Cuarta Conferencia de Directores de Tecnología de Información y Comunicación en Instituciones de Educación Superior: Gestión de las TICs para la investigación y colaboración

Modelo de encriptación con llaves colegiadas: Aplicación para el voto electrónico en la Universidad Técnica Federico Santa María, Chile.

Gustavo Anabalón González, Sergio Fuentes León, Daniela Larenas

Universidad Técnica Federico Santa María, Avenida España 1680,
Valparaíso, Chile
gustavo.anabalon@usm.cl, sergio.fuentesleon@usm.cl, daniela.larenas.13@sansano.usm.cl

Resumen: El presente trabajo, expone la solución a un mecanismo manual de votación realizado por la Universidad Técnica Federico Santa María, el cual se realiza para la elección de un representante de los ex alumnos en el Consejo Superior[1] de la Universidad. Este proceso tradicional de votación resulta tener grandes falencias, ya que es realizado mediante sobre cerrado o a través de fax enviados por los votantes a secretaría general con algunos requisitos de información, lo que lleva a la Dirección de Tecnologías de la Información de la Universidad junto con Secretaría General a idear y realizar un modelo que estuviese a la altura de la importancia del proceso.

Este proyecto es realizado a través de un modelo de encriptación que utiliza llaves colegiadas para asegurar la confiabilidad en el sistema a sus usuarios y a la misma Universidad, mejorando en gran parte el mecanismo tradicional de la Universidad, como así también aumentando la participación de los ex alumnos.

Así también, este trabajo relata la experiencia obtenida por la Universidad en su primer evento de votación a través de este modelo realizado.

Palabras claves: Voto electrónico, seguridad, encriptación colegiada, llave pública, llave privada, elecciones electrónicas.

1. Introducción

La Universidad Técnica Federico Santa María (USM), siempre ha tenido como desafíos acrecentar el prestigio con el cual cuenta y consolidar su liderazgo en Ingeniería, Ciencia y Tecnología, esto a través de la continua mejora de los procesos internos que entrega la Universidad a sus usuarios, para así mantener su fidelidad con la institución.

Es en post de este plan estratégico de la Universidad, que la Dirección de Tecnologías de la Información (DTI) se alinea a través de uno de sus objetivos, el cual es

[1] Consejo Superior: Organismo Colegiado que representa la máxima autoridad de dirección y gobierno de la Universidad.

coordinar y administrar los servicios centrales de Tecnologías de Información y Comunicaciones de la Universidad, para apoyar a las unidades académicas, docentes y administrativas en temas del área y apoyar los grandes lineamientos de la institución en relación a las tecnologías de información y comunicaciones. Es por esto que se analiza el proceso tradicional de la elección para representante de los ex alumnos en el Consejo Superior, siendo un mecanismo manual que se realiza a través de sobres enviados por los votantes o fax, destinados a la Secretaría General de la Universidad, teniendo grandes limitantes, tanto para los ex alumnos como para el Colegio Eleccionario[2] (CE).

Es por esto que se hace necesario crear un nuevo proceso, un modelo que facilite tanto el registro (verificación de requisitos pertinentes) como la votación de los ex alumnos, para hacer más participativa esta instancia. Sin dejar de lado que tenga la seguridad suficiente para ser de la total confianza de los votantes, candidatos y del CE.

2. USM y su Gobierno Corporativo

La estructura organizacional de la Universidad Técnica Federico Santa María está compuesta por un Gobierno Corporativo, el cual consta de Rectoría y los siguientes Consejos:

- **Consejo Superior.** Está conformado por: un Presidente, el Rector, el Secretario general, un representante de los alumnos y nueve Consejeros.
- **Consejo Académico**, está constituido por el Rector, Vicerrector académico, Representantes Federación Casa Central, Secretario General y Consejeros.
- **Consejo Normativo**, constituido por el Rector, Vicerrector académico, Director Sede Viña del Mar, Director Sede Concepción, Secretario general, Alumno Federación Sede Viña del Mar, Alumno Federación Sede Concepción y Consejeros.

