

**Comentarios sobre el Borrador de
Recomendaciones del Consejo de Europa acerca
de Estándares para el Voto Electrónico**

**Fortaleciendo los requerimientos técnicos para mejorar la
confianza pública en el voto electrónico en Europa**

30 de Agosto de 2004

**Dr. Andreu Riera Jorba
Consejero Delegado
Scytl Online World Security, S.A.
Barcelona, España
andreu.riera@scytl.com**

© Copyright 2004 Scytl Online World Security S.A.

Introducción

Numerosos Estados europeos analizan actualmente las posibilidades ofrecidas por las tecnologías de la información y las comunicaciones para mejorar sus prácticas democráticas. El uso de métodos electrónicos de votación (*e-voting*) se ve como un campo prometedor que no obstante suscita a su vez un conjunto de nuevos desafíos los cuales deben ser cuidadosamente estudiados.

El Consejo de Europa, a través de un Grupo Ad Hoc Multidisciplinar de Especialistas en Estándares Legales, Operacionales y Técnicos para la Votación Electrónica (IP1-S-EE), ha estado estudiando durante los dos últimos años el tópico de la votación electrónica en elecciones públicas y referéndums, bajo los auspicios del Proyecto Integrado “*Making Democratic Institutions Work*” (“Las Instituciones Democráticas en Acción”). El 6 de Julio de 2004, el Grupo IP1-S-EE adoptó un Borrador Final¹ de la “Recomendación del Comité de Ministros a los Estados Miembros acerca de estándares legales, operacionales y técnicos para el voto electrónico”.

El Grupo IP1-S-EE nombra en el Borrador de Recomendación numerosos factores que justifican claramente el avance en el estudio, experimentación y adopción del voto electrónico en elecciones públicas y referéndums en toda Europa:

“Sabido que a medida que las nuevas tecnologías de la información y las comunicaciones se utilizan cada vez más en la vida cotidiana, es necesario que los Estados Miembros tomen en cuenta estos desarrollos en su práctica democrática;

Teniendo en cuenta que la participación en las elecciones y referéndums a nivel local, regional y nacional en algunos Estados Miembros se caracteriza por una asistencia baja y en algunos casos, progresivamente descendiente;

Teniendo en cuenta que algunos Estados Miembros ya están utilizando o están pensando en utilizar el voto electrónico para numerosos propósitos, incluyendo:

¹ El documento de Recomendación definitivo estará disponible antes del final de 2004 en <http://www.coe.int/democracy>

- *permitir a los votantes votar desde otro lugar aparte del centro electoral de su distrito;*
- *facilitar la emisión del voto por el votante;*
- *facilitar la participación en elecciones y referéndums a todos aquellos autorizados para votar, y particularmente a ciudadanos residiendo o viviendo en el extranjero;*
- *ampliar el acceso al proceso de votación a votantes con discapacidades o a aquellos que tengan otras dificultades a la hora de estar físicamente presentes en un centro electoral y utilizar los dispositivos disponibles;*
- *aumentar la asistencia de votantes proporcionando canales de votación adicionales;*
- *mejorar los procesos electorales con los nuevos desarrollos en la sociedad y el aumento en el uso de las nuevas tecnologías como medio para la comunicación y el compromiso civil en búsqueda de la democracia;*
- *reducir, con el tiempo, el coste total que supone a las autoridades electorales el llevar a cabo una elección o referéndum;*
- *mandar los resultados de la votación con confianza y más rápidamente; y*
- *proporcionar al electorado un mejor servicio, ofreciendo una variedad de canales de votación.”*

Por todo ello el Borrador de Recomendación promueve la adopción del voto electrónico por parte de los Estados Miembros. Aún así, el Grupo IP1-S-EE es totalmente consciente de los potenciales riesgos derivados de una introducción descuidada del voto electrónico. Como consecuencia, el Borrador de Recomendación exige elevados prerequisites objetivo para asegurar una introducción precisa y sensata, que genere confianza pública, del voto electrónico:

“Conscientes de la preocupación acerca de determinados problemas de seguridad y fiabilidad posiblemente inherentes en determinados sistemas de voto electrónico;

