en su artículo 120 garantiza la el acceso a los datos de titularidad pública

El Código Civil define el concepto de intimidad, su alcance, usos aceptables de la información, y cuando constituye un abuso, así como su responsabilidad jurídica y en su caso penal

La Ley Orgánica de Tratamiento Automatizado de Datos, es el actual marco legal donde se regulan las bases de datos, gestión, funcionamiento, toma de datos, etc. Esta ley ha ido adaptandose progresivamente a las diversas directivas de la Unión Europea. Establece además las normas y entes reguladores de los derechos y deberes asociados al tratamiento informático de datos. Podemos afirmar, no sin orgullo, que la legislación española sobre bases de datos es de las más avanzadas y completas de Europa

3.3.1 Ley Orgánica de Tratamiento Automatizado de Datos (LORTAD)

Los datos de carácter personal pertenecen en exclusiva a la persona que los detenta. Si se recopilan, tendrá que ser con su consentimiento y conocimiento de quién, cómo y para qué lo hace, y en todo caso, debe poder corregirlos y modificarlos. Si son datos sanitarios, se reforzará su confidencialidad. Deberán establecerse limitaciones a los archivos policiales. La importancia de la protección de datos de carácter personal, viene impuesta por que supone una intromisión en la esfera íntima, familiar y confidencial, y porque agrupando todos los datos se puede saber el perfil de una persona, su comportamiento y tendencias políticas.

La LORTAD en su exposición de motivos, sensibiliza sobre la facilidad de captura de datos de carácter personal, que con las modernas tecnologías y su posible tratamiento, dan lugar a la recolección e identificación del perfil personal, constituyendo una violación del derecho a a la intimidad. Por ello la ley permite la impugnación de valoraciones que se deduzcan solo y exclusivamente de un tratamiento automatizado de datos.

Se contempla el hecho de la cesión y compartición de datos, agravado por el hecho de que las modernas técnicas de comunicación, InterNet, etc, están multiplicando el número de registros personales y favoreciendo el entrecruzamiento de datos

Se identifican y clasifican los diversos datos personales, diferenciandolos entre identificativos, sensibles, ultra-sensibles, y definiendo diversos protocolos de actuación y restricciones respecto de cada tipo de datos

Se protege y garantiza el derecho al acceso, cancelación y rectificación. Se establecen estatutos especiales para ficheros específicos, como puedan ser los de dominio público (registros mercantiles o de la propiedad), ficheros policiales, censo electoral, Registro Civil, etc, y se preveen leyes adicionales reguladoras de estos ficheros

Se discrimina entre ficheros de titularidad pública y privada, regímenes que se deben aplicar a cada uno. Se define la figura del responsable del fichero de datos, atribuciones y responsabilidades

La cesión de datos entre ficheros está también regulada. Se establece la obligatoriedad de que los propietarios de los datos conozcan los términos en que se lleva a cabo dicha cesión, y la obligación de notificación de la cesión de los datos a la autoridad competente

Se define la figura de la Agencia de Protección de Datos, como organismo garante de los derechos y libertades relacionados con la protección de datos. Se establece la potestad de la administración para poder proceder legal y en su caso penalmente contra las infracciones a esta ley

Por último se trata el intercambio de ficheros entre entes de diversos países, las normas de derecho internacional que deben aplicarse, y los diversos convenios existentes

3.3.2 Agencia de Protección de Datos

La figura de la Agencia de Protección de Datos es definida, pero no desarrollada en la LORTAD. Para ello se definen una serie de reglamentos adicionales. Las atribuciones de la agencia son:

- Velar por el cumplimiento de la legislación sobre control de datos
- Emitir las autorizaciones e inscripciones de Bases de Datos de carácter personal
- Dictar los reglamentos de actuación y aplicación de las leyes
- Atender las peticiones, reclamaciones, y solicitudes de información
- Ordenar la cancelación de ficheros
- Informar de los preceptos y leyes de aplicación en su campo
- Potestad sancionadora ante infracciones de la ley
- Recabar de los responsables de ficheros información y ayuda sobre los datos que obren en su poder
- Mantener un registro público de bases de datos inscritas
- Elaborar memorias e informes para el Ministerio de Justicia
- Potestad para proceder a realizar inspecciones

La legislación contempla además el régimen jurídico de la APD, sus relaciones con la Administración del Estado y Autonómica, presupuestos, gobierno y administración, y personalidad y potestad jurídica y sancionadora

Además, se han elaborado diversos decretos que concretan y especifican detalles sobre:

- Estatuto de la Agencia de Protección de Datos
- Reglamento de seguridad de la LORTAD
- Diversas directivas europeas, incorporadas a nuestra legislación

3.3.3 Aplicación de la LORTAD a las bases de datos de un sistema de voto electrónico

De la lectura y estudio de los reglamentos mencionados, se deduce que un sistema de voto electrónico entra de lleno en el ámbito de aplicación de estas leyes.

En primer lugar es preciso realizar un inciso: La LORTAD establece que el censo electoral y el Registro del Censo son excepciones a la aplicación de la ley, y que tienen regulación propia. En efecto, su cesión, publicación, y registro están regulados por la Ley Electoral, que tiene carácter de Ley Orgánica.

Nuestro fichero, por el contrario sí está regido por dicha ley. El contenido y alcance de los datos viene definido por la finalidad. En el caso de un sistema de voto, la finalidad es la identificación unívoca del votante. Por ello, solo son requeridos datos con categoría de identificativos.

El reglamento de seguridad de la LORTAD, y su aplicación a los datos de caracter identificativo obliga a una serie de procedimientos:

- El primero y más importante es el de *registro*. La Agencia de protección de datos facilita enormemente la tarea, distribuyendo los formularios y permitiendo la inscripción -gratuíta- a través de InterNet
- Se establecen protocolos de actuación, que nos obligarán -entre otros- a:
  - Codificar contraseñas
  - Establecer protocolos de backup y recuperación
  - Tener un registro de incidencias
  - Proporcionar a los electores procedimientos de consulta, modificación, verificación y cancelación de datos
  - Poseer un manual de procedimientos
  - Tener unas condiciones mínimas de provacidad y seguridad
  - Definir a los responsables y sus responsabilidades
- Puesto que los datos son de caracter meramente identificativos, sólo es necesaria la aplicación de medidas de seguridad de nivel básico, tal y como están definidas en el reglamento
- El usuario debe tener en todo momento conocimiento de la existencia de la base de datos, y de sus derechos y deberes
- Un censo electoral para fines particulares es de caracter privado. No hay necesidad de cesión a terceros, y tal hecho debe constar en la inscripción en la APD. Es sancionable la cesión de estos datos a terceros, salvo en los supuestos contemplados por la ley (requerimiento judicial, etc)

3.3.4 La nueva legislación sobre protección de datos

De conformidad con las directivas de la Unión Europea, han surgido diversas ampliaciones y modificaciones a la LORTAD. El texto, reglamentos y directivas, han sido refundidos en un nuevo texto, con carácter de Ley Orgánica denominado **Ley de Protección de Datos**

El nuevo texto amplía y profundiza en las atribuciones de la Agencia de Protección de datos, Desarrolla el concepto de Fichero de Datos a los sistemas de bases de datos distribuídas y directorios de índices y sistemas de búsqueda. Determina y clarifica el concepto de uso público y privado de una base de datos

En general, la nueva ley armoniza la legislación española con el resto de la Unión Europea, de manera que las leyes sean idénticas en todos los países miembros

4 Libre

El concepto de Libertad en el ejercicio de la democracia electrónica tiene varias facetas:

- Libertad para el *ejercicio* del voto
- Libertad para la *orientación* del voto
- Libertad de Información antes, durante, y despues del ejercicio del voto

En lenguaje llano, debemos poder escoger *qué* votar, *cómo* votar, e incluso si *queremos* votar, y por supuesto, estar en todo momento en posesión de toda la información necesaria

Traducido ésto al lenguaje informático tenemos lo siguiente:

4.1 Libertad para el *ejercicio* del voto

No deben existir restricciones al acceso al sistema de votación: si para votar necesitamos el software "XXXX" o el sistema operativo "XXindows YYY", dicho sistema o dicho software deben ser *libres y gratuítos*. Si utilizamos un protocolo dado dicho protocolo debe ser público. En el caso de usar el Web, el sistema de voto debe ser *independiente del navegador* y no utilizar extensiones no públicas. No pueden existir restricciones físicas o lógicas que impidan, por ejemplo a una persona discapacitada sensorial, ejercer su derecho