La elección de los integrantes de estos Consejos y Rectoría, se realiza cada cuatro años y es necesario el voto de ciertos académicos, administrativos y ex alumnos en algunos casos.

En cuanto a los integrantes del Consejo Superior, que son los que ameritan en este proyecto, están compuestos por:

- Un Consejero representante del Presidente de la República
- Un Consejero representante de los ex alumnos
- Cuatro Consejeros representantes de los académicos
- Dos Consejeros representantes de los docentes
- Un Consejero elegido por el Consejo académico y los Directores de sedes, (persona ajena a la institución).

---

[2] Colegio Eleccionario (CE): En chile el Colegio Eleccionario tiene el nombre de Tribunal Calificador de Elecciones (TRICEL); para efectos de este documento se le cambio el nombre a Colegio Eleccionario.

- El Presidente, quién es elegido por el Consejo académico y los Directores de sedes, de entre los ex alumnos.

3. Buscando la mayor representatividad del Consejero que representa a los Ex Alumnos

El miembro representante de los ex alumnos de la Universidad del Consejo Superior tiene particular relevancia porque representa la visión externa desde el mundo profesional hacia el gobierno corporativo.

Para la elección de dicho representante, se necesita la participación de los ex alumnos, quienes para ser electores, deben estar en posesión de un título o de los grados de licenciado, Magíster o Doctor, otorgados por la Universidad, siempre que lo anterior implique un programa de estudios equivalente a un programa académico regular de al menos 2 años de duración.

Este mecanismo siempre conllevó una poca participación por parte de los votantes, por lejanía, falta de tiempo, poca comunicación con la institución, etc. Con este modelo, manejar controles de identidad rigurosos siempre deja brechas que dan espacio a la posibilidad de suplantación o fraude.

La baja participación y las debilidades en la seguridad, llevó a la institución a buscar medios más confiables y participativos que entregara tanto a los votantes como a los miembros del "CE" la confianza, oportunidad, facilidad e información necesaria para realizar un proceso limpio y participativo que asegure la elección de un Consejero que cuente con el real reconocimiento de la comunidad que lo elige.

La Universidad hacía un llamado por medio de la prensa escrita y otras instancias a sus ex alumnos para votar por los candidatos propuestos por estos mismos, aparte del llamado de la Universidad, los candidatos se encargaban de contactar e incentivar a los ex alumnos a votar por ellos, donde el sistema de votación era de dos maneras: a través de un sobre cerrado dirigido a secretaría general indicando el remitente, o en el caso de que esté geográficamente lejos de la Universidad, podría emitir su preferencia a través de fax con una copia de su carnet, donde el Secretario General verificaba identidad y pertinencia y custodiaba los documentos hasta el minuto del escrutinio.

Como resultado, se obtenía gran cantidad de votos que en su mayoría provenían de pocos remitentes y con un gran nivel de correlación entre ese remitente y la preferencia por algún candidato, es el ejemplo de las últimas votaciones con el mecanismo tradicional, el año 2008, donde la cantidad total de votantes fueron 1973, donde existieron 126 votos rechazados por distintos motivos, como fax incompletos o defectuosos, sobres sin remitentes o sin ser dirigidos a Secretaría General, por lo que no fueron considerados en las votaciones, implicando un margen de error en la elección de los candidatos.

Debido a que el representante de los ex alumnos en el consejo superior debe velar por los intereses de la mayoría de sus representados, es que se hace necesario contar con la mayor participación posible de votantes que cumplan con los requisitos para ejercer este derecho.

La Universidad Técnica Federico Santa María durante sus 83 años ha graduado a miles de profesionales, los cuales desde cualquier lugar del mundo podrían ejercer su derecho a sufragio.

