UNIVERSIDAD SAN PABLO - CEU

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA INFORMÁTICA

PROYECTO FINAL DE CARRERA

<TÍTULO DEL PROYECTO FINAL DE CARRERA>

Autor: José Carlos Jiménez Gómez
Director: Raúl García García

16 de octubre de 2015

Versión SVN

Rev: **-2**
por
URL :

Calificación

Pagina reservada para la calificación del proyecto

Resumen

Con el creciente desarrollo de la tecnología y su implantación en la mayoría de los campos de la vida cotidiana, es inevitable pensar en soluciones electrónicas para un elemento tan importante de nuestra sociedad como son los procesos electorales.

Encontramos procesos electorales en multitud de organizaciones, desde estados nacionales a empresas privadas, pasando por juntas de administraciones u organismos públicos.

En cambio, contrario a lo que puede parecer por el intenso uso de las nuevas tecnologías en campos como las transacciones bancarias, telemedicina, comunicaciones o gestiones con la Administración, en el mundo electoral no se está terminando de introducir el voto telemático a gran escala. De hecho, aunque encontramos algunas excepciones como pueden ser Estonia, Venezuela, Brasil y algunos territorios más reducidos, no se utiliza a estos niveles en la totalidad del proceso electoral, quedando reducido a algunas fases del proceso o, simplemente, a ninguna.

En este PFC, vamos a evaluar la implantación del voto telemático a pequeña escala para tratar de escalar los problemas que comportan a nivel nacional. Para ello, vamos a realizar un sistema de voto por Internet que soportará de forma íntegra las elecciones a la Junta de Escuela de la Escuela Politécnica Superior de la Universidad San Pablo CEU.

A partir de este desarrollo, trataremos de hacer frente, a pequeña escala, a los problemas que nos encontramos en estas grandes elecciones, aunque para ello tengamos que establecer requisitos que resulten exagerados para la consecución de la elección que implementamos por su simplicidad frente a un proceso a nivel nacional o autonómico.

Abstract

Abstract in English.

Agradecimientos

Es de bien nacidos ser agradecidos.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

Un sistema de voto por Internet puede tener diferentes formas de ser afrontado. Se puede diseñar un sistema basado en sufragio desde cabinas electorales gestionadas electrónicamente que envían el conteo a través de la red. En el marco opuesto, también se puede diseñar un sistema completamente distribuido en el cual el votante puede ejercer su derecho al voto desde cualquier dispositivo electrónico y cualquier lugar del planeta, enviando el contenido de su voto a través de Internet a la autoridad de recuento electoral.

Ambas soluciones son extremos opuestos de lo que entendemos como voto por Internet (i-voting) y que, en muchos documentos y ámbitos, se conoce también como voto electrónico (e-voting). Este término no es que sea erróneo, sino incorrecto, ya que carece de exactitud llamando a un subconjunto con el nombre del conjunto que lo contiene. El voto por Internet, obviamente, se considera voto electrónico, pero no todos los sistemas de voto electrónico se realizan a través de Internet. ********** IMAGEN DOS CONJUNTOS, UNO (E-VOTING) CONTIENE AL OTRO (I-VOTING) **********

Este proyecto trata de entrar en la problemática del voto electrónico remoto frente al presencial, de las reticencias sociales y tecnológicas que influyen en su reducida implantación en procesos electorales de gran importancia y alto número de electores. Para ello, vamos a reproducir la situación a escala reducida. Plantearemos una posible solución al proceso necesario para llevar a cabo las Elecciones a la Junta de Escuela de la Escuela Politécnica Superior de la Universidad San Pablo - CEU.

Con este planteamiento es obvio que no vamos a solucionar las trabas técnicas y sociales del voto por Internet a nivel de unas elecciones legislativas en, por ejemplo, España. Es un tema que se escapa del objetivo de este PFC, pero

sí que vamos a tratar de identificar algunos de los agentes influyentes y buscar una posible solución aplicable a la elección a la Junta de Escuela.

Así, conseguiremos dos objetivos. Por un lado, estudiar la dificultad existente para la implantación del voto por Internet en las elecciones nacionales. Por otro, un soporte electrónico al proceso completo de las Elecciones a la Junta de Escuela, con el cual obtendremos una mejora significativa en el mismo respecto a procesos anteriores.

Antes de entrar en detalle en el proceso, habrá que definir el tipo de votación que queremos implementar. No se habla en este PFC de voto electrónico como tal, ni siquiera de voto electrónico remoto. Lo que se quiere implementar es una solución de voto por Internet, en el que no haga falta la presencia física del votante en el centro de votación, que tenga la oportunidad de ejercer su derecho al voto desde cualquier punto del planeta con conexión a Internet. Este detalle, que puede parecer trivial al querer separarlo del concepto de voto electrónico, en realidad es fundamental. En un próximo capítulo se ahondará en ello, pero podemos avanzar que una de las grandes diferencias a tener en cuenta es que con voto electrónico remoto, podemos utilizar máquinas de votación (que también emitirían el voto por Internet), las cuales pueden generar un recibo con el voto emitido por el votante, al estilo de las papeletas que llenan la urna electoral, mientras que con el voto por Internet puro, esto no es tan obvio. Con este mecanismo, la auditoría es más simple para el voto electrónico con máquinas en el centro de votación, pues se podrían contar las papeletas generadas. ¿Qué ocurre con el voto por Internet, en el que no se generan estos recibos ni hay una urna física donde se depositan? ¿Qué ocurre si el sistema tiene fallas y no se contabilizan (o lo hacen de forma incorrecta) los sufragios, teniendo en cuenta que puede ser imposible un conteo físico de papeletas al no existir estas? Como estas, hay muchas cuestiones a las que el voto por Internet debe dar solución de forma fiable antes de poder acometer su implantación en procesos electorales de envergadura e importancia.