4.2 Libertad de Información antes, durante, y despues del ejercicio del voto

El ejercicio de la libertad de opción nos lleva a que debe poder conocerse a priori las cuestiones consultadas, las opciones de elección, la metodología de voto, y los presupuestos e implicaciones de cada opción posible en una consulta dada. Es muy común que los sistemas de consulta electrónica lleven asociado un tablero o foro de discusión, donde los votantes potenciales, dialogan y disciernen sobre las diversas posibilidades

4.3 Libertad para la *orientación* del voto

Por último, el ejercicio de la libertad de voto conlleva el de la *no obligatoriedad*. No son admisibles "votos por omisión", o valores por defecto en la lista de opciones

4.4 Implicaciones del ejercicio de la libertad en los programas de voto electrónico

Todos estos condicionantes nos llevan a una serie de requerimientos sobre el software:

- Utilización de *Software Libre* en *Sistemas Operativos Libres*, basando el programa en *Protocolos Abiertos* y *Estándares Públicos*
- El sistema no debe imponer restricciones al votante: debe funcionar en cualquier plataforma y sistema, con o sin capacidades gráficas o sonoras. En el caso de usar el Web, debe ser independiente del navegador o de los *plug-ins* instalados

- Deben de proveerse mecanismos de información y de feedback al votante: Foros de discusión, uso intensivo del correo electrónico

Un detalle que no debemos olvidar en cuanto al concepto de Libertad: El usuario debe ser libre también para poder escoger si lo desea otros mecanismos para ejercer el voto... por mucho que estemos en la era digital, el correo certificado existe todavía...

Bueno, ya no sólo tenemos una base de datos: tenemos un sistema que tiene que estar basado en estándares abiertos, independiente de plataforma y sistema, con un sistema completo de comunicación entre el votante y el organizador de la encuesta. Ahora viene lo difícil...

5 Directo

La palabra *Directo* conlleva

- La no existencia de delegación del voto
- La implicación personal del votante en el proceso de votación

Se plantea el problema de la *Autentificación* del voto y del votante. Debemos garantizar que quien vota es quien dice ser, que no existen problemas de "suplantación de personalidad", y que cuando el votante ejerce su derecho, éste se lleva a cabo.

5.1 El problema de la autentificación

En lenguaje informático tenemos cuatro problemas diferenciados:

1. La autentificación y certificación de la máquina desde la que opera el votante
2. La autentificación y certificación del servidor o servidores del sistema de votación
3. La identificación del votante
4. La verificación del sistema de voto

5.2 Procedimientos de identificación del votante

Dejaremos el último punto para el próximo capítulo. Los tres primeros corresponden a los conocidos problemas de certificación, comunes en los sistemas de comercio electrónico. Tenemos diversas alternativas:

- La primera, y que se debe rechazar sin dudarlo un momento es el uso de sistemas de *cookies* para proceder a la identificación. La naturaleza de este método (un sistema de marcas que el servidor deja en el cliente para una posterior identificación y seguimiento) lo hace inviable para nuestra aplicación. No es posible fiarse de la máquina cliente para proceder a la identificación de un votante. Las *cookies* se copian, borran, modifican, etc, sin ningún control por parte del servidor. Es garantía segura de impugnación de voto
- Un procedimiento mejorado, implica el uso de claves por parte del usuario. En este caso, es responsabilidad del votante, mantener un sistema de claves para:
  - Registrarse en el sistema de voto
  - Proceder al ejercicio del voto

Diferenciamos estos dos procesos porque corresponden a operaciones distintas. En la primera el usuario se identifica ante la base de datos. Corresponde al punto de acceso al sistema. El segundo caso es cuando el votante quiere ejercer su derecho al voto y así lo manifiesta: el sistema le proporciona medios adicionales para ello.
Uno puede preguntarse la necesidad de esta disociación. Tiene dos motivos: El primero es de organización. Son operaciones diferenciadas. El segundo es de seguridad adicional: es perfectamente posible que el sistema mantenga diversas consultas simultáneas, y debe independizarse en lo posible cada una de ellas, de manera que el votante expresamente decida dónde, como y cuando participar en cada una de ellas (recordemos el principio de libertad)

- Podríamos utilizar un sistema de cookies para, una vez autentificado el usuario, que éste acceda libremente al sistema de voto. Esto no es recomendable, pues recordemos que el protocolo HTML es sin estado, y no tiene el concepto de *sesión*, con lo que se podrían falsificar las cookies, o en el caso de que el usuario abandonara el equipo, alguien usurpara su puesto. Por otro lado, el sistema de doble clave permite separar el proceso de solicitud del derecho al ejercicio del voto, a su realización efectiva, lo que puede tener ventajas en ciertos casos (por ejemplo, cuando es necesario lograr un quorum para poder votar)
- El tercer nivel de seguridad está basado en el uso de protocolos encriptados y de agentes de certificación. Con el primero, garantizamos el secreto, tanto de las claves como de los diversos datos de la consulta y del usuario. Con el segundo, autentificamos y certificamos de una manera segura y fiable, el origen, destino y personalidad de los participantes

Casi todos los sistemas de consulta electrónica existentes en la actualidad están basados en el uso de *cookies*. No son válidos mas que para encuestas, sondeos de opinión, etc. Unos pocos se basan en sistemas de claves, pero sólo para autentificar al votante. El programa desarrollado por el autor lleva el sistema de doble clave para identificación y derecho al voto.

Las claves se comunican al usuario mediante correo electrónico. En función del sistema se utilizaran o no mensajes encriptados, siendo común el uso de **PGP** para su encriptación

No he encontrado todavía ningún sistema de voto electrónico que utilize sistemas de certificación electrónica. Realmente debería ser un requisito imprescindible para un sistema de voto, pues es el único capaz de certificar y autentificar completamente a un usuario.

Hay que tener en cuenta que el voto electrónico es una suerte de transacción electrónica. La legislación española contempla el uso de firmas y certificados digitales, por lo que un sistema basado en éstas sería completamente válido y legal.

Como resultado de éste análisis, tenemos ahora también un sistema basado en certificados digitales, con realimentación al usuario mediante correo electrónico encriptado, y con sistemas de doble clave para registro y emisión de voto.... Los lectores que hayan hecho la Declaración de la Renta 1999 por Internet sabrán del engorro que significa el procedimiento de obtención de certificados digitales.... y sin embargo no es sino lo que hacemos cuando presentamos el Documento de Identidad ante la mesa electoral: garantizar que somos nosotros y no otro quien vota. La normativa Española es de las más avanzadas de Europa en cuanto aceptación de firmas digitales, siendo de las pocas que permite que ciertos trámites administrativos puedan realizarse a través del Web. En este caso, el voto viene a ser un trámite más.

La figura ilustra un esquema de autentificación basado en certificación digital. Básicamente los pasos son:

- Cuando el servidor desea proceder a la comunicación encriptada y certificada ante sus clientes, primero debe proceder a autentificarse en una autoridad reconocida de certificación. Dicha autoridad signa con su clave privada la clave pública del servidor
- El servidor, cuando desea enviar un mensaje a un cliente, lo signa con su clave privada, y le acompaña de la certificación digital recibida de la autoridad

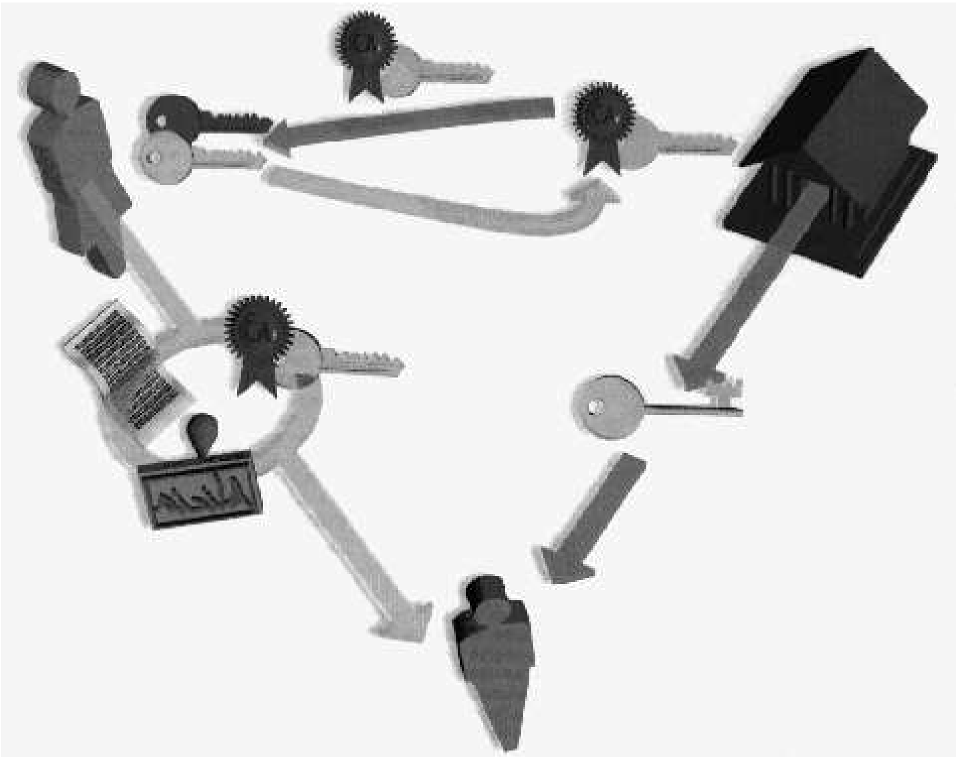

Figura 1: Sistemas de certificación digital

- El cliente recibe el mensaje y la firma digital. Autentifica la firma a través de la clave pública de la autoridad de certificación, obteniento entonces la clave pública certificada del servidor, y utilizandoésta para desencriptar el mensaje del servidor
- El procedimiento reciproco se utiliza por parte del servidor para autentificar los mensajes que el cliente le envíe