En estas circunstancias, las condiciones para participar en un proceso de este tipo están dadas por los siguientes elementos.

- El nivel de información que como ex alumno reciba de la USM en su lugar de residencia o trabajo.
- El nivel de compromiso y vínculo emocional que el exalumno sienta por su institución formadora.
- El nivel de vinculación que el profesional tenga con su comunidad de egresados.
- La facilidad de comunicación que el egresado tenga con diferentes organismos al interior de la institución.
- Los servicios que la institución le provea como egresado y la valoración que este tenga de ellos.
- Las facilidades que se le den, tanto en información como en acceso, para participar de un proceso de este tipo.

Suponiendo que se cumplen algunas de las condiciones de carácter emocional, es posible mejorar con el estado actual de las TICs el nivel de integración y comunicación con este universo, de manera que su participación no sea solamente al momento de manifestar su preferencia por un representante, sino también durante todas las actividades y eventos que merezcan su participación.

4. Debilidades del sistema tradicional

Dado que el sistema tradicional era a través de un sobre cerrado o por medio de fax, se encontraron las siguientes debilidades que obstaculizaban el proceso:

- Votación mediante sobre cerrado: este mecanismo era utilizado por las personas que tenían mayor cercanía geográfica con la Universidad, uno de los más utilizados pero que muchos solían ser rechazados por estar sin las características mínimas que se pedían para considerarse válidos (identificación inequívoca y comprobable del votante).
- Votación por fax: el menos común de los canales usados por los votantes, teniendo una gran cantidad de rechazados por estar con información incompleta o defectuosa, lo que disminuía aún más la participación de los ex alumnos, además del hecho de ser no verificable (cualquier persona podía mandar un fax a nombre de otra con el voto)

La recepción de los votos, tanto en sobre cerrado como a través de fax, era un método muy poco confiable, así como también el proceso de conteo de votos.

5. Aprehensiones aplicables a un sistema en línea y acciones abordadas para contenerlas.

- ***Riesgo de Suplantación***

  Si los medios manuales utilizados tenían esta debilidad, lo desconocido tiende a acrecentarla, la necesidad de minimizar de manera simple y a costos razonables este riesgo fue uno de los desafíos que se plantearon. El criterio fue buscar la mejor opción que asegurara niveles superiores a los que existían.

- ***Fraude en el registro y conteo de los votos***

  El hecho de que la administración de las operaciones dependiera de profesionales especializados y que la responsabilidad del proceso estuviera en manos de un organismo colegiado que en general no tiene dominio sobre los aspectos finos de la tecnología produce un alto grado de desconfianza en este tipo de herramientas. A ello debe agregarse el permanente riesgo de intrusión o hackeo y la posibilidad de que durante el desarrollo de las aplicaciones se hubiese incorporado código malicioso que pudiese alterar los resultados del proceso.

  Para entregar elementos suficientes de seguridad tanto al CE, a los candidatos y la comunidad en general se debía diseñar un modelo de auditoría que asegurara tanto las aplicaciones como la plataforma y el proceso mismo.

- ***Poca participación por brecha digital***

  Aunque la posibilidad de que algunos votantes por sus condiciones etarias o de conocimientos y por poca accesibilidad a medios tecnológicos se pudiese ver reducida, se consideró que utilizar un medio masivo y universal siempre va a dar la oportunidad de mayor cobertura que la que se tenía. Sin embargo, el modelo a implementar debía tener un conjunto de herramientas complementarias que facilitasen el uso y comunicación con la institución, en la mayor cantidad de etapas del proceso.

- ***Pérdida ante desastre en la infraestructura tecnológica***

  Existía el temor de que el proceso se viese invalidado debido a fallas catastróficas en la infraestructura tecnológica, o al ser en un periodo de tiempo acotado, tuviese caídas y cortes impidiendo el libre ejercicio del derecho a voto de los participantes y poniendo en duda su confiabilidad.