Conscientes, por lo tanto, que sólo aquellos sistemas de voto electrónico que sean seguros, fiables, eficientes, técnicamente robustos, abiertos a verificación

independiente y fácilmente accesibles a los votantes construirán la confianza pública que es un prerrequisito para llevar a cabo el voto electrónico;”

El Borrador de Recomendación del Consejo de Europa es el resultado de un estudio completo y cuidadoso, llevado a cabo por el Grupo IP1-S-EE, que establece una serie de estándares y requerimientos sobre los aspectos legales, operacionales y técnicos del voto electrónico. El objetivo del presente documento es desarrollar más en profundidad algunos de esos estándares y requerimientos aprovechando nuestra experiencia en los aspectos técnicos relacionados con la seguridad y la confianza en los sistemas de voto electrónico. Como expertos en seguridad del voto electrónico con una dilatada experiencia en este campo, proporcionamos en este documento nuestros comentarios sobre el Borrador de Recomendación, en particular sobre las secciones D (Seguridad) y E (Auditoria) de su Apéndice III (Requerimientos Técnicos).

En nuestra opinión es posible fortalecer aún más los requerimientos técnicos relacionados con la privacidad, seguridad y verificabilidad, para adaptarse mejor al principio que dicta que *“el voto electrónico deberá ser tan fiable y seguro como las elecciones democráticas y referéndums que no implican el uso de medios electrónicos”*.

Descripción general de nuestros comentarios

Nuestros comentarios acerca del Borrador de Recomendación se refieren exclusivamente a los estándares técnicos expuestos en el Apéndice III (Requerimientos Técnicos), y concretamente en las secciones D (Seguridad) y E (Auditoría). Aún así, los comentarios y adiciones propuestas también podrían afectar los Estándares Legales –específicamente la sección sobre Verificabilidad y Responsabilidad– en cuanto a la provisión de mecanismos que habiliten la verificación del voto por parte del votante.

En nuestra opinión, el Borrador de Recomendación de hecho ya establece unos niveles de seguridad notablemente altos para el voto electrónico. Nuestro objetivo en este documento es el de destacar o desarrollar algunos aspectos que creemos pueden ser reforzados todavía una poco más, con el objetivo de alcanzar sistemas de voto electrónico aún más seguros y fiables. No proponemos grandes cambios en el texto original, sino una serie de adiciones que en algunos casos ya se encuentran, aunque implícitas, en el texto actual.

A grandes rasgos, nuestra contribución consiste en:

- Introducir la capacidad de verificación por parte del votante.
- Introducir el requerimiento de secreto de los resultados intermedios de la votación como un Requerimiento Técnico y no tan sólo como un Estándar Operacional.
- Reforzar la protección del proceso democrático ante atacantes internos (es decir, personal técnico con acceso privilegiado al sistema de voto electrónico). Creemos que no sólo la red de comunicación empleada para transportar los votos, sino también todo el sistema de votación utilizado para recabar y almacenar esos votos debe ser considerado como entorno hostil sujeto a manipulaciones –en concreto por parte de atacantes internos–. Las acciones fraudulentas cometidas por personal técnico en el sistema de votación no deberían amenazar la integridad de los resultados o la privacidad de los votantes.
- Enfatizar la capacidad de auditoría.

Comentarios detallados sobre la seguridad y la auditoria en el voto electrónico

Nuestros comentarios hacen referencia a las secciones D (Seguridad) y E (Auditoria) del Apéndice III (Requerimientos Técnicos) del Borrador de Recomendación. Algunos de los comentarios introducen un nuevo Requerimiento, mientras que otros desarrollan/destacan un Requerimiento existente. Los comentarios se presentan siguiendo la misma estructura de secciones empleada en el Borrador de Recomendación. En total hay 9 comentarios presentados en este documento, los cuales han sido numerados utilizando numeración romana para evitar confusión con la numeración de los Requerimientos empleada en el Borrador de Recomendación.

Sección D: Seguridad

Requerimientos Generales

- I. Sugerimos la creación de un nuevo Requerimiento reclamando que *“Se tomen medidas técnicas y organizativas para asegurar que ni el personal técnico ni ninguna autoridad o connivencia de autoridades con acceso privilegiado al sistema de voto electrónico suponga un riesgo para la privacidad de los votantes o para la integridad de los resultados de la votación”*. A pesar de que esto ya figura implícitamente en algunos de los Requerimientos existentes, creemos que debe hacerse explícito dada la extraordinaria importancia de la declaración en el contexto del voto electrónico.