La forma de llegar a la solución buscada debe comenzar identificando los factores que afectan a un proceso electoral general y, a continuación, personalizar los que se encuentran en el que vamos a estudiar. Una vez identificados estos agentes, definiremos las fases que comportan unas elecciones y estudiaremos cómo podrían ser apoyadas tecnológicamente, evaluando cómo llegar al punto óptimo de integración con el sistema tradicional para mejorar el proceso.

La primera fase se concentrará en desarrollar los sistemas asociados a la fase preelectoral. En ella, se recoge el censo electoral y se identifican tanto los

candidatos como los diferentes cargos que se votan.

La segunda fase, la electoral, la identificamos con los procesos que se requieren durante el periodo que dura la elección (ya sea un día o varios). Esta consistirá en desarrollar los sistemas de identificación y validación de votantes, el sistema de votación, ss

1.1. Motivación del Proyecto

********** COMENTADO POR AHORA ********** ********** FALTA. ¿CÓMO SE INDENTA CUANDO TAN SÓLO HEMOS HECHO UN SALTO DE PÁGINA **********

1.2. Antecedentes

En la actualidad, son muchos los proyectos que tratan de incluir el voto electrónico en los procesos electorales por todo el planeta. Estos intentos, de hecho, no se limitan a pequeños sufragios de entidades privadas o gobiernos locales, ya que se han propuesto múltiples paradigmas diseñados para ser implementados en elecciones a nivel estatal, como se puede ver en las experiencia de Estonia, país en el que se desarrolla la votación electrónica remota vinculante con mayor censo activo.

El voto electrónico se lleva tratando de desarrollar e implementar desde hace bastante tiempo. Concretamente, podríamos datar el comienzo en el año 1868, cuando el inventor estadounidense Thomas Alva Edison (1847-1931) registró su primera patente, consistente en un instrumento simple para el recuento mecánico de votos. El instrumento se podía colocar en la mesa delante de cada congresista y tenía dos botones, uno para el voto a favor y otro para el voto en contra. Pese a considerarlo un avance, no consiguió ser aceptado en el Congreso de Washington, donde le dieron el siguiente motivo para argumentar el rechazo de los representantes a esta nueva tecnología: XXXXOJO "*If there is any invention on Earth that we don't want down here, that is it.Joven, si hay en la tierra algún invento que no queremos aquí, es exactamente el suyo. Uno de nuestros principales intereses es evitar fraudes en las votaciones, y su aparato no haría otra cosa que favorecerlos*".

A partir de este intento, el voto electrónico ha avanzado tecnológica y socialmente, logrando herramientas más sofisticadas y seguras en conjunción con un

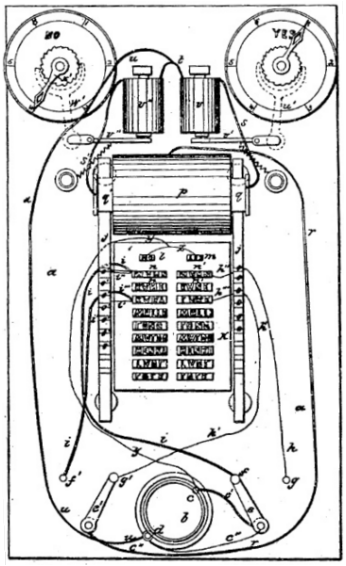

Figura 1.1: *U.S. Patent 0,090,646 – Electrographic Vote-Recorder: Primera patente de Thomas A. Edison. Permitía un voto de tipo 'A favor' o 'En contra' a través de dos interruptores. (1869). Fuente: Wikipedia*

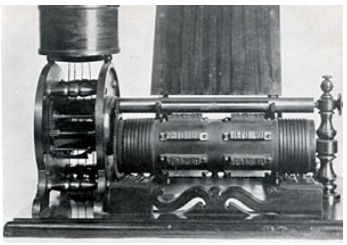

Figura 1.2: *Electrographic Vote-Recorder: Fotografía del invento de Thomas A. Edison. Fuente: Rutgers.edu*

entendimiento, comprensión y, en algunos casos, aceptación de su uso. Estos factores han hecho posible que se hayan podido implementar soluciones e integrarlas en procesos electorales reales, ya sea a nivel nacional o de entidades o estamentos.

Se considera que el inicio del desarrollo del voto electrónico moderno está datado en 1964, año en el que site condados de EEUU utilizaron un sistema de voto electrónico para las Elecciones Presidenciales.