  Para mantener niveles de confianza suficiente, el modelo debía contar con el máximo de protecciones y resguardos que reduzcan estos riesgos.

- ***Temor a no poder recuperar los datos, una vez cerrado el proceso***

  Este riesgo es inherente a la posibilidad de implementar un proceso cuyos niveles de seguridad, una vez implementados y ante fallas o contingencias no previstas impidiese obtener los datos para ser procesados, obligó al equipo de desarrollo a diseñar resguardos especiales que mantuviesen la seguridad pero que diesen niveles de acceso complementarios que serían utilizados en caso de ser requeridos. Por ejemplo que los votos no pudiesen ser desencriptados al finalizar el proceso.

6. El Modelo

- ***Premisas***

  Considerando los elementos básicos que debe contar un sistema eleccionario y buscando la forma de incorporar todos los aspectos derivados de las aprehensiones y riesgos asociados a los nuevos paradigmas de la tecnología, se establecieron las siguientes premisas como condicionantes de diseño que el modelo debía contener.

  - ***Secreto***

    El voto debe mantener su condición de secreto y no ser vinculable bajo ningún aspecto con el votante.

  - ***Simple***

    El acto de votación y administración debe ser simple tanto para el votante como para los miembros del Tribunal Calificador de Elecciones (CE)

  - ***Verificable***

    El voto debe ser verificable, tanto en relación a quienes sufragaron, como también al voto emitido; sin entrar en conflicto con la premisa de "secreto"

  - ***Auditable***

    Tanto el proceso como las herramientas deben ser auditables de manera interna y externa.

  - ***Confiable***

    El sistema debe contar con las herramientas y protocolos de seguridad que impidan el acceso no autorizado tanto al sistema como también a las bases de datos.

  - ***Identificación segura (Firma Electrónica)***

    .1.1.1. Simple: Rastreable (Votantes)

    Se debe identificar inequívocamente a la persona que está emitiendo el sufragio, acreditando que es quien dice ser y bajo qué condiciones actuó.

    .1.1.2. Avanzada: Irrefutable (CE)

    Para identificar a las personas y actos de miembros del CE con seguridad, confidencialidad y validez tal, que no puedan ser desconocidos ulteriormente

- ***Modelo Funcional***

La figura Nº1 ilustra la manera como se abordó el diseño del proceso eleccionario; no dista de ser muy diferente desde el punto de vista general a los procesos clásicos. El proceso se inicia con el llamado a participar y registrarse para conformar el padrón electoral, posteriormente y en las fechas definidas se realiza el sufragio, el cual es supervisado por el CE, al cerrar el período de votaciones se ejecuta escrutinio para finalmente certificar y comunicar los resultados.

Adicionalmente el modelo debe considerar los elementos necesarios para realizar una segunda vuelta si fuese necesario o para facilitar los procesos de auditoría.