- II. Siguiendo el argumento precedente, sugerimos aumentar el Requerimiento 18 añadiendo que *“... la confidencialidad ... debe mantenerse, aún en el caso de que personal técnico con acceso privilegiado al sistema de voto electrónico mantenga un registro de las identidades de los votantes y/o de las direcciones electrónicas de los votantes a medida que éstos votan”*.

Requerimientos en la Fase de Votación

- III. Como suplemento al Requerimiento 34, sugerimos la creación de un nuevo Requerimiento reclamando que *“El hecho de que un voto haya sido emitido por un votante con derecho a votar deberá ser verificable”*. El objetivo de este nuevo Requerimiento es el de permitir la auditoria de cada voto individual con absoluta confianza en todo momento, y así prevenir que personal técnico con acceso privilegiado al sistema de voto electrónico pueda emitir votos falsos en nombre de votantes que se hayan abstenido.
- IV. Sugerimos añadir al Requerimiento 35 lo siguiente *“... la urna electrónica. No será posible eliminar o manipular los votos sellados, ni siquiera por parte de personal técnico con acceso privilegiado al sistema de voto electrónico.”* El objetivo de esta adición está claro por sí mismo.
- V. Sugerimos la creación de un nuevo Requerimiento Técnico pidiendo que *“Los resultados intermedios de la votación deberán permanecer en secreto antes de que las autoridades electorales pertinentes hayan tabulado los votos.”* El objetivo de este nuevo Requerimiento es prevenir que personal privilegiado filtre información referente a la evolución del proceso electoral con el objetivo de influir de algún modo en el comportamiento de los votantes que todavía no hayan votado. El Borrador de Recomendación ya establece un Estándar Operacional (número 18) que sugiere esto. Aún así, pretendemos ir más allá haciéndolo técnicamente imposible, incluso para personal privilegiado e incluso después del cierre de la urna electrónica.

Sección E: Auditoria

General

- VI. Sugerimos la creación de un nuevo Requerimiento Técnico solicitando que *“Las auditorias orientadas a la exactitud de los resultados de la votación deberán basarse en datos no manipulables”*. De nuevo, el objetivo es impedir que personal privilegiado pueda manipular los resultados.

Monitorización

- VII. Siguiendo con el comentario II, sugerimos añadir al Requerimiento 46 “... *anonimato del votante en todo momento, incluso si se mantiene un registro que permita correlacionar cualquier voto particular en la urna electrónica con la identidad del votante correspondiente*”.

Verificabilidad

- VIII. Sugerimos reforzar el Requerimiento 47 añadiendo “... *y demostrar que todos los votos recontados son auténticos, no han sido manipulados, se emitieron dentro de los límites de tiempo prescritos, y que todos y cada uno de los votos emitidos han sido contados*”.
- IX. La falta de transparencia del voto electrónico puede provocar incomodidad al electorado ya que se enfrenta a una “caja negra”. Las auditorias por parte de terceros pueden no resolver completamente esta problemática. Por ello, creemos que deben introducirse mecanismos adicionales que permitan a los votantes la verificación por sí mismos del sistema de voto electrónico. El Estándar Legal número 14 del Borrador de Recomendación ya reclama que “*El sistema de voto electrónico deberá indicar claramente al votante el hecho de que el voto se ha emitido con éxito y el hecho de que todo el proceso de votación ha sido completado*”. Sin embargo, sugerimos ir un paso más allá mediante la creación de un nuevo Requerimiento Técnico reclamando que “*Se tomen medidas técnicas y organizativas para asegurar que cada votante pueda verificar que su voto en particular ha sido transmitido, intacto, a los miembros de la mesa electoral o autoridades electorales correspondientes, y que el voto se ha tomado en cuenta en el proceso de recuento. Estas medidas no deberán poder ser utilizadas por parte del votante para demostrar qué ha votado, para así no permitir o facilitar la compra de votos y/o la coacción.*” Creemos que se debe informar al votante no sólo de que su voto ha sido correctamente registrado por el sistema de voto electrónico sino que además el votante debe tener la plena garantía de que su voto ha sido entregado intacto por el sistema de voto electrónico a los miembros