********** UN POQUITO MÁS DE HISTORIA ******* HABLAR DE DRE Y TARJETAS PERFORADAS **********

En el año 1981 se produce un hito en la historia del voto electrónico. El criptógrafo David Chaum publica [5] la primera propuesta de un sistema criptográfico diseñado para proteger la privacidad del votante. Entre otras propuestas, en esta publicación se recoge su primera idea de un sistema verificable *end-to-end*, basado en el uso de redes mixtas (mix networks o mixnets).

En la época actual, prácticamente la totalidad de los procesos electorales implementan soluciones tecnológicas para algunos pasos de la fase de recuento de votos, con el fin de un recuento más rápido de votos y una difusión de resultados sólo varias horas después del cierre de los colegios electorales. Es el caso de, por ejemplo, España, donde tanto el Ministerio del Interior como las Comunidades Autónomas requieren que el conteo provisional de los votos se realice en un tiempo corto durante la misma noche electoral.

En este caso, las empresas adjudicatarias implementan soluciones tecnológicas para llevar a cabo el proceso. Así, se puede destacar la tecnología electoral de empresas como Indra [24] - pionera en uso de tablets para enviar información de recuento o la Mesa Administrada Electrónicamente que agiliza y da soporte a la labor de los miembros de mesa, desde gestión del censo a generación de actas de escrutinio - o Scytel [26], referente a nivel mundial en proyectos de voto electrónico, tanto presencial como remoto.

1.3. Estado de la cuestión

1.3.1. Voto electrónico

Cuando se habla de voto electrónico, una primera acepción del término se refiere a los procesos electorales cuyas fases pueden llevarse a cabo haciendo uso de tecnologías de la información. Dentro de estas fases susceptibles de ser implementadas con protocolos informáticos se incluyen el registro de votantes,

diseño de mapas de distritos o circunscripciones electorales, y la gestión, administración y logística electoral; así como el escrutinio provisional o definitivo, transmisión de resultados y difusión de los mismos, o el sufragio del voto en sí mismo.

No obstante, una definición más simple del voto electrónico se refiere únicamente a este último acto de votar, ya sea a través Internet o simplemente utilizando sistemas que no estén intercomunicados a través de Internet, aunque sí con un servidor receptor del voto.

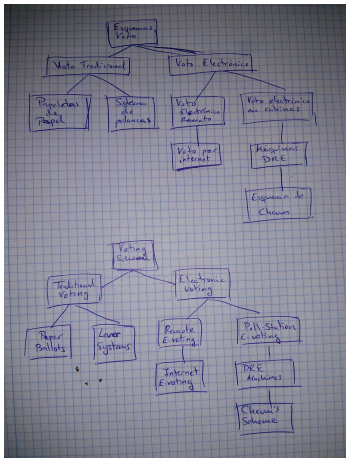

Figura 1.3: *Categorización de los sistemas de voto*

Podemos estudiar el voto electrónico separándolo en varios niveles, dependiendo de su implantación en el proceso.

- Nivel 0

  Es el sistema de voto tradicional, sin hacer uso de elementos electrónicos para llevar a cabo ninguna fase del proceso. Es el sistema que se ha venido utilizando desde las primeras votaciones hasta bien entrado el siglo XX y todavía en uso en muchos territorios del planeta.

- Voto electrónico sustitutivo

  En este nivel, se sustituyen algunos procedimientos manuales o elementos utilizados en el voto tradicional por sistemas electrónicos determinados. Lo que se intenta es que el proceso de votación sea lo más parecido al que se ha venido llevando a cabo, pero pudiendo utilizar avances técnicos que mejoren el procedimiento en algunos de los puntos del mismo. Así, dependiendo de la legislación, el nivel democrático y social y la aceptación de la innovación tecnológica, se han adoptado procesos electorales en los que

se hace uso de algunos elementos tales como tarjetas magnéticas o documento de identidad electrónico (para identificar al votante o incluso para emitir el voto), urnas de votación electrónica que recuentan los votos de forma automática (RFID, lector código de barras, etc.), pantallas de votación para selección de candidaturas (en EEUU es una de las formas en las que se elige la opción a votar), sistemas de totalización y consolidación de resultados (para evitar el escrutinio manual), e incluso sistemas para guiar el recuento definitivo pasados unos días de la jornada electoral. Así podemos encontrar muchos más ejemplos.

Como se puede observar, todos los sistemas que se tienen en cuenta en este nivel están orientados a sustituir un elemento del proceso tradicional de votación. Todos están pensados para tener una función en el local electoral, ya sea para la identificación del votante, emisión del voto, escrutinio o (en otro tipo de local electoral) recuento definitivo. Aquí podemos observar, de paso, diferentes fases del proceso electoral, que son fácilmente reconocibles.

- Voto electrónico remoto

  En este nivel, el concepto del voto traspasa el local electoral común. Se trata de que el voto se transmita desde un punto de votación a una ”urna remota”. Dependiendo del punto de origen, podemos dividir este grupo en dos subgrupos, uno en el que los diferentes colegios electorales están interconectados entre si y otro en el que el voto se emite desde cualquier punto con conexión a Internet.