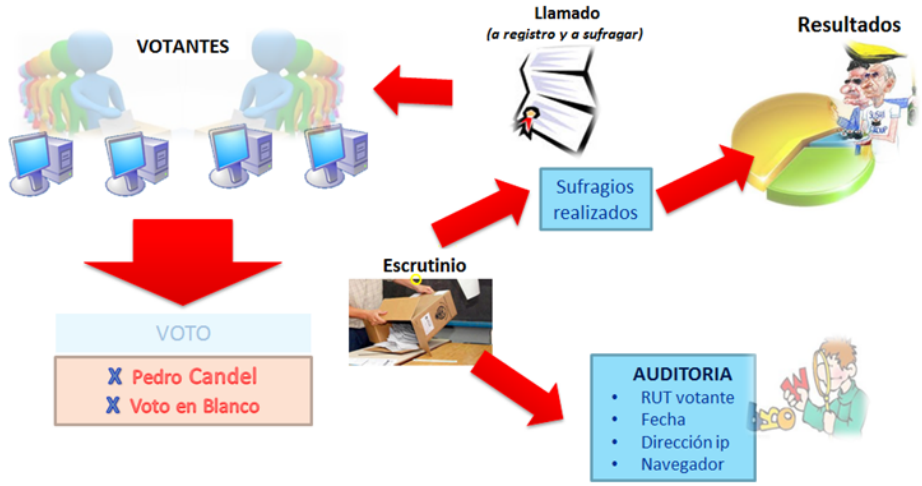

Figura Nº 1: ***Diagrama del Proceso de Votación Electrónica***

- ***Principales Componentes***
  - ***Padrón electoral***

El padrón electoral debe ser formalizado por los mismos participantes, validando previamente su participación a través de la generación de su cuenta de acceso (firma simple)

  - ***Incorporación de Firma Electrónica Avanzada***

La firma electrónica se realizó con certificados seguros, los cuales fueron almacenados en las tarjetas de identificación personal (TUI)[3] de cada miembro del CE. Esto permitió la firma personal para realizar la encriptación de la clave privada con la que se abrió la urna, además de generar la clave pública con la que se encriptaron los votos al momento de efectuar la votación.

  - ***Procedimiento colegiado para abrir y cerrar la "urna electoral"***

La apertura de las urnas, con la obtención de la clave privada de desencriptación, se realizará en forma colegiada. Esto quiere decir que para poder desencriptar se requería de al menos un 50% más uno de los miembros del CE que participaron en el cierre de la "urna electoral". En caso de catástrofe (imposibilidad de participar en la apertura del mínimo), se contaba con dos tarjetas comodín las que estaban

[3] El chip de contacto es el ISO 7816, provisto por Gemalto

custodiadas en caja fuerte por el Secretario General y que permitían reemplazar a uno o dos Consejeros para lograr el quórum necesario en la "apertura de la urna[4]".

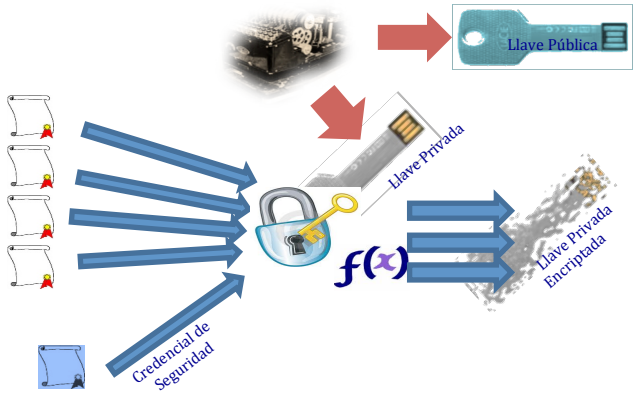

Figura Nº2: ***Diagrama proceso de encriptación.*** *Los certificados blancos corresponden a los de cada miembro del CE. Las aplicación genera una llave pública (verde) para encriptar los votos y una llave proivada para desencriptarlos. La llave privada es encriptada con la concurrencia de todos los miembros del CE presente en el acto de inicio del proceso.*

Para lograr este objetivo se desarrolló un algoritmo que permite encriptar un documento con la concurrencia de los miembros de el CE de manera tal que se pueda desencriptar en el futuro sólo con la existencia de un quórum definido que no dependa del 100% de los firmantes.

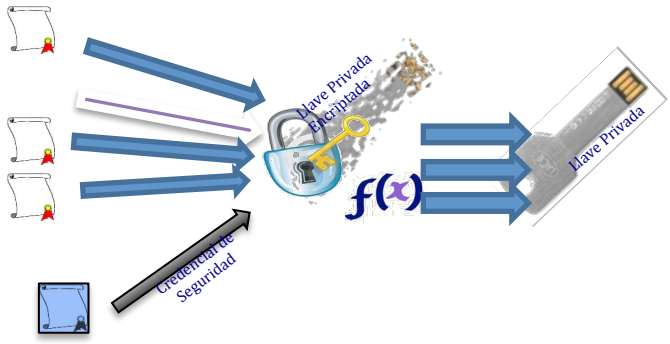

Figura Nº3: ***Diagrama proceso de desencriptación.*** *Los certificados blancos corresponden a los de cada miembro del CE presente al momento de abrir las urna. Existiendo quorum, el algoritmo permite desencriptar la llave privada para proceder a abrir la urna. Sólo en el caso de no haber quorum se hace uso de la credencial de seguridad.*