6 Igual y Secreto

6.1 El problema de la *Confiabilidad*

"*Igual y Secreto*". Estas dos palabras introducen el concepto de la *Fiabilidad* y la *Confiabilidad* en el sistema de votación.

- ¿Cómo puede saber un votante, que no hay "pucherazo electrónico"?
- ¿Cómo puede el votante tener garantía de que su voto es realmente secreto?
- ¿Qué mecanismos de supervisión se pueden poner en marcha?
- ¿Qué ventajas nos aporta el software libre respecto al tema de la confiabilidad?
- ¿Qué sistemas se pueden implementar para evitar pucherazos intencionados o no?
- Ante caídas del sistema, ¿cómo puedo recuperar el estado anterior para que la votación no quede invalidada?
- ¿Hasta que punto el sistema es fiable, y resistente a ataques?

- ¿Es el servidor de voto seguro? ¿Cómo garantizar un ª prueba de Hackers"?

Por un sistema *Confiable* entendemos aquel en el que no se hace trampas, en el que se garantiza que el sistema funciona sólamente como se prevee que va a funcionar, sin puertas traseras ni trampas ocultas que modifiquen los resultados

Por otro lado un sistema *Fiable* es aquel sistema que es capaz de funcionar en condiciones adversas, que se recupera ante fallos, que incorpora mecanismos de seguridad específicos...

Son las dos caras de la moneda del proceso de identificación, recuento y verificación de resultados.

6.2 Control de la confiabilidad en el sistema de voto tradicional

Para ponernos en antecedentes, repasemos el proceso de recuento de votos en un sistema tradicional:

1. En la mesa existen presidente, secretario y dos vocales
2. Además cada partido político nombra a discrección diversos interventores en cada mesa
3. El usuario una vez autentificado y emitido el voto, queda registrado de manera que no puede volver a votar
4. La urna garantiza el anonimato del voto
5. El recuento se hace en vista pública
6. El registro y acta de la votación se hace por triplicado, enviándose los datos al Centro de Proceso de datos por teléfono, y por correo certificado. Una de las copias del acta se lleva a la Junta Electoral de Zona, para ser utilizada en caso de discrepancias
7. La introducción de datos se realiza por duplicado. Cada operador del centro de proceso de datos recibe una copia del acta, de manera que sólo se contabilizan las actas cuando dos operadores introducen los mismos datos referidos a la misma mesa. En caso de discrepancias, un sistema de alarma hace entrar en juego al supervisor que contrasta los datos con la segunda copia del acta. En caso de dudas se acude a la junta electoral de zona, para cotejar con el tercer acta
8. El ordenador está permanentemente supervisado y mantenido en previsión de posibles caídas. El sistema de presentación de información es totalmente independiente del de conteo, de manera que en caso de caída de uno, -o de ataque- el otro no se ve afectado
9. Por supuesto, un sistema de consultoría y certificación externa dependiente de la Junta Electoral Central garantiza que el ordenador hace lo que debe...

6.3 La confiabilidad en un sistema informático de voto

Vamos a trasladar ésto al mundo electrónico. Para ello vamos a identificar y tratar cada uno de los problemas por separado. El proceso de autentificación fue tratado en el apartado anterior, por lo que no lo comentaremos más.

6.3.1 El secreto del voto

El concepto de *Secreto* del voto tiene varios aspectos:

- Secreto en las comunicaciones

- Secreto en la contabilidad
- Secreto en la información de datos parciales

Hemos visto que una adecuada encriptación oculta las comunicaciones. No obstante, aún es posible una mejora adicional: la fragmentación de la información. No es lo mismo que circule un mensaje que diga "José López vota SI a la supresión de los exámenes de Septiembre" que decir "El usuario 34 escoge la opción 2 de la consulta 14". En el primer caso basta con descifrar un mensaje; en el segundo hacen falta descifrar al menos cuatro.

El mejor método para asegurar el secreto de la contabilidad es que ésta no exista. Para ello las tarjetas de voto de cada usuario, solo deben contener campos que digan si el usuario ha solicitado o no el voto, y si éste ha sido emitido o no (opcionalmente, la fecha de emisión). Del mismo modo cada opción de la consulta no almacena datos individuales, sino un contador. Los resultados son evaluados a la vez que se generan, no a posteriori.

Un último punto en este apartado lo representa, los aspectos de *visibilidad* de resultados parciales: en función de la votación, puede ser conveniente o no, presentar datos de participación, resultados parciales, porcentajes, etc El sistema debe ser capaz de proporcionar esta flexibilidad a la hora de la elaboración de consultas

6.3.2 La seguridad (fiabilidad) del sistema

El concepto de *Seguridad* lo medimos en:

- La protección del sistema frente a ataques externos
- La protección frente a caídas o fallos en el software o en el equipo
- La protección frente a manipulación por parte del administrador

Puesto que trabajamos con un sistema que utiliza una serie de bases de datos, y dado que dicha base de datos está sujeta a una serie de requerimientos legales en base a la LORTAD, estos puntos son de obligado cumplimiento. Especialmente severa es la LORTAD en cuanto al papel y actuación del responsable del sistema y las sanciones por inclumplimiento de las normas establecidas. Entre estas, podemos citar la obligatoriedad de existencia de protocolos de actuación, sistemas de encriptación, mecanismos de backup y recuperación, registro de incidencias, etc. Todo esto está reglamentado y documentado en los en los reglamentos de aplicación de la LORTAD, y su correcta aplicación permiten confiar -hasta cierto punto- en el administrador. Realmente haría falta una "Autoridad de emisión de consultas", al igual que existe una "Autoridad de emisión de certificados digitales"

6.3.3 La verificabilidad del sistema

El concepto de *Verificabilidad* incluye los puntos:

- Acceso al código fuente del sistema de voto
- Acceso a los registros de funcionamiento
- Obtención de certificados de autenticidad por parte de terceros
- Existencia de procedimientos de log que permitan resolver dudas e impugnaciones, manteniendo el carácter de secreto del voto

Estos puntos garantizan que el votante puede conocer en todo momento, qué hace, y como funciona el sistema. Para ello debe tener algún mecanismo adicional que le garantice que su código corresponde a su binario, bien mediante firma digital, bien mediante acta notarial, o incluso mediante sistemas de acceso directo al código del servidor

Los sistemas de registro y *logging* deben conjugar el registro de operaciones e incidencias, con el secreto del voto. Es admisible registrar que un usuario votó en un momento dado pero no lo es registrar su voto

6.4 Software libre como medio ideal para generar sistemas confiables

El uso de software Libre proporciona el medio ideal para poder realizar los procesos de verificabilidad: si el votante tiene acceso al código fuente, y tiene a su vez la certificación de que dicho software es efectivamente el que se está ejecutando en el servidor, los demás problemas son obviados, pues es directamente verificable en el código que éste hace lo que dice, y no otra cosa

Queda por resolver el problema del uso malintencionado del sistema. Se pueden utilizar técnicas de replicación y de doble chequeo, como las que se utilizan en los recuentos electorales actuales. De esta manera, a menos que el administrador tenga acceso a TODOS los servidores de que consta el sistema, no podrá falsificar los datos de la consulta... En la práctica suele ser más sencillo recurrir a supervisión y monitorización por parte de terceros.