  - Voto telemático en local de votación

    En esta primera aproximación al voto telemático sigue pensándose en el sistema de voto tradicional en cuanto a que el votante ha de acudir a un local de votación acondicionado para ejercer su derecho al voto. En este local, encontraría una serie de sistemas de identificación (tanto personal frente a los miembros de mesa - como en el sistema tradicional - como telemático frente a una autoridad certificadora remota a través de una identificación digital) para superar el primer paso del proceso. Una vez cerrada la votación, se conectarían los diferentes colegios electorales para comunicar cada uno sus escrutinios y pasar los resultados para la fase de totalización.

  - Voto por Internet

> La aproximación del voto por Internet es la más ambiciosa en términos tecnológicos y de seguridad. En esta, el votante puede ejercer su derecho al voto desde cualquier punto conectado a Internet, como puede ser su propia casa o el lugar en el que se encuentre de viaje. La identificación del votante debe ser digital y remota. El voto emitido tiene que ser transmitido a la urna electrónica remota que corresponda. No obstante, desde un punto de vista sociológico, este sistema tiene todavía una serie de retos que debe cumplir, como es el acceso universal al proceso de votación, ya que es complicado asegurar que la totalidad de la población podría hacer uso de un sistema informático de este tipo. Además, encontramos dificultades en cuanto a fraude electoral, ataques al sistema, tolerabilidad al fallo, etc.

El término de voto electrónico, por tanto, se utiliza también para referirse a los novedosos sistemas electorales que tratan de automatizar algunas fases del proceso, como autenticación de votantes, sufragio y escrutinio de los votos y difusión de los resultados. Todos estos sistemas que, además de hacer uso de tecnologías de la información para la automatización de estos procesos, se basen en una comunicación de redes telemáticas para interconectar votantes con mesas electorales - urnas digitales - y estas con los centros de procesamiento de resultados se pueden encuadrar en el nivel 3 de la clasificación anterior.

Son estos sistemas los que están en auge para los investigadores de protocolos electorales. Con el aumento de la participación ciudadana en Internet, en la sociedad digital, la gente realiza todo tipo de procesos cotidianos a través de la red de forma remota, ya sea interactuar con las entidades estatales o municipales con trámites burocráticos, multas o pagando impuestos, gestionando los recursos familiares o de la empresa con el banco desde casa o el despacho, o incluso compras por Internet o consumición de ocio digital. Con este panorama es cuestión de tiempo que cierto sector demande una actualización de los procesos de votación. He aquí donde el voto electrónico remoto tiene que estudiarse si es el candidato ideal para cubrir este nicho o, sin embargo, los riesgos de seguridad y procedimiento que sus detractores le achacan realmente imposibilitarán este cambio en un corto período de tiempo.

Plantean para los expertos un conjunto de retos, tanto desde el punto de vista tecnológico, sobre todo a nivel de seguridad del sistema y privacidad del votante, como a nivel social, ya que estos sistemas electrónicos deben garantizar la misma confianza al votante que la que le proporciona el sistema de voto tradicional.

Los sistemas de voto electrónico deberían tener como base antes de la imple-

mentación la consigna de aportar al proceso al menos las mismas garantías de seguridad que el sistema tradicional al que está sustituyendo / complementando. El voto presencial tradicional permite un recuento de la votación, lo mismo que la mayoría de los sistemas del primer nivel que hace uso de urnas electrónicas, pues generan un recibo o papeleta física. En cuanto al último nivel, esto no está tan claro, pues la mayoría de estos sistemas no generan un resguardo físico de los votos electrónicos emitidos, por lo que es complicado pensar en un recuento en caso de fallo o de duda de la autoridad electoral o del propio electorado.

Según publican *Fujioka, Okamoto y Ohta* [10], un sistema de voto secreto es *seguro* si cumple con los siguientes requisitos:

Completitud (Completeness) : Todos los votos válidos son contados de correctamente.

Solidez (Soundness) : Un votante deshonesto no puede interrumpir la votación.

Privacidad (Privacy) : Todos los votos deben ser secretos.

(Unreusability) : Ningún votante puede votar dos veces.

Elegibilidad (Elegibility) : Nadie que no tenga permitido el voto puede votar.

Fiabilidad (Fairness) : Nada debe afectar la votación.

Verificabilidad (Verifiability) : Nadie puede falsificar el resultado de la votación.

A estos requisitos básicos, el equipo de Fujioka añade otros cuatro que considera importantes para la correcta implementación de un sistema de voto electrónico:

— **(Robustness)** : faulty behavior of any reasonably sized coalition of participants can be tolerated. In other words, the system must be able to tolerate to certain faulty conditions and must be able to manage these situations

— **(Universarl Verifiability)** : Any part can verify the result of the voting.

— **(Receipt Freeness)** : Voters are unable to prove the content of his/her vote

Sin recibo (Receipt Freeness) : El votante no necesita una prueba del voto realizado.

— **(Incoercibility)** : Voter cannot be coerced into casting a particular vot by a coercer.

Sin duplicados (Non-Duplication) : Nadie puede duplicar el voto de otra persona.

