PROCEDIMIENTO NORMATIVA ELECTORAL VOTO ON-LINE Y ACTUALIZACIÓN RGPD

Objeto

Desarrollar la normativa electoral establecida en el Título V de los Estatutos de la Asociación de Ingenieros Industriales de Aragón (en adelante AIIA), principalmente con el objetivo de integrar el voto online en la forma de la elección (art. 27 y ss).

Asimismo, se pretende actualizar la interpretación de los artículos de este Capítulo a la Normativa de Protección de Datos y más concretamente a la reciente normativa europea y estatal aprobada en esta materia, así como aclarar otros aspectos del procedimiento.

Antecedentes

El contexto tecnológico en el que nos encontramos actualmente y la situación de los Asociados, diseminados por todo el territorio nacional e internacional, hace imprescindible acometer una adecuación de la forma de elección que contemple la posibilidad del voto online.

Esta forma de elección o voto no se refleja expresamente en nuestros Estatutos.

Con la introducción del voto online se acerca y facilita la participación de todos los Asociados independientemente de su situación o lugar de residencia, siendo una manera segura y certificada de ejercer el derecho al voto en la AIIA, lo que, al menos en el presente contexto sanitario, resulta imprescindible.

Asimismo, la nueva normativa europea relacionada con la protección de datos impide realizar algunas de las actuaciones que indican los Estatutos en relación con la publicación de datos de los Asociados.

Desarrollo del voto online

Durante el proceso de convocatoria de elecciones, se enviará a los Asociados, junto a la información sobre las elecciones y las diferentes opciones de votación, un documento explicativo detallando el procedimiento para la votación online.
El mismo día fijado para la elección se enviará un email a cada asociado a la dirección de correo electrónico que figure en ese momento en la base de datos de la AIIA, con las indicaciones para votar de manera online, forma de acceso, manera de autenticarse y todos los pasos a seguir, garantizando la accesibilidad del proceso, la seguridad del canal de transmisión del voto, la confidencialidad, secreto y anonimato de los votos y la integridad del escrutinio.

El horario de la votación online coincidirá con el de la votación presencial.

Dada la imposibilidad de anulación del voto online, éste tendrá preferencia sobre el voto por correo y sobre el voto presencial.

La Mesa Electoral comprobará en un listado que todos los Asociados que asisten a votar de manera presencial no han ejercido su derecho al voto de manera online previamente a su llegada a la urna. En el hipotético caso de que algún Asociado quiera votar de forma presencial y ya haya votado online, se le explicará que no puede votar de nuevo y se hará constar en acta esta circunstancia.

La Mesa comprobará si alguno de los Asociados que ha votado por correo ya lo ha hecho online, si es así, no introducirá el sobre en la urna y deberá hacer constar en acta las causas que han motivado la invalidez y remitir un oficio al Asociado notificándole las mismas.

Terminada la votación, la Mesa procederá al escrutinio de los votos presenciales y los votos por correo a los que unirá los votos online. Las dudas sobre la validez o interpretación de un voto serán resueltas de forma inmediata por la Mesa electoral.

La AIIA pondrá a disposición de los Asociados los datos de contacto de un soporte técnico durante el periodo de votación para solventar buena parte de los problemas, relacionados con el método, que pudieran surgir. Dado que el objetivo de esta modalidad de voto es facilitar la participación, las dudas que puedan producirse por los problemas técnicos, siempre que se justifiquen, se resolverán en el sentido que sea más favorable a la participación, siempre que se garantice la autenticidad y el secreto del voto.

Actualización de la interpretación del artículo 30 de los Estatutos para cumplir con la normativa en materia de protección de datos

En el Art. 30 de los Estatutos se indica “Una copia del acta de la elección, así como una lista de los asociados que hayan ejercido el derecho a voto, se publicará en el tablón de anuncios de la Asociación.”

Este artículo resulta contrario a la normativa legal vigente en materia de protección de datos[1] debido a que la publicación de las listas de Asociados con derecho a voto no se ajusta a las bases legitimadoras que están previstas en el artículo 6 del RGP.

Es por ello que no se publicará en el tablón de anuncios de la AIIA el listado de Asociados que hayan ejercitado su derecho al voto.

[1] Veáse Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Avales

En ningún caso la AIIA promocionará o facilitará la recogida de avales para ninguna candidatura por ningún medio, debiendo permanecer en todo momento absolutamente neutral.

Campaña electoral

La campaña electoral tendrá la duración establecida en los Estatutos. El día previo a la jornada de las votaciones, tendrá la consideración de "jornada de reflexión" y durante dicho día no se podrán realizar actos ni remitir publicidad alguna en relación con la campaña.

Durante la campaña electoral (a excepción de la jornada de reflexión), los candidatos podrán organizar, a su coste, actos para comunicar su programa a los Asociados. La AIIA podrá ceder las instalaciones de que disponga para estos actos, sin coste y en igualdad de condiciones a todos los candidatos.