[4] Se mantiene el concepto de "urna", la realidad es que se trata del archivo con los votos encriptados por el Colegio Electoral.

- ***Plataforma de Servidores Exclusiva y cerrada***

La figura Nº 4 muestra un diagrama del diseño de la configuración. La plataforma de servidores, tanto de aplicación como de base de datos, se encontraba en un segmento de red aparte sin otros equipos, solo con los puertos web abiertos (https) y el resto cerrados por firewall que a su vez actuaba como balanceador de carga.

La base de datos además se encontraba replicada y con respaldos automáticos cada 5 minutos.

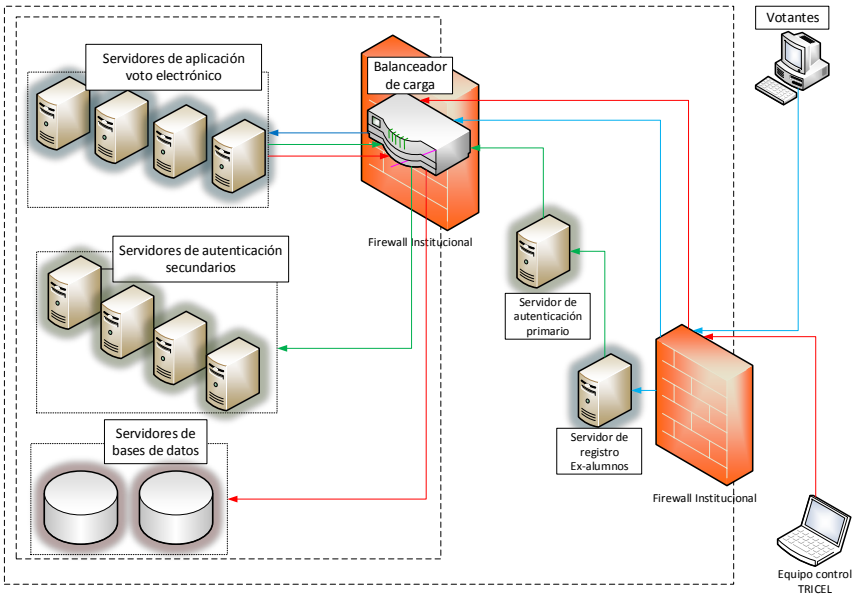

Figura Nº4: ***Diagrama de Distribución de Servidores y equipos.*** *Las lineas rojas representan las vías de comunicación a la base de datos, las lineas verdes representan las vías de comunicación a los servicores de directorio (autenticación) y las vías azules indican las vias de comunicación hacia los servidores de aplicaciones.*

El primer frente de seguridad corresponde al firewall institucional, el cual permite el ingreso a la base de datos solo desde el computador del CE para la recuperación en caso de desastre. Permite además el ingreso al registro (previo a las votaciones) para todas las personas y el ingreso al sistema de votación.

El segundo frente de seguridad se define dentro de esta red segura, a la cual se accede solo a través de un segundo firewall que actúa como balanceador de carga. Dentro de este segmento se permite la comunicación desde los servidores de aplicaciones hacia los servidores de autenticación (LDAP) y hacia la base de datos.

- ***Modelo de almacenamiento de sufragios seguro (encriptado)***

El voto se almacena encriptado en la base de datos con la llave pública generada por los miembros del CE. Estas llaves son generadas por medio de certificados estándar X509 y el algoritmo RSA.