Participación Pública (Public Participation) : La lista de quiénes votaron o quiénes no lo hicieron ha de ser pública.

Corrección Privada de Errores (Private Error Correction) : Un votante puede probar que su voto no fue contado correctamente sin tener que revelar qué opción votó.

A partir de esta primera definición de los requisitos del voto electrónico, muchos equipos de desarrolladores o teóricos de infraestructuras para el voto electrónico han redactado sus propias interpretaciones, aunque suelen ser análogas a las ofrecidas por Fujioka. Por ejemplo, las propiedades que debe tener un sistema de voto electrónico a través de Internet, según publican desde la Universidad de Extremadura [7] son las siguientes:

Universal Todos los implicados en la toma de una decisión tienen voz y parte en ella, es decir, que todos aquellos ciudadanos que tienen derecho a votar podrán hacerlo a través de las redes telemáticas. Luego constarán unos requerimientos mínimos que permitan a los usuarios realizar sus votos a través de Internet.

Libre Los usuarios que tengan derecho a realizar una votación tendrán total libertad para elegir si ejercen su derecho a través de Internet o por cualquier otro mecanismo dispuesto para este fin. No se podrá obligar a los usuarios a realizar su voto de una determinada forma. Los usuarios del sistema de votación podrán escoger qué votar, cómo votar, e incluso si quieren o no votar. Luego la libertad del ejercicio de la votación estará referida a varios aspectos: libertad para los usuarios que realizan su voto, libertad para la orientación del voto, y libertad de información antes, durante, y después de realizar su voto. No deberán existir restricciones de acceso al sistema de votación, es decir, el sistema de votación deberá ser independiente del sistema operativo que tengan los usuarios o del navegador que éstos utilicen. Tampoco deberán existir restricciones físicas o lógicas que impidan, por ejemplo, a una persona discapacitada ejercer su derecho a votar.

Directo Será el usuario del sistema de votación el que personalmente emita su voto, es decir, éste no podrá delegar su voto en otra persona. El votante deberá tener una implicación personal dentro del proceso de votación. Esto plantea el problema de la autentificación del voto y el votante, es decir, se

debe garantizar que quien vota es quien dice ser, que no existen problemas de suplantación de personalidad y, que cuando el votante ejerce su derecho a votar, éste se lleva a cabo. Para solucionar estos problemas de autentificación, los usuarios dispondrán de su propio dispositivo criptográfico, la cual, mediante el uso de claves por parte del usuario permitirá garantizar todo lo anterior. El usuario utilizará las claves y certificados almacenados en su dispositivo junto con las funciones que éste le aporta tanto para registrarse en el sistema de votación, como para proceder al ejercicio del voto. El motivo de separar estos dos procesos es el de asegurar la confidencialidad del voto como se explicará posteriormente.

Igual El sistema de votación electrónico deberá ser igual para todas las personas, aunque podrá tener algunas diferencias, por ejemplo para personas disminuidas. Luego se deberá permitir el acceso a todas las personas que tengan algún tipo de necesidad especial. El sistema deberá ser confiable, es decir, se deberá garantizar que funciona sólo como se prevé que va a funcionar, sin puertas traseras ni trampas ocultas que modifiquen los resultados. Además el sistema deberá ser fiable, es decir, deberá ser capaz de funcionar en condiciones adversas, se recuperará ante fallos, incorporará mecanismos de seguridad,...

Secreto El voto emitido por un usuario sólo podrá ser conocido por él y por la Autoridad encargada del recuento de votos. Para asegurar esta propiedad la fase de votación se divide en dos partes, la autenticación y la votación en sí. El voto emitido por un usuario nunca podrá ser asociado con el usuario que lo emite.

Hasta aquí están las características inherentes a un sistema de votación tradicional, el realizado hasta ahora en cualquier proceso electoral que haya habido en España, por ejemplo. A conrinuación, añaden una serie de propiedades ligadas a las propuestas por Fujioka en cuando al voto electrónico:

Autentificación Sólo se permitirá emitir un voto a aquellos usuarios que estén debidamente autorizados. Para el cumplimiento de este requisito, se requerirá a los usuarios estar en posesión de un certificado digital (Anexo II) almacenado en el dispositivo criptográfico. Para asegurar la identidad de los usuarios se deberá crear un censo electrónico de posibles votantes, el cual se deberá ir actualizando no sólo con los votantes que realizan sus votos a través de Internet, sino que además deberá ser actualizado a través de todas las formas posibles de votación. Esto es para evitar que un

votante realice su voto en más de una ocasión, por ejemplo, a través de Internet y físicamente en un colegio electoral.

Unicidad A cada usuario con derecho a votar, sólo se le deberá permitir realizar su voto una sola vez. Esto se consigue, como se comentó en el apartado anterior, manteniendo una base de datos totalmente actualizada por los distintos administradores de cada una de las formas de voto permitidas.

Integridad Un voto, una vez que ha sido emitido y registrado, no podrá ser modificado o eliminado por ninguna entidad. El sistema deberá tener mecanismos que permitan la realización de copias de seguridad, ficheros donde se apunten las operaciones que se realizan y quien la realiza, etc. para solucionar cualquier posible duda acerca de la integridad de un voto.