Sin perjuicio de los canales de comunicación que cada candidato quiera utilizar, se entiende por él sufragados, la AIIA será también un vehículo de comunicación a disposición de los candidatos hacia los Asociados, y deberá remitirles la documentación que los candidatos consideren necesaria para comunicar su programa. Esta se limitará, por razones de organización y para no colapsar el funcionamiento normal da la AIIA, a un máximo de dos envíos, bien sea por correo electrónico o por correo postal.

Durante la campaña electoral, los candidatos podrán disponer de un espacio, en igualdad de condiciones, en la web de la AIIA.

En ningún caso la AIIA cederá los datos personales de los Asociados a ningún candidato.

Resolución de conflictos

La Mesa Electoral es el órgano competente para dirimir y resolver cualquier circunstancia no prevista de forma explícita en el Procedimiento.

Recomendaciones Protección de datos

Se adjuntan a continuación recomendaciones de Protección de Datos en relación a este Procedimiento Normativa Electoral.

RECOMENDACIÓN Rec(2004)11 DEL COMITÉ DE MINISTROS DEL CONSEJO DE EUROPA A LOS ESTADOS MIEMBROS SOBRE LOS ESTÁNDARES LEGALES, PROCEDIMENTALES Y TÉCNICOS DE LOS SISTEMAS DE VOTACIÓN ELECTRÓNICA, FIRMADA EN ESTRASBURGO EL DÍA 30 DE SEPTIEMBRE DE 2004.[1]

Con carácter previo a la introducción de cualquier sistema de voto electrónico, y, una vez introducido, en los intervalos que se estimen oportunos, así como tras cualquier modificación que se haga al sistema, un organismo independiente, designado por las autoridades electorales, verificará que el sistema de voto electrónico funciona correctamente y que todas las necesarias medidas de seguridad se han adoptado.

La realización de un recuento será posible. Cualquier característica del sistema de voto electrónico que pudiera influir en la exactitud de los resultados será objeto de verificación

El sistema de voto electrónico incluirá medidas para preservar la disponibilidad de sus servicios durante el proceso de votación. En particular, el sistema deberá ser inmune a disfunciones, "breakdowns" o ataques de denegación de servicio.

Únicamente las personas autorizadas por las autoridades electorales podrán tener acceso a la infraestructura central, a los servidores y a los datos electorales. Dichas autorizaciones serán objeto de una clara regulación. Las tareas técnicas más complejas se realizarán por equipos integrados por al menos dos personas. La composición de dichos equipos se renovará periódicamente. En la medida de lo posible, estas actividades deberán llevarse a cabo fuera del periodo electoral.

El sistema de voto electrónico preservará la disponibilidad y la integridad de los votos. También preservará la confidencialidad de los votos y los mantendrá sellados hasta el momento del escrutinio. En el caso de que los votos se almacenen o transmitan fuera de entornos controlados éstos habrán de encriptarse.

El diseño de todo sistema de votación electrónica debe basarse en un comprensivo análisis de los riesgos que conlleva la efectiva y exitosa realización de unas elecciones o de un referéndum en concreto. El sistema de votación electrónica incluirá las garantías que, basadas en el análisis de riesgos antes citado, se consideren apropiadas para superar los riesgos que eventualmente se hayan identificado. Los fallos o la degradación del servicio deberán mantenerse dentro de unos límites predefinidos.

A. Accesibilidad

A1. Se adoptarán medidas para garantizar el acceso de todos los votantes al software y a los servicios que se utilicen y, en su caso, se proveerá el acceso a sistemas de voto alternativos.
A2. Los usuarios deberán ser tenidos en cuenta a la hora de diseñar los sistemas de votación electrónica, en concreto con el fin de que ayuden a identificar el grado de facilidad de uso y las limitaciones del sistema en todas y cada una de las etapas principales en el desarrollo del proceso.
A3. Se suministrará a los usuarios, cuando sea necesario y posible, medios adicionales, como pueden ser, entre otros, interfaces especiales o asistencia técnica. Los medios que se pongan a disposición de los electores habrán de respetar tanto como sea posible los principios establecidos por la Web Accessibility Initiative (WAI). [4]
A4. La presentación de las opciones de voto habrá de optimizarse para el votante.

B. Sistemas operativos. (Para la infraestructura central y los clientes en lugares controlados)

B1. Las Autoridades Electorales competentes harán público el listado oficial del software utilizado en las elecciones o referéndums electrónicos. Los Estados Miembros podrán excluir de este listado, por razones de seguridad, el software de protección de datos. Como mínimo, en ese listado oficial se incluirá el software utilizado; las versiones; su fecha de instalación; y una breve descripción del mismo. Se regulará un procedimiento que permita la instalación periódica de versiones actualizadas, y parches, del software de alta protección. En cualquier momento deberá ser posible la revisión del estado de protección del equipamiento del sistema de votación electrónica.