La llave pública es almacenada en la base de datos para realizar el proceso de encriptación de los votos; al no contar directamente con la clave privada no es posible desencriptarlos hasta el fin del proceso, cuando en CE en un acto colegiado proceda a abrir la urna[5].

- ***Acceso a plataforma transferido al CE***

Con el objeto de asegurar que durante todo el proceso no existirá intervención humana a las máquinas y servicios implementados, a los servidores les fueron cambiadas las claves de ingreso en forma aleatoria, guardándose encriptadas dichas claves con las firmas electrónicas avanzadas de los miembros del CE donde sólo el quorum de ellos la puede rescatar y cambiar.

- ***Archivos del proceso respaldados y firmados electrónicamente***

Los documentos, archivos y código fuente fueron respaldados en un disco compacto y firmados electrónicamente por los miembros del CE, para asegurar una correcta auditoría de los aplicativos y de la documentación presentada.

- ***El Proceso***

- ***Conformación del Padrón***

El acto de conformación del Padrón electoral tiene varias etapas: A partir de toda la información de contactos con ex-alumnos que tiene la universidad en los diferentes departamentos, organizaciones y centros de contacto[6]. Junto con publicaciones en los principales diarios del país, se les envió correos de invitación a todos los datos disponibles para que participen en el proceso.

Cada participante debió registrarse como usuario de la USM; para asegurar su identidad, debió ingresar su ID Personal[7], el cual es verificado por la vía de un servicio web en el Servicio de Registro Civil e Identificaciones de Chile. Una vez registrado, se procedió a verificar su condición de titulado o graduado y el cumplimiento de los requisitos o inhabilidades que pudiese tener, para habilitarlo como elector e informarle su condición.

Una vez conformado el padrón a la fecha de cierre del mismo, se procede a obtener un archivo de resguardo que será utilizado en el proceso eleccionario y en la segunda vuelta si ocurriese.

---

[5] Se mantiene el concepto de "urna", la realidad es que se trata del archivo con los votos encriptados por el Colegio Electoral.

[6] AEXA: Una de las principales fuentes fue la Asociación de Ex Alumnos de la universidad.

[7] ID Personal: En Chile se le llama RUN, corresponde al Rol Único Nacional, es un rol único que tiene todo chileno o residente en el país. Para el caso de extranjeros, se les indicaba que para confirmar su identidad debían enviar por email, su cédula o identificador de su país de residencia.

- ***Certificación de las Aplicaciones y de la Plataforma***

Para asegurar que la plataforma respondiese al diseño, tanto desde las aplicaciones como desde la configuración se diseño una metodología para que una empresa externa procediese a certificar ambos elementos de la siguiente manera:

Una vez generada la última versión del software, se le entrega a la empresa certificadora una copia de todo el código fuente para que aseguren que las aplicaciones están acordes al diseño y no contienen ningún tipo de código malicioso.

Una vez realizada la configuración de la plataforma, se permite que la empresa certificadora verifique que esta está realizada de acuerdo a diseño.

Posteriormente al inicio del proceso, antes que el CE tome el control, la empresa certificadora debería asegurar que el software y configuración coincide exactamente con lo verificado previamente por ellos.

- ***Apertura del Proceso***

El proceso se inicia verificando la carga del padrón y sacando un respaldo de toda la base de datos, archivo que es firmado y encriptado electrónicamente por el Secretario General, para ser grabado en un CD y guardado como registro testimonial.

La generación de las llaves públicas y privadas para encriptar los sufragios se realiza con la aplicación desarrollada para ello y con la concurrencia de los miembros asistentes del CE más el Secretario General.

Para dar inicio a las votaciones, se hace uso de la segunda funcionalidad, la que se habilita una vez terminada exitosamente la primera, el CE genera una segunda llave de seguridad, se cambian todas las claves de administración de los servidores de la plataforma y se almacena la nueva clave encriptada con la segunda llave. Una vez realizado ello, el proceso de votación se habilita automáticamente.