Despues de leer todo este análisis, no le quedará duda al lector de que el voto electrónico es algo más que un simple contador. Está claro que en bastantes casos muchos de estos requisitos no son necesarios, e incluso pueden significar un engorro por parte de los usuarios, pero no podemos olvidar que el ejercicio de la Democracia es un derecho constitucional, que debe estar garantizado y preservado. La legislación y el sentido común obligan a todos estos condicionantes, que deben ser cumplidos para que el voto sea válido y la consulta representativa, verídica y que tenga validez ejecutiva

Una vez que nos hemos puesto tan serios, vamos a bajar al mundo real, y vamos a analizar los diversos sistemas de software libre que existen en la actualidad para el voto electrónico, así como las técnicas de certificación, encriptación, verificación, etc de que disponemos los amantes del software libre.

7 Aplicaciones de voto electrónico

Lo primero que hay que hacer constar es que no existe en la actualidad ningún software, tanto libre como propietario, que cumpla con todos los requerimientos explicitados en este ensayo para ser considerado como un sistema completo de voto electrónico. Podemos clasificar los sistemas existentes en diversas categorías:

7.1 Sistemas de toma de decisiones

Existen multitud de soluciones propietarias para el problema de la toma de decisiones. En general, estas soluciones, son módulos adicionales a programas de videoconferencia, trabajo cooperativo, etc

7.2 Sistemas de recuento de votos

Del mismo modo existen sistemas electrónicos para el proceso de conteo de resultados. Detallaremos por su "fama" dos de ellos:

- En algunos estados de USA, el voto no se efectua en una urna, sino a través de un mecanismo similar a una máquina tragaperras: El votante, una vez autentificado y autorizado su voto, accede a una cabina, en la que en dicha máquina selecciona el voto deseado, y lo emite. El recuento es automático, y al finalizar la jornada electoral se obtienen directamente los resultados

- Una empresa española ha creado un sistema de recuento automático basado en el reconocimiento del voto a través de un lector óptico. El votante inserta el voto a la manera habitual en la urna, disponiendo ésta de un lector óptico que reconoce un código de barras incorporado en la papeleta. Este sistema es actualmente propiedad del Gobierno Vasco, y está pendiente de autorización gubernamental

7.3 Sistemas de encuestas y consultas anónimas

Es muy corriente en el Software Libre la existencia de programas de consulta. Portales, como Slashdot, BarraPunto, Technocrat, etc son foros de discusión donde se proponen diversos temas de actualidad, noticias, etc. Incluyen además sistemas de encuestas, donde los participantes en los foros manifiestan su opinion sobre un tema propuesto por los editores

7.4 Sistemas de voto

Una nueva categoría constituyen los programas de voto propiamente dicho

El primer caso son aquellos sistemas simples, sin posibilidad de reconfiguración: un ejemplo lo tenemos en *MyPools* desarrollado por Josh Levine (josh@levinenet.com), basado en PHP y MySQL. En este programa, el administrador edita un fichero de configuración, donde se define la consulta y las opciones. Mediante cookies, se guardan las votaciones y sus resultados.

En general este y otros programas similares están orientados a una única votación sobre un tema concreto. El administrador es quien define los datos de la encuesta, teniendo que proceder manualmente a la mayor parte de las operaciones. El usuario no tiene ningún sistema de realimentación para recepción de claves

7.4.1 Un servidor de voto comercial: *E-Vote*

Una empresa alemana *E-Vote* ofrece diversos servicios de toma de decisiones distribuída. Para ello alquila una aplicación que actúa como cliente de sistemas Windows, y que permite conectarse a un servidor de toma de decisiones.

Dicha aplicación tiene todas las características que se esperan de un sistema de voto:

- Sistema de registro de usuarios
- Elaboración de consultas y votaciones
- Foro de discusiones
- Mecanismos de chat y videoconferencia en línea
- Planificadores de actividades

La empresa alquila el servidor a las diversas organizaciones que quieren utilizar sus herramientas de decisión. El servidor en sí mismo no se vende: solo la aplicación cliente

Se utilizan mecanismos especiales para identificar unívocamente a los usuarios, y garantizar la unicidad y secreto del voto, así como para cumplir la reglamentación europea sobre tratamiento de datos personales.

Realmente, más que un sistema de voto es un sistema de toma de decisiones, orientado a entornos de telereunión y teletrabajo.

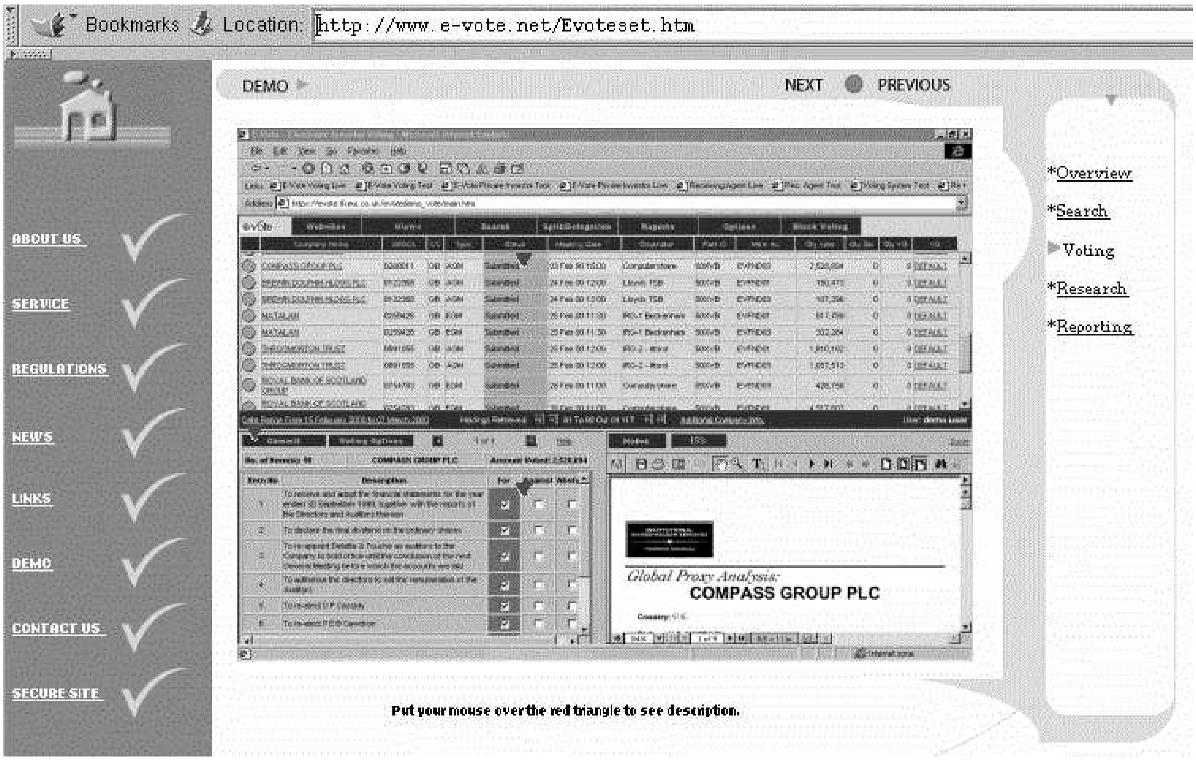

Figura 2: E-Vote, Servidor comercial de consultas electronicas

7.4.2 Ejemplo de sistema de voto: *Free-Vote*

En vista de la carencia en el mundo del software libre de este tipo de programas, el autor ha desarrollado uno que, sin tener una validez plena a efectos legales, cubre la mayor parte de los requisitos de los sistemas de voto electrónico. se trata de ***Free-Vote***

Free-Vote ha sido diseñado para servir y dar soporte a sistemas de votación electrónica con un nivel razonable de seguridad y fiabilidad. Las características principales de ***Free-Vote*** son:

Multiconsulta

Se pueden realizar y monitorizar simultáneamente varias consultas

Configurable

Cada consulta tiene diversos parámetros, definibles por el organizador de la consulta:

- Consulta pública o restringida
- Datos de consulta públicos o privados
- Foros de debate sobre las diversas consultas
- Periodos de notificación, registro, y votación
- Control de información disponible durante la consulta:
  - Acceso a listas de votantes
  - Saber si un votante ha votado o no
  - Datos sobre porcentajes de participacion
  - Datos sobre resultados parciales de la consulta
- Selección y definición de las opciones de voto