B2. Los responsables del funcionamiento del sistema deberán diseñar un procedimiento a seguir en caso de emergencias. Todo sistema de emergencia deberá atenerse a los mismos estándares y requisitos que el sistema original.

B3. Con el fin de garantizar que el proceso de votación se desarrolla sin problemas, será preciso que se habiliten, y que estén permanentemente disponibles, los correspondientes mecanismos de apoyo o backup. El personal a cargo del proceso de votación deberá estar preparado para intervenir con rapidez siguiendo el procedimiento diseñado por las autoridades electorales competentes.

B4. Los responsables de los equipos deberán seguir unos procedimientos que garanticen que durante el periodo de votación, el equipo de votación y el uso del mismo cumplen todos los requisitos. Regularmente se proveerá a los servicios de backup (copia de seguridad) con protocolos de seguimiento (monitoring protocols).

B5. Toda operación de carácter técnico habrá de seguir un determinado procedimiento de control de modificaciones. Deberá comunicarse cualquier modificación sustancial que afecte a los equipos clave.

B6. El equipamiento clave en unas elecciones o en un referéndum electrónico deberá ubicarse en un lugar seguro, y dicho lugar, a lo largo del periodo electoral, o del referéndum, deberá ser protegido de cualquier interferencia, venga ésta de donde venga y sea esta realizada por quien sea. Durante el periodo electoral, o del referendum, deberá aplicarse un plan de recuperación frente a desastres que provocaran pérdidas materiales. A mayor abundamiento, cualquier dato retenido tras el periodo electoral, o del referéndum, deberá guardarse de manera segura.

B7. En el supuesto de que se produzcan incidentes que pudieran amenazar la integridad del sistema, los responsables de operar con los equipos informarán de manera inmediata a las autoridades electorales competentes, la cuales seguirán los pasos que sean necesarios para mitigar los efectos del incidente en cuestión. Con carácter previo, las autoridades electorales especificaran el nivel de gravedad de los incidentes a partir del cual se deberá informar de los mismos.

C. Seguridad

C.I. Requisitos generales.

C.I.1. Se adoptarán medidas técnicas, y de organización, con el fin de asegurar que en el caso de break down (caída del sistema), o si se produce un fallo que afectase al sistema de votación electrónica, no sea posible la pérdida definitiva de datos.

C.I.2. El sistema de votación electrónica protegerá la privacidad de los individuos. Se mantendrá también la confidencialidad de los registros de votantes que estén guardados en, o que hayan sido comunicados a través del sistema de votación electrónica.

C.I.3. El sistema de votación electrónica se someterá regularmente a chequeos para garantizar que sus componentes funcionan de acuerdo con sus especificaciones técnicas y que sus servicios están disponibles.

C.I.4. El sistema de votación electrónica restringirá el nivel de acceso a sus servicios dependiendo de la identidad del usuario o de las funciones atribuidas a determinados tipos de usuarios. Sólo se dará acceso a los servicios expresamente asignados a ese usuario concreto o a esa clase de usuario. Antes de poder acometer cualquier operación se requiere que se haga efectiva la autenticación del usuario.

C.I.5. El sistema de votación electrónica protegerá los datos utilizados para la autenticación de manera que las entidades sin autorización no puedan utilizar fraudulentamente, interceptar, modificar o apercibirse de los datos relativos a la autenticación, o de parte de ellos. En el supuesto de votación en medios no controlados (Vg. votación no presencial) se recomienda la utilización de mecanismos de encriptación para la autenticación.

C.I.6. Se garantizará el proceso de identificación de votantes y candidatos de tal modo que puedan diferenciarse inequívocamente de otras personas (identificación única o singular).

C.I.7. Los sistemas de votación electrónica generarán datos fiables y suficientes para que se pueda llevar a cabo una observación electoral. Deberá poder determinarse de manera fiable el momento en el que el evento que genere dichos datos sea susceptible de ser observado. Deberá mantenerse la autenticidad, disponibilidad e integridad de los datos.

C.I.8. El sistema de votación electrónica mantendrá fuentes temporales sincronizadas que han de ser fiables. La fuente temporal seré lo suficientemente exacta como para mantener la constancia del paso del tiempo - las marcas temporales son necesarias para los procesos de auditoria y para los datos susceptibles de ser observados- así como para mantener el control temporal aplicable a los límites establecidos para el registro electoral, la presentación de candidatos, la votación o el escrutinio.

C.I.9. Las autoridades electorales son responsables de que estos requisitos de seguridad, que serán supervisados por organismos independientes, se cumplan.

II. Requisitos en las etapas previas a la emisión del voto (y requisitos predicables de los datos generados en la etapa de emisión del voto).

CII.1. La autenticidad, disponibilidad e integridad de las listas del Censo Electoral y de las candidaturas habrá de ser mantenida. La fuente que genera los datos será autentificada. Se tendrán en cuenta las previsiones relativas a la protección de datos.

Conservación

Los datos deberán ser eliminados al término del proceso electoral.