Confidencialidad El voto realizado por un usuario sólo será conocido por él, es decir, nadie podrá averiguar qué votó un usuario. La entidad encargada del recuento de votos no podrá determinar qué usuario emitió un determinado voto. Tampoco la entidad encargada del registro de los usuarios podrá saber el voto que realiza ese usuario.

Fiabilidad Una vez el voto es emitido, éste queda registrado, y el sistema de votación no perderá ningún voto, aún en el caso de producirse algún fallo en algún dispositivo de votación o comunicaciones ajenos al sistema de voto. Se deberá dar a los usuarios la fiabilidad de que todos los votos, una vez el usuario los ha emitido, son incluidos en el recuento final.

Flexibilidad Para permitir que todos los usuarios puedan emitir sus votos a través de Internet, independientemente del sistema operativo o navegador con el que trabajen o de la discapacidad que tengan. Para emitir un voto a través de Internet sólo será necesario estar en posesión de nuestro dispositivo criptográfico junto con su certificado digital almacenado, para identificar de forma totalmente segura a los usuarios.

Comodidad Los usuarios podrán votar rápidamente a través de Internet, independientemente de sus habilidades o conocimientos informáticos. Para conseguir esta comodidad, pueden ayudar entornos parecidos a las papeletas tradicionales.

Ergonomía Ayuda a los usuarios en el uso del sistema (eficiencia de los diálogos, brevedad de los mensajes, alarmas...), gestión de errores (previniéndolos y corrigiéndolos cuando se presenten), y compatibilidad entre las

características personales de los usuarios (memoria, percepción, hábitos, habilidades, edad) y los diálogos del sistema.

1.3.2. Certificados Digitales

La propia web de la Fábrica Nacional de Moneda y Timbre [4] indica que *un certificado digital es un documento electrónico que asocia una clave pública con la identidad de su propietario*. Complementa la definición añadiendo que *adicionalmente, además de la clave pública y la identidad de su propietario, un certificado digital puede contener otros atributos para, por ejemplo, concretar el ámbito de utilización de la clave pública, las fechas de inicio y fin de la validez del certificado, etc. El usuario que haga uso del certificado podrá, gracias a los distintos atributos que posee, conocer más detalles sobre las características del mismo.*.

La utilidad de los certificados digitales, simplificando el contexto, se resume en *asegurar que una determinada clave pública pertenece a un usuario en concreto*.

Con las tecnologías actuales, la economía ha vuelto su desarrollo al comercio electrónico y las relaciones remotas. Muchas transacciones que antes se realizaban en persona han evolucionado al mundo digital, por lo que, para la mayoría de ellas es indispensable poseer mecanismos que puedan demostrar que los sujetos intervinientes en la comunicación están unívocamente identificados y con la seguridad de que no se produce suplantación.

Una herramienta fundamental para cumplir con este propósito ha sido el desarrollo de las certificaciones digitales.

********** MÁS MÁS MÁS MÁSSSSSSSS **********

1.3.3. NFC

1.3.4. Smart Cards

Una SmartCard

1.3.5. DNIe

****

DNIe

Añadir DNIe 3.0 **********

1.3.6. Tarjeta Universitaria Inteligente - TUI

1.3.7. Experiencias de Voto Electrónico

En lo referente al voto electrónico...

En cuanto al estado de la cuestión del voto por internet, como hemos destacado, la experiencia más ambiciosa es, sin duda, las elecciones que se llevan a cabo en Estonia (1.3.8.1), que, desde el año 2005, proveen de un sistema de voto por internet a un cierto sector de la población.

Es destacable el desempeño de empresas como la española Scytl, que ha implementado sistemas de voto por Internet para voto desde el extranjero para algunos condados de Estados Unidos, ciertos cantones de Suiza y varias provincias de India, la mayor democracia del mundo (en número de votantes). Otra empresa española, Indra, también tiene soluciones de voto por Internet utilizados para elegir las cúpulas directivas de organismos como la Guardia Civil, universidades como la UAH (Universidad de Alcalá de Henares) o la UNED (Universidad Nacional de Educación a Distancia) e incluso de partidos políticos, como es el caso de UPyD (Unión Progreso y Democracia).

1.3.8. Voto por Internet (i-voting)

Dentro de las soluciones de voto electrónico telemático, es importante el desarrollo que se ha hecho en cuanto al voto por Internet.

1.3.8.1. Estonia

Estonia. Estonia es quizá el ejemplo más destacado en cuanto a la utilización del voto por Internet en elecciones a nivel estatal. Desde el año 2005 lleva usando una solución de voto electrónico remoto no presencial complementando al voto tradicional.

El impacto del voto electrónico sobre el electorado estonio ha ido evolucionando en cada comicio. En el 2005, el primer año en que se comenzó a utilizar, no llegó al 2 % de los votantes los que se decantaron por votar por Internet, mientras que en el 2014, este porcentaje superó el 30 % de los sufragistas.