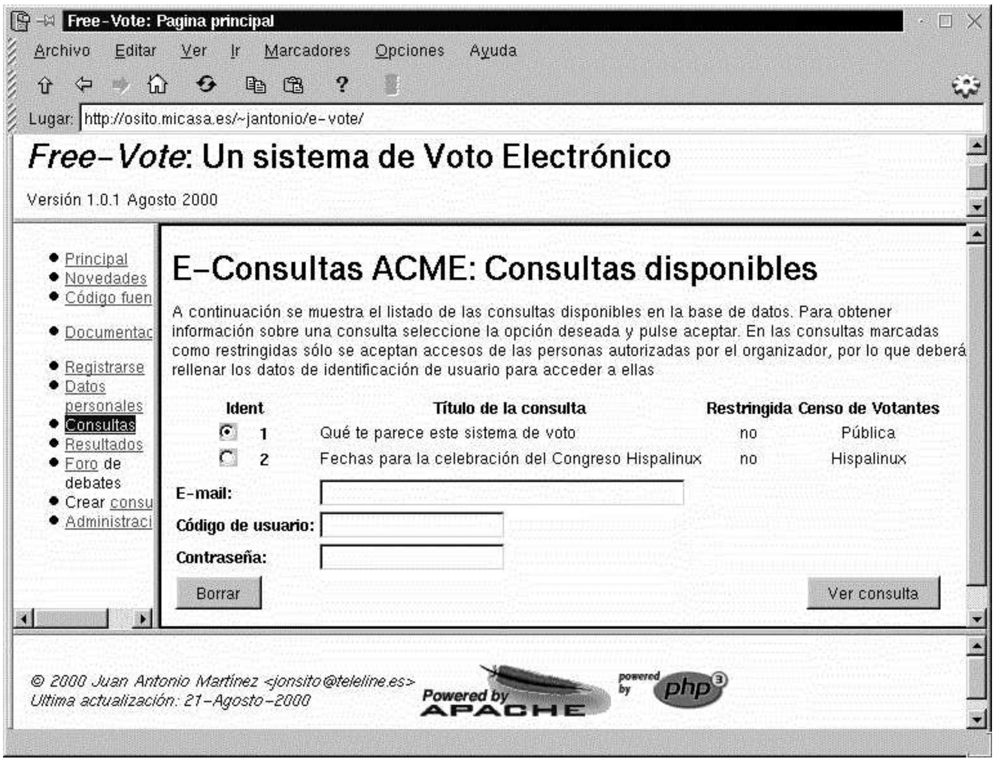

Figura 3: Free-Vote, un programa GPL de voto electronico

Autentificación de votantes

Cada votante recibe al realizar la acreditación una *tarjeta* de voto, válida una única vez

Garantía de voto único y secreto

El sistema sólo registra si el usuario ha votado o no, nunca el valor de su voto

Control de acceso

En consultas privadas sólo tienen derecho a voto aquellos votantes definidos por el organizador.

Administración distribuída

El papel del administrador, aunque importante, es secundario: existen diversas categorías de usuarios, cada uno con un nivel de privilegios definible, que permiten una administración distribuída del sistema: alta y baja de usuarios, de consultas, acceso al sistema, etc. Además, punto funtamental en cuanto a seguridad: no hacen falta privilegios de *root* para su instalación y ejecución

Documentación y procedimientos de instalación automatizados

Se proporciona una documentación completa en formato SGML, así como diversos scripts de instalación y configuración. Dicha documentación y scripts, han sido escritos de manera que sean conformes a los reglamentos de aplicación de la LORTAD

El usuario empieza por registrarse en el sistema, obteniendo una clave de acceso. Posteriormente, puede seleccionar las diversas consultas disponibles, y en función de su autorización o no puede emitir voto en aquellas en las que esté autorizado. Para ello debe solicitar una tarjeta de voto, que añade a sus datos de registro una clave adicional para proceder al voto en una votación concreta. La tarjeta de voto es única por cada usuario y cada consulta

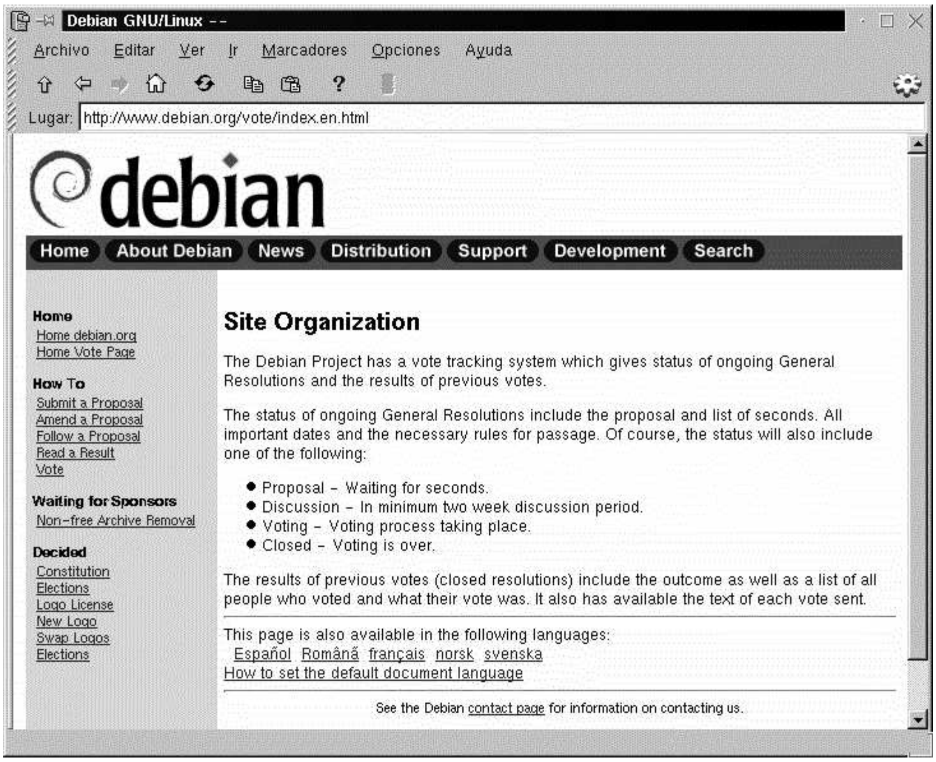

Figura 4: Vote-Debian, Sistema de voto basado en correo electónico

Si su nivel de privilegio lo permite, un usuario puede crear y definir consultas, e insertarlas en el sistema. En función del privilegio asignado podrá dar de alta usuarios, autorizar consultas, etc. El máximo nivel de privilegio otorga acceso vía Web a la consola SQL de la base de datos, lo que permite actuar de Administrador

Free-Vote Está basado en *PHP-3.0* y *PostgreSQL-7.0*. Para la elaboración de las páginas web se utiliza en aras de la compatibilidad HTML-3.0 sin extensiones adicionales. Una copia de la última versión del código fuente está disponible vía web en *http://drake.dit.upm.es/˜jantonio/e-vote/evote.tgz*. Se distribuye bajo Licencia GPL.

7.4.3 Sistemas de voto basados en correo electrónico:

El mundo del Software Libre ofrece muchas más posibilidades que el web a la hora de poder realizar aplicaciones de voto electrónico. Vamos a estudiar ahora un sistema de voto basado en el uso del correo: *Vote-Debian*

Vote Debian es un sistema enteramente basado en el correo electónico, y enteramente integrado en la filosofía de desarrollo de debian. El proceso de toma de decisión consta de las siguientes fases:

- **Propuesta** en la que se manda un mensaje a debian-vote@debian.org en la que se especifican los puntos de discusión, las motivaciones y los textos de la consulta
- **Debate** Fase en la que los participantes discuten a través del correo la propuesta, añadiendo enmiendas, o modificando los contenidos
- **Votación** Donde se procede al voto. Existen unos formularios predeterminados para la elaboración y tratamiento automatizado del voto
- **Resultados** En los que los participantes reciben los resultados de las votaciones, y se adoptan las decisiones pertinentes.