de la mesa electoral o las autoridades electorales correspondientes. Esta garantía sólo puede ofrecerse después de que los votos hayan sido tabulados por las autoridades electorales, y asegura que los sistemas de voto electrónico serán como mínimo tan fiables y seguros como los métodos de votación actuales. Es muy importante tener en cuenta que el nuevo Requerimiento sugerido no representa un conflicto con el Estándar Operacional número 16, el cual afirma que *“Un sistema de voto electrónico remoto no deberá permitir al votante llegar a poseer una prueba del contenido del voto emitido”*. La última declaración del nuevo Requerimiento sugerido compatibiliza la verificación por parte del votante con la ausencia de pruebas que podrían utilizarse para la compra de votos y/o la coacción.

Conclusiones

El Grupo Ad Hoc Multidisciplinar de Especialistas en Estándares Legales, Operacionales y Técnicos para la Votación Electrónica, reunido por el Consejo de Europa, ha publicado un Borrador Final de su Recomendación del Comité de Ministros a los Estados Miembros acerca de estándares legales, operacionales y técnicos para el voto electrónico. El Borrador de Recomendación dispone una serie de estándares legales, operacionales y técnicos para la correcta adopción del voto electrónico en las elecciones públicas y referéndums en Europa.

Creemos que el Borrador de Recomendación es un trabajo excelente que contiene estándares correctos y adecuados. El Borrador de Recomendación establece unos niveles de exigencia bastante altos en la seguridad del voto electrónico. A pesar de ello, creemos que algunos aspectos pueden destacarse, desarrollarse o explicitarse aún más. En concreto, sugerimos la introducción de la verificabilidad por parte del votante como ha sido presentada en este documento, con el objetivo de incrementar la confianza del electorado en el voto electrónico.

Este documento ha introducido un total de 9 comentarios sobre los Requerimientos Técnicos del Borrador de Recomendación, específicamente los de las secciones de Seguridad y Auditoria, con el objetivo de fortalecer los niveles de seguridad, honradez, auditoria, y privacidad de los sistemas de voto electrónico. La meta final es alcanzar un nivel de seguridad en el voto electrónico totalmente equiparable al que presentan los sistemas de voto convencionales.

Acerca del autor

Andreu Riera inició sus estudios académicos en la seguridad para el voto electrónico en el año 1995, obteniendo una extensa lista de publicaciones científicas internacionales y capítulos de libro. Su Tesis Doctoral "*Design of Implementable Solutions for Large Scale Electronic Voting Schemes*" se publicó en 1999. Ha sido coautor de seis solicitudes de patente internacionales, tres de las cuales se refieren a modelos técnicos para aportar confianza a los sistemas de voto electrónico. También ha llevado a cabo numerosas ponencias sobre seguridad para voto electrónico en conferencias y seminarios en varios países europeos. También aconsejó al Senado Español acerca de la correcta implementación del voto electrónico en cuanto a sus aspectos de seguridad.

En el año 2001, el Dr. Riera fundó Scytl Online World Security S.A. (Scytl)² como spin-off de su grupo académico sobre seguridad en el voto electrónico. La actividad de investigación del grupo académico fue financiada inicialmente por el Ministerio Español de Ciencia y Tecnología y durante más de 6 años generó más de 20 documentos científicos que se presentaron en conferencias y jornadas internacionales. El grupo también produjo las dos únicas (hasta la fecha) Tesis Doctorales europeas sobre sistemas de seguridad para el voto electrónico remoto. Además, el grupo de investigación español desarrolló un prototipo práctico que se empleó en el año 1997 para llevar a cabo las primeras elecciones vinculantes en Europa (para la presidencia del Capítulo Español de Teoría de la Información del IEEE).

Aprovechando toda esta experiencia, el equipo de I+D de Scytl ha creado un innovador sistema de seguridad que asegura la privacidad, integridad y verificabilidad en los sistemas de voto electrónico. Este producto único, el cual ya ha sido implantado con éxito en varias plataformas europeas de voto electrónico oficiales, cumple satisfactoriamente con los estándares de seguridad y auditoría establecidos en el Borrador de Recomendación del Consejo de Europa e incluye también las adiciones y comentarios sugeridos en este documento.

² <http://www.scytl.com>