********** Adjuntar TABLA de participación histórica **********

********** **********

Estonia es el primer estado que utiliza, oficialmente, el voto electrónico remoto por internet de forma vinculante. Este sistema puesto en práctica en el año 2005

Elección	Tipo	IV	% tv
2005	Elecciones Locales	9.317	1,90 %
2007	Elecciones Parlamentarias	30.275	5,50 %
2009	Elecciones Parlamento Europeo	58.669	14,70 %
2009	Elecciones Locales	104.413	15,80 %
2011	Elecciones Parlamentarias	140.846	24,30 %
2013	Elecciones Locales	133.808	21,20 %
2014	Elecciones Parlamento Europeo	103.151	31,30 %

Tabla 1.1: *Evolución del voto por internet en Estonia*

es una parte de un plan de modernización del país báltico. De hecho, previamente a la puesta en producción del sistema electoral, se comenzó a desarrollar en el años 2000 un despliegue técnico importante para la implantación del documento de identidad electrónico, junto con mecanismos de comunicación con la Administración para facilitar los trámites con la misma por parte de los ciudadanos de forma electrónica y remota.

La ley electoral estonia permite a los votantes ejercer su derecho al voto de tres formas:

a) Voto tradicional. Los votantes pueden acudir a los colegios electorales e introducir su voto en la urna previa identificación del votante por parte de los miembros de la mesa.

b) Voto postal. Los votantes estonios tienen la posibilidad de acudir en unas fechas determinadas anteriores al día electoral a unas Estaciones de Votación, que funcionan de forma análoga a Correos en España, donde pueden entregar el voto en papel y una acreditación que le identifique. Esta Estación se encarga de hacer llegar el voto y la identificación a la mesa o Distrito Electoral donde el votante esté censado.

c) Voto por Internet. Durante un período de tiempo anterior al día electoral, los votantes tienen la posibilidad de entregar el voto por medio de Internet.

Aunque el votante haya emitido su voto de forma electrónica, la Ley Electoral estonia permite al mismo ejercer su voto de cualquiera de las otras dos formas invalidando su voto electrónico. Es decir, que si una vez votado por Internet, el votante decide votar por correo, éste voto anulará el emitido por Internet. Lo mismo pasaría si decidiese votar presencialmente el día electoral, que su voto emitido por Internet quedaría anulado y fuera del escrutinio. Este hecho es una medida de la Autoridad Electoral para proteger a los votantes frente a la **coacción**, proveyendo de un mecanismo por el cual un votante que haya elegido una formación

determinada por presiones de terceros podría libremente cambiar la dirección de su voto una vez emitido el primero.

Son requisitos fundamentales de este sistema de voto electrónico remoto la seguridad, confiabilidad y la precisión, así como proveer de mecanismos eficaces contra la coacción. Otra necesidad importante del sistema es su acceso, que debe ser prácticamente universal, lo cual implica que sea fácil y accesible para los usuarios y que funcione en la mayoría de las plataformas tecnológicas.
Hay una serie de puntos, recogidos en [19], que consiguen que el sistema satisfaga tales requisitos:

1. Uso de ID-cards o Mobile ID para la identificación de los votantes.
2. Un votante puede emitir cualquier número de votos durante el periodo habilitado para la votación electrónica. El último voto enviado será el único que cuente en el escrutinio. No obstante, si el votante se encuentra bajo algún tipo de coacción, siempre podrá volver a votar más adelante (cuando no ejerzan presión sobre su decisión) y este último será el que cuente. Así se intenta minimizar el riesgo de la coacción.
3. Prioridad del voto tradicional. Si el votante ejerce su derecho al voto de forma presencial, cualquier voto que hubiese emitido de forma electrónica será cancelado y no se contará en el escrutinio.
4. Todos los servidores en el sistema de voto son seguros y siempre estarán bajo monitorización durante el periodo de la votación.
5. El servidor de almacenamiento de voto está detrás de un firewall. Nadie puede acceder a este servidor desde Internet.
6. El servidor de conteo de votos está offline, sin conexión a Internet y asegurado por medio de clave privada compartida.
7. Todas las comunicaciones a través de Internet usan cifrado SSL.
8. El cifrado y la firma digital usan un mecanismo de cifrado RSA.

******** EXPLICAR UN POCO EL FUNCIONAMIENTO Y ANALIZARLO ******* ******** SEGÚN BELLEBONI, EN SUS CONCLUSIONES: - Interesante por ser una elección a nvel nacional y vinculante. - Aceptación nacional, con nº votantes en tendencia creciente y dando validez a los votos emitidos por este medio. Debilidades: - No uso de mecanismos seguros que garanticen la protección del

derecho a voto secreto. - El voto no está protegido por mecanismos de firma ciega, anonimizadores, ni mecanismos equivalentes (y se conserva de 4 a 10 días almacenado junto a la identificación del votante), sino que traslada al sistema por Internet las debilidades ya existentes en el voto tradicional (¿?) **********

La importancia que tiene el sistema de voto utilizado en Estonia radica en el hecho de que provee un mecanismo de voto por Internet a un potencial de votantes consistente en el 100 % de la población de uun estado democrático. Hasta el momento de su implantación, esto no ocurría. Se daban casos en los que se proporcionaba un sistema electrónico remoto a diversos espectros de la población, como podían ser los residentes en el extranjero, los militares en misiones activas o los focos de posibles proyectos pilotos.