Debian Vote es un sistema de toma de decisiones orientado a decidir el funcionamiento interno del grupo de desarrolladores de Debian. Desde este punto de vista es completamente funcional, si bien, desde los aspectos tratados en este artículo tiene estas particularidades:

- No se garantiza el secreto del voto. De hecho el contenido y resultado de las votaciones es público
- La autentificación del votante se realiza vía PGP. Existe un registro previo de usuarios

Las páginas web de *Debian Vote* se encuentran en *http://vote.debian.org*

7.4.4 Sistemas de voto basados en IRC

En general, podemos observar que cualquier sistema electónico que sirva para la comunicación multipunto puede ser empleado para realizar tareas de toma de decisión. Vamos a describir someramente un posible ejemplo de realización a través del *Internet Relay Chat* (IRC o Chat)

La idea básica del voto a través de IRC consiste en la existencia de un *bot*, un usuario automático que supervisa todas las actividades relacionadas con el proceso de votación. Los bots son ampliamente utilizados en los sistemas de IRC para muchas aplicaciones. El voto electrónico no es es sino otra aplicación más

La organización es como sigue:

- Existe un canal de información *#vote_info* donde se anuncian las diversas votaciones en curso
- Existe un canal *#vote_xxxx* por cada consulta, que actua como foro de debates
- Existe un *bot* que realiza las siguientes operaciones
  - Presentación de resultados
  - Recogida de votos
  - Control de accesos
  - Registro de usuarios

  Por lo general, este bot está asociado a una base de datos, al estilo de un sistema vía web
- Para proceder a una votación el usuario debe registrarse en el canal asociado, y proceder al voto

El principal problema de este sistema es el de la autentificación del usuario: IRC está basado en aliases y "nicks", de manera que son necesarios mecanismos adicionales de identificación

7.5 Otros sistemas de voto electrónico. Consideraciones

Como hemos comentado el mundo del voto electónico no acaba aquí cualquier sistema que permita comunicación multipunto podría ser utilizado para consultas y votaciones. Citemos algunos ejemplos:

- Servidores de noticias
- Sistema de mensajería de los teléfonos móviles
- Servicios de televisión vía satélite y por cable

En general cualquier sistema que tenga una estructura cliente-servidor puede servir. No estamos restringidos en absoluto a los sistemas basados en equipos informáticos. No obstante hay que tener en cuenta una serie de consideraciones:

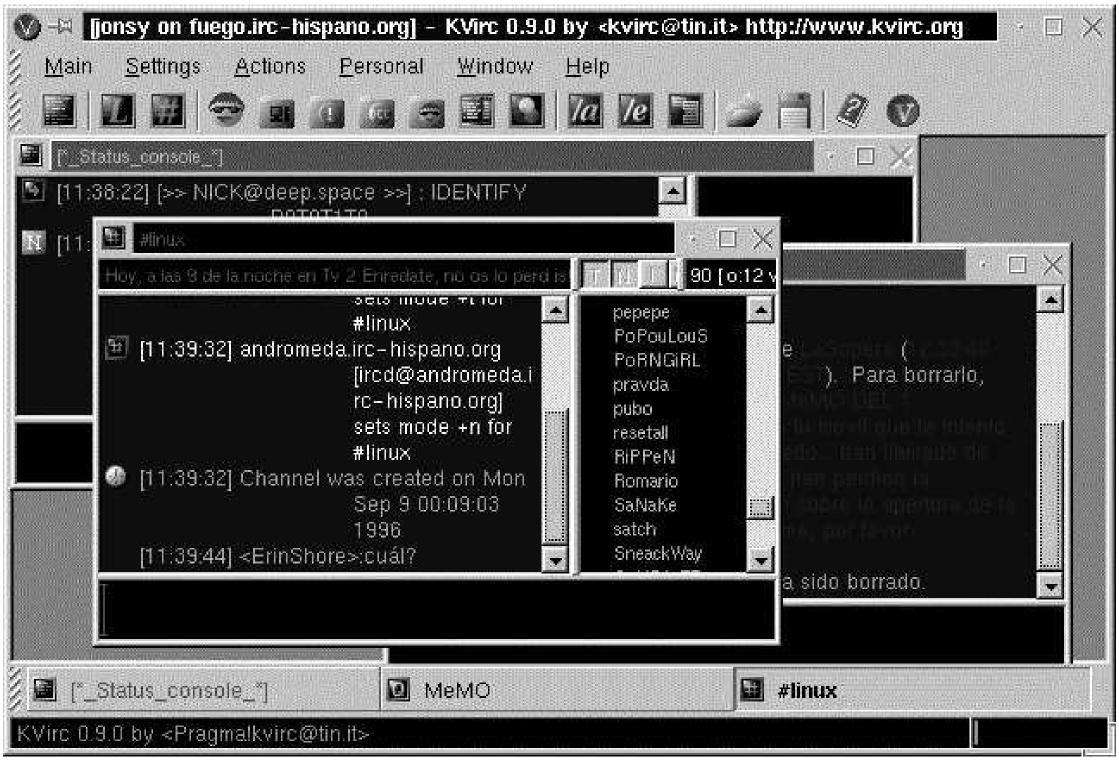

Figura 5: KvIRC, un programa de chat

- deben garantizarse las premisas que definen el voto:
  - Unicidad
  - Secreto
  - Autentificación del votante
  - Libertad de acceso y de voto

Con la tecnología actual el principal problema reside en la *autentificación del votante*. Un ejemplo sencillo: en un sistema de voto basado en mensajes de móviles, no hay garantia de que quien envíe el mensaje sea el propietario del teléfono...

No obstante, y debido a la necesidad que en éste y otros aspectos existe sobre el tema identificación, se están desarrollando diversas técnicas de autentificación: reconocimiento de voz, identificación de huellas, etc. Si bien el principal objetivo es el econónico (piénsese en la telecompra por teléfono móvil) el ámbito de actuación de estas técnicas incluye -por supuesto- el voto

Otro problema asociado a la tecnología es el de la *universalidad*: Cualquiera que sea el sistema de voto escogido, se debe poder garantizar el que todo aquel que esté interesado tenga posibilidades de participar. Es preciso un acceso universal a las tecnologías asociadas a la toma de decisiones. No puede tolerarse el que existan "no-ciudadanos"por causa de analfabetismo tecnológico, o carencia de medios o recursos económicos

El Software Libre ofrece a nuestra sociedad una vía para la universalización de las tecnologías de la información: Por sus características y licencias de uso, es accesible para todo el mundo a un coste casi nulo.

7.6 Estructura de un programa de voto electrónico

Las diversas ilustraciones que acompañan a este ensayo muestran ejemplos de los sistemas citados, y de alguna de las herramientas utilizadas

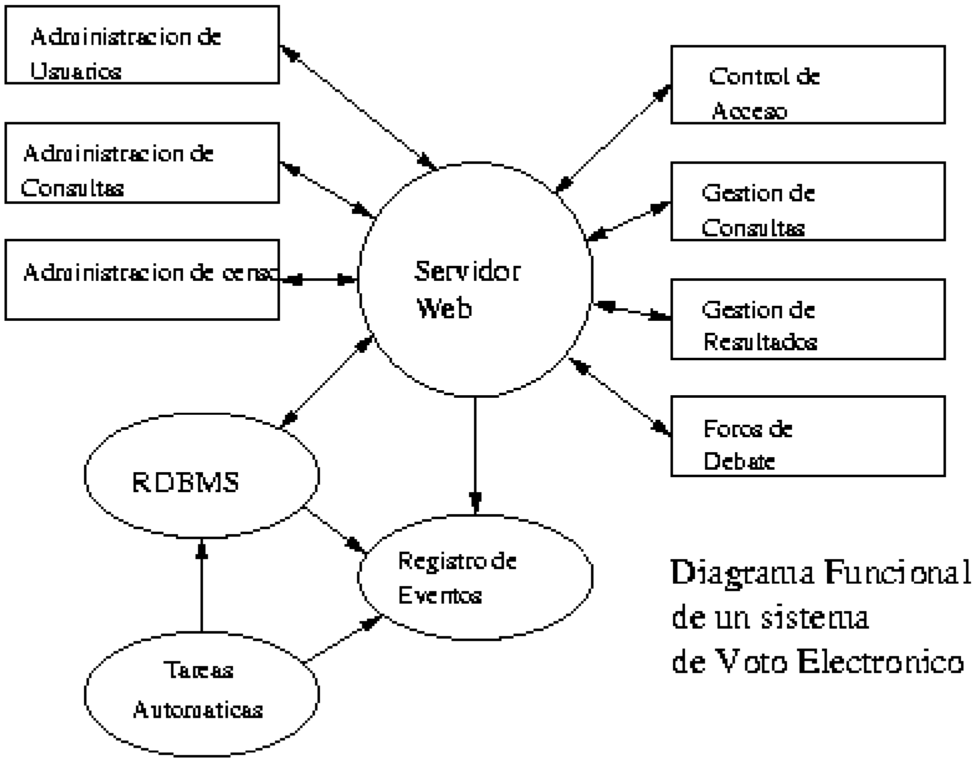

Figura 6: Diagrama funcional de un programa de voto

Básicamente, podemos descomponer el programa en diversas subestructuras:

7.6.1 Base de datos

Cualquier sistema de voto deberá tener al menos las siguientes tablas de datos:

- Registro de datos personales
- Registro de censo electoral
- Registro de votaciones
- Registro de resultados