- ***Proceso de Votación Electrónica***

El proceso de sufragio se realiza por el período de tiempo definido por el CE, a los electores se les recuerda por la vía de correos electrónicos enviándoles directamente la URL de la aplicación, información complementaria de los candidatos y tutoriales de uso de la aplicación.

Durante esta etapa, todo el control está en manos del CE quienes por la vía de una aplicación de monitoreo pueden visualizar solamente la cantidad de sufragios emitidos y su relación con el padrón electoral. Si hubiese una emergencia, el protocolo definido fue abrir la caja de seguridad de la llave de administración para entregárselas a los operadores con el fin de superar la contingencia y realizar nuevamente el cierre de la plataforma.

- ***Cierre y Publicación de Resultados***

El cierre del proceso comienza con la decisión del CE por medio de la concurrencia de la mitad más uno de los miembros que concurrieron a la apertura; el sistema les pide a cada uno de ellos su password y TUI. El primer paso es el instante en que se cierran los accesos a la plataforma, posteriormente pasados cinco minutos y para dar

tiempo a los electores que están en medio del trámite lo puedan finalizar, se cierra el resto de las transacciones que aún pudiesen quedar abiertas.

Finalizado el cierre, se realiza el respaldo de la base de datos completa y se procede a la certificación y resguardo de ese registro "testimonial" con el mismo protocolo de la apertura.

En tercer lugar, se lleva a cabo el escrutinio; proceso automático a partir del acto formal del CE abre la llave privada y la envía a un registro de la base de datos para proceder a la apertura y conteo de votos.

El escrutinio es finalizado con la verificación y certificación de los resultados, a través de la firma de un acta formal de resultados emitida directamente por el sistema.

La última etapa es la entrega de la administración de los servicios al equipo de TI de la universidad.

7. La Experiencia

Aunque la experiencia fue ejemplar y no tuvo ningún contratiempo o impugnación, la presentación de un solo candidato fue un factor no deseado que por una parte facilitó el proceso de cambio de paradigma y la aceptación del modelo, pero por otra parte dejó una sensación de frustración porque al no producirse una confrontación de opciones, no hubo suficiente interés por participar ni campañas fuertes de invitación por parte de los candidatos.

En consecuencia, las etapas del proceso se dieron de la siguiente forma:

- ***Conformación del Padrón***

De más de 20 invitaciones y recordatorios enviados a 34.000 direcciones de correos electrónicos, sólo se consiguió registrar a 783 electores se logró un padrón con 585 electores validados.

- ***La elección***

Las elecciones se realizaron desde el 23 de mayo a las 12:00 horas al 25 de mayo 12:00 horas. El CE estuvo compuesto por seis miembros y se obtubieron 367 sufragios; es decir un 63% de participación respecto al padrón.

- ***Resultados***

El resultado final fue la elección del candidato único con 309 votos y 58 votos en blanco; es decir con un 84% de los votantes.

8. Conclusión

Aunque por las razones expuestas el grado de masividad que se esperaba no se logró, permitió construir un modelo de procesos y aplicaciones seguras que permitirán continuar con las elecciones de estas características aplicando y mejorando sobre lo ya desarrollado.

El modelo de encriptación y manejo de claves colegiadas es una oportunidad, no solo para resolver los actos eleccionarios, sino para formalizar electrónicamente todos los

actos o decisiones que requieran la concurrencia de personas sin la exigencia de tener quórums de un 100% para resolver satisfactoriamente.

9. Referencias

http://registroexalumnos.usm.cl/index.php/80-noticias/comunicados/71-reglamento-general-sobre-votaciones-y-elecciones

http://www.registroexalumnos.usm.cl/index.php?start=4

http://www.registroexalumnos.usm.cl/