Dichas tablas se organizan según un sistema de dependencias. La figura ilustra las dependencias entre tablas que utiliza *Free-Vote*

7.6.2 Gestión de usuarios

Deberemos tener programas para realizar las siguientes tareas:

- Registro, alta, baja, y modificación de usuarios
- Control de contraseñas, tarjeta de voto, etc
- Seguimiento, seguridad, autentificación
- Interacción con el correo electrónico

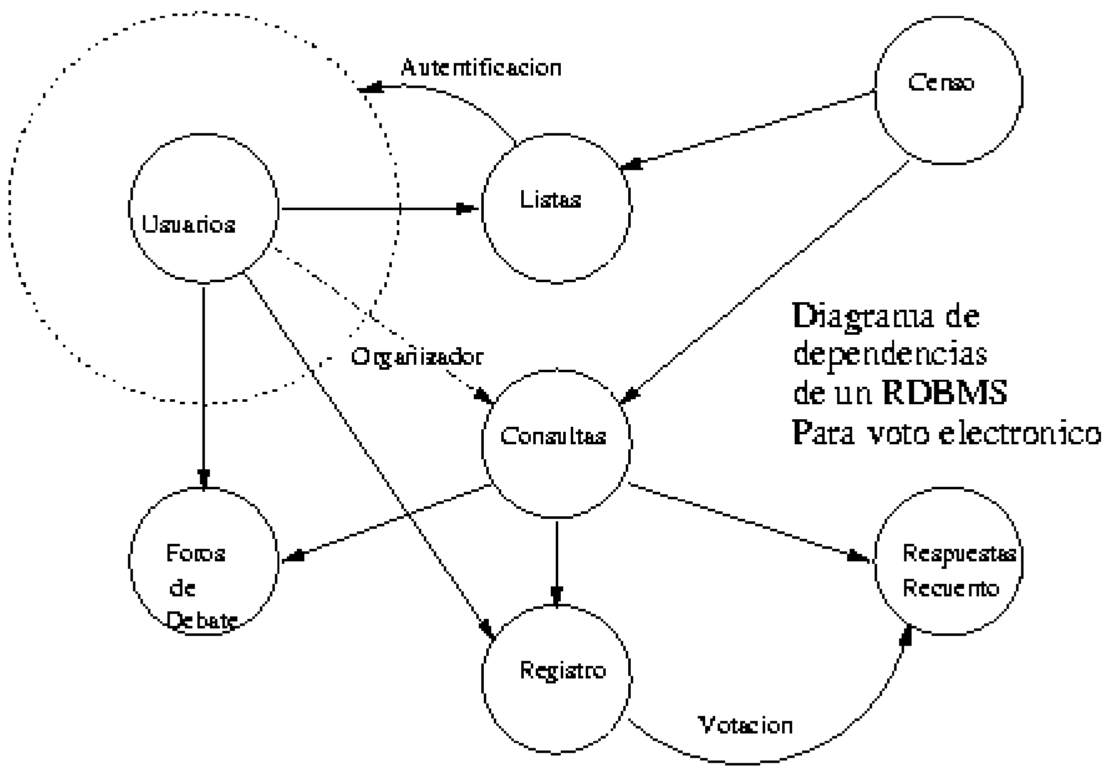

Figura 7: Estructura de la base de datos

7.6.3 Gestión de consultas

- Creación de consultas
- Validación de usuarios y votos
- Recuento de votos
- Presentación de resultados
- Persistencia de las votaciones dentro del sistema

7.6.4 Foros de debate. Chat y sistemas de comunicaciónes en línea

Es muy común la existencia de foros de debate asociados a cada consulta. En ellos, los usuarios manifiestan las diversas opiniones sobre las consultas y sus resultados:

- Gestión del foro
- Envío y recepción de mensajes

No sólo sistemas de foros son posibles. Algunos entornos incluyen sistemas de chat o de videoconferencia. Dependiendo del grado de interactividad que se pretenda, y de la complejidad del servidor, estos sistemas estarán o no presentes

7.6.5 Correo electrónico

Hemos tratado anteriormente, cómo el correo electrónico debería ser el medio principal de comunicación entre el servidor y el usuario. Lo utilizaremos para:

- Notificaciones
- Envio de datos sensibles
- En general todo tipo de información generada en el servidor, de interés para el usuario

Dependiendo del sistema, el grado de verbosidad será mayor o menor: Algunos sistemas envín información sobre consultas de manera automática; en otros es responsabilidad del organizador notificar a los interesados la existencia o incidencias relacionadas con alguna consulta.

7.6.6 Mecanismos de administración remota

Dependiendo de la complejidad del sistema, las tareas de administración serán más o menos compleja. Lo normal es que el o los administradores tengan acceso directo al servidor, y puedan realizar directamente sobre el sistema las tareas de administración

En ocasiones esto puede ser o no conveniente, por lo que algunos sistemas incorporan mecanismos de administración remota. Esto permite además definir niveles de privilegios. Podemos identificar diversas tareas de administración:

- Altas y bajas
- Modificaciones
- Gestión de recursos
- Gestión de incidencias

Por supuesto, al margen de estos sistemas, siempre existen los sistemas de gestión local, tanto automáticos como manuales.

Es necesario controlar estrictamente los recursos de administración: el responsable del sistema tiene acceso directo a las bases de datos y a su integridad y contenido. Al responsable del sistema se le asume integridad, pero nunca está de más una ayudita electrónica... chequeos, controles de integridad, registros automáticos de eventos, etc

7.7 Herramientas de software libre disponibles para programas de consulta

7.7.1 Los clientes libres

El recurso básico de un sistema libre de voto electónico es el Web: Recordemos que el principio de libertad, nos obliga a huír de soluciones que liguen a un determinado software o sistema operativo. Si bien en el servidor no es tanto problema, es una razón *sine qua non* en el cliente de voto. El uso del web y del lenguaje html es una garantía de portabilidad

Por el mismo motivo huiremos de soluciones web propietarias o no extendidas: *plug-ins*, *javascript*, *applets java*. No podemos olvidar que cualquiera, con independencia de su sistema y recursos debe poder participar En resumen, el cliente será cualquier navegador web que soporte HTML-3.2, sin extensiones

7.7.2 El lado del servidor

Aunque en el lado del servidor se dispone de más libertad, vamos a evaluar las herramientas necesarias y su disponibilidad como software libre

- En primer lugar está el servidor de bases de datos. Necesitaremos software que soporte integridad referencial, agrupamiento de transacciones, actualizaciones en cascada.... En el momento de escribir estas líneas sólo tenemos un RDBMS libre que cumpla estas condiciones: ***PostGreSQL-7.X***, distribuído bajo licencia BSD
- Necesitamos, por supuesto un servidor Web. En este caso no hay duda ninguna: Apache es nuestra elección. No solo por su carácter de software libre, sino por su seguridad y estabilidad: el 60% de los servidores Web de InterNet están basados en él. Deberemos añadir soporte para SSL (*Secure Socket Layer*), y de scripts CGI.
- Para unir el sistema Web con el servidor de bases de datos, escogeremos un lenguaje de programación de CGI's. Aquí la disponibilidad de software es mucho más variada: Perl, PHP, e incluso ejecutables compilados, bien nativos o bien servlets Java. No obstante, por su sencillez y posibilidades de acceso a bases de datos, PHP es una de las mejores elecciones
- Por debajo de todo este entorno necesitaremos un entorno de desarrollo libre y un sistema operativo libre... FreeBSD, o GNU/Linux son las elecciones del momento.

El lector puede analizar los ejemplos de software libre sobre voto electrónico que se ofrecen.

En resumen: para realizar un servidor de voto electrónico de calidad no es preciso recurrir a ningún tipo de solución propietaria: El software libre ofrece recursos más que suficientes

8 Conclusiones

En este ensayo se ha descrito la problemática del Voto Electrónico, requerimientos legales, de software y de funcionamiento, y se han descrito a modo de ejemplo diversas aplicaciones de Software Libre para su implementación. El lector puede consultar las referencias que se citan si desea mayor información.

8.1 Software libre como garante de los derechos y libertades en un sistema de voto

Internet ha abierto nuevos campos de aplicación para el ejercicio de la libertad y la democracia. Si bien son precisos diversos mecanismos para que dicho ejercicio sea realizado con validez, no es menos cierto que disponemos de herramientas tanto técnicas como legales para llevarlo a cabo. El software libre es una pieza fundamental en este proceso, pues es el único que puede dar garantías al ciudadano de que se respetan plenamente sus derechos

Hemos visto que el uso de software libre es el único que puede garantizar los criterios de libertad, seguridad, y confiabilidad. El acceso al código fuente del servidor garantiza la detección de posibles fallos, intencionados o no. No podemos olvidar que para una democracia libre, la información debe ser tambien libre, y por supuesto tambien el ejercicio de nuestros derechos

8.2 Aplicación del voto electrónico a un entorno real

Para que lo descrito en estas líneas sea de aplicación válida y legal, habrá que hacer una serie de modificaciones en aras de mejorar la efectividad y la seguridad

- El primer paso es la descentralización. Puesto que no es posible hoy por hoy garantizar un acceso universal a la red, y puesto que los sistemas de voto tradicional son de gran arraigo y tradición, no podemos olvidar la división tradicional de colegios electorales y zonas.

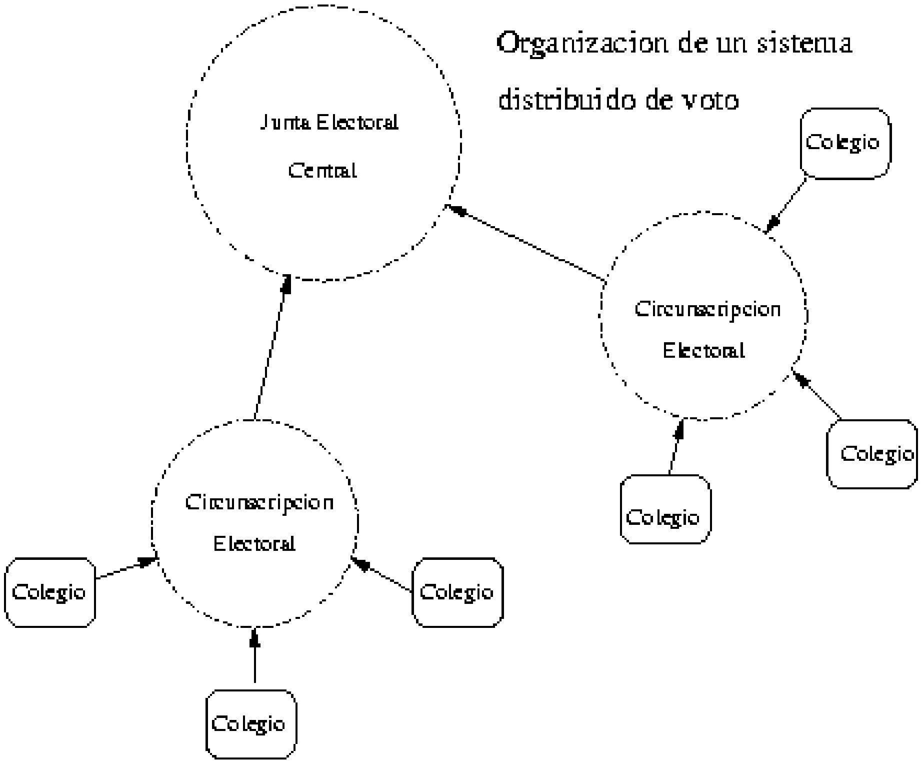

Figura 8: Sistema de voto distribuido

Así pues, En lugar de un servidor, dispondremos de tantos servidores como colegios electorales, cada uno con su propio censo. La votación se puede realizar de dos formas:

- Desde casa, vía internet, accediendo al servidor de zona
- En el propio colegio electoral, realizando las tareas de certificación y autentificación en una mesa al estilo tradicional, y accediendo posteriormente a una consola para emitir el voto
- En el caso del voto por correo, se procederá a proporcionar un sistema de voto diferido en las oficinas de correo, de manera que quede el voto almacenado de forma segura hasta el momento de la consulta. Especial cuidado se debe poner en la garantín de secreto. No obstante, en un sistema de voto por internet, el voto por correo es una actividad que realmente no será necesaria

- El segundo paso es la utilización de servidores replicados, para evitar problemas de seguridad o sobrecarga: las operaciones se realizan a la vez sobre varios servidores replicados en paralelo. De éste modo se evitan muchos problemas sobre confiabilidad en los administradores
- Según este esquema, el o los servidores centrales no son sistemas de votación sino sistemas de recuento al estilo de los actuales, con la diferencia de que los datos no son introducidos por operadores, sino que son recibidos en tiempo real desde cada uno de los servidores
- Deberemos proporcionar sistemas de protección y recuperación ante fallos, para no tener que invalidar las votaciones asociadas a un colegio electoral. Quizás no debamos dejar la urna tradicional demasiado lejos de la mesa... seguro que no hará falta

8.3 Más allá del voto tradicional. Consideraciones

Se ha hablado mucho sobre la Sociedad de la Información y sobre cómo la posibilidad de la democracia electrónica puede cambiar la sociedad. Sin entrar en detalles -para lo que se remite al lector a la literatura especializada sobre el tema- podemos indicar algunos aspectos de la democracia electrónica:

- El primer punto trata sobre las implicaciones de la posibilidad de un sistema de consulta universal, sencillo y rápido.
  - El hecho de que los ciudadanos puedan votar de forma directa, implica la dilución de atribuciones del parlamento: los asuntos importantes pueden ser decididos directamente y en pocos minutos
  - Esto conlleva una serie de problemas: sociológicamente se puede demostrar que un sistema así lleva aparejado una organización y planificación a corto plazo en la sociedad. Sin un soporte cultural fuerte, y una concienciación seria de la población acaba imperando un sistema de *"panem et circus"*, que si bien es atractivo a corto plazo, a medio y largo plazo conduce a la anarquía
  - Es necesario pues, que estén claramente definidos qué aspectos de la sociedad pueden y deben ser sometidos a consulta pública y cuales son privativos del parlamento y del gobierno
- Otro tema primordial es el de la universalidad: todo el mundo debe tener posibilidad de acceder al sistema de voto
  - Un problema real del fenómeno de la globalización es que tiende a aumentar las diferencias entre los países tecnológicos y los que no lo son. Dentro de cada sociedad ocurre lo mismo: se está creando una nueva división social entre los que tienen acceso a la tecnología y los que no
  - El software libre tiene entre otras la misión de hacer la tecnología accesible a todas las capas de la sociedad. Es misión de las Administraciones Públicas el garantizar la igualdad de derechos y oportunidades
  - No es admisible en una sociedad democrática el que una persona, por falta de conocimientos o recursos, no pueda ejercer sus derechos de ciudadano. No es tolerable, por consiguiente, un sistema de consulta que restrinja el acceso a dicho derecho
- El mundo de la toma de decisiones no se limita al voto electrónico: las técnicas y procedimientos aquí descritos tienen múltiples ámbitos de actuación. Es seguro que el futuro nos depara una pléyade de nuevas aplicaciones...

9 Referencias

Software

- El servidor de toma de decisiones ***E-Vote*** lo encontraremos en *http://www.e-vote.net*
- El programa ***MyPools*** se puede obtener en *http://www.phpbuilder.com*
- El programa ***Free-Vote*** se puede obtener en las páginas del autor: *http://drake.dit.upm.es/~jantonio/e-vote*
- Vote-Debian, el sistema de toma de decisiones de Debian se encuentra en: *http://vote.debian.org*
- En Slashdot (*http://www.slashdot.com*) y en BarraPunto (*http://www.barrapunto.com*) Encontraremos referencias a su código fuente, y con él a su sistema de encuestas

Reglamentación

- La Agencia de Protección de datos tiene su propia web: *http://www.agenciaprotecciondatos.org*. Allí podremos encontrar referencias a la Ley Orgánica de Tratamiento Automatizado de Datos, a los reglamentos de aplicación de la LORTAD y al funcionamiento de la APD, así como obtener los diversos formularios de registro del sistema en la Agencia
- La Fábrica Nacional de Moneda y Timbre es la autoridad española de certificación reconocida por nuestra legislación. A ella se deberá acudir para la obtención de certificados digitales de autentificación

Documentación adicional

Carlos Barriuso Ruiz
"Interacción del derecho y la informática"
Ed. Dykinson 1996. ISBN 84-8155-148-1

"Seguridad: Construír la confianza"
Revista *Novática*. Especial monográfico Septiembre-Octubre 1999

"Informe especial: Garantía de privacidad en Internet"
Revista *Investigación y Ciencia*. Diciembre 1999

Recursos

Consultar los diversos HOWTO's sobre encriptación, protocolos seguros Certificación electrónica, etc. Existe Software Libre para todas estas aplicaciones

En el paquete *Free-Vote* se incluye un completo manual de usuario. En él se podrán ver todos los datos y requisitos contemplados por la ley así como su implementación en un sistema real