Es destacable que, con el objetivo de alcanzar a la totalidad de la población, incluso, el propio estado estonio aumentara el desarrollo de infraestructura tecnológica en el país para intentar reducir la brecha digital de sus habitantes, tratando de proveer el acceso a Internet a la mayor parte del país. Igualmente importante fueron los esfuerzos por la certificación digital, teniendo como punto esencial la implantación del documento nacional de identidad electrónico para la totalidad de la población.

La mayoría de los estados no pueden implantar unas elecciones como las llevadas a cabo en Estonia por diversos motivos, véase el miedo a la falta de transparencia, fraude, logística o, en muchos casos, ilegalidad con respecto a las leyes electorales actuales.

En diversos países se ha logrado implementar sistemas reales de votación deslocalizada por Internet en varios de sus territorios, alternativamente y al mismo nivel que el sistema tradicional presencial. Un ejemplo veremos que es Suiza con los proyectos de varios de sus cantones. No es comparable a la experiencia estonia, pues cada cantón se rige de forma diferente y son diferentes empresas las que realizan los desarrollos del sistema independientemente del resto, además de que no todos los cantones han implementado estos sistemas remotos.

1.3.8.2. ¿¿¿¿¿**********Noruega**********????

1.3.8.3. Suiza

El estado suizo se divide administrativamente en cantones. Estos cantones son los responsables de la celebración de procesos electorales en sus territorios. Con esto, varios de ellos, impulsados por el Estado, han dedicado mucho esfuerzo al estudio y desarrollo del voto por Internet para poder implementarlo

de forma general.

Con el objetivo de la implantación del voto electrónico, el estado suizo marcó tres fases de actuación como línea a seguir para la resolución de estudios y pruebas pilotos previas a una futura utilización de este sistema con garantías de viabilidad y seguridad. [1] En una primera fase, de 2000 a 2002, se realizaron una serie de estudios e investigaciones que derivaron en la creación de programas piloto de voto electrónico. De 2002 a 2006, tres cantones - Neuchatel, Ginebra y Zurich, comenzaron a realizar pruebas piloto que mostraron que era posible implantar el voto electrónico remoto en Suiza, lo cual acentuó el apoyo del Gobierno en el proyecto. A partir de 2006, las pruebas piloto se expandieron a otros cantones, utilizando estos los sistemas desarrollados por el cantón de Zurich o el de ginebra. En 2010 ya eran 12 los cantones que realizaron pruebas pilotos en los comicios del 28 de noviembre. El número de votantes que podían votar de forma electrónica ascendía a 193.236 personas aunque, sin embargo, tan sólo 28.192, no llegó al 15 %, lo hicieron de esta forma. Sin embargo, en 2011, el Gobierno Federal

1.3.8.4. UNED

(Indra)

1.3.8.5. Universidad del País Vasco

(Scytel)

1.3.8.6. Votescript

El esquema de votación telemática Votescript tiene su origen en el proyecto de investigación *Votación Electrónica Segura basada en criptografía avanzada* [3], denominación de la cual adquiere el nombre, Votescript. Este proyecto es una colaboración entre el grupo de la Universidad Politécnica y la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (una de las principales entidades emisoras de certificados digitales de España).
A partir de este proyecto de investigación, los autores publican diversos artículos sobre el funcionamiento y alcance de los resultados obtenidos. En este apartado, nos basamos en la versión más actual del proyecto, desarrollado en su tesis doctoral [22] por una de las autoras del original, la Dra. Emilia Pérez Belleboni.
En esta tesis, además de analizar el estado del voto telemático, teniendo en

consideración, esquemas, problemas y riesgos, realiza un estudio de varias implementaciones reales a nivel nacional, como por ejemplo un extenso análisis del procedimiento electoral electrónico de Estonia 1.3.8.1. No obstante, a partir de estos análisis, desarrolla el esquema que proponen, con base en el Votescript original, evolucionándolo para solucionar las debilidades del resto de sistemas y para su aplicación en la elección de representantes para el Parlamento Europeo. En contraposición a los sistemas que estudia en la tesis, el sistema Votescript centra sus esfuerzos en la superación de debilidades identificadas en los anteriores, en especial en la fase de identificación del votante. En elecciones como las del Parlamento Europeo, una entidad supranacional, es muy importante que la identificación de los votantes se pueda realizar electrónicamente de una forma altamente confiable, pues deben ser válidas no sólo en el país del propio votante, sino en el resto de países europeos.
El esquema que propone Votescript define la necesidad de unos puntos específicos de votación, centros donde han de acudir los votantes a votar telemáticamente. En estos centros se implantarían los medios y equipamientos tecnológicos para que el votante emita su voto en un entorno controlado.
Según su documentación, las bases del sistema se pueden adecuar sin problemas a un *sistema abierto* (voto por Internet), pero el precio que implica la comodidad de los votantes de poder votar sin necesidad de trasladarse a locales oficiales incurre en un incremento de los riesgos de coacción.

1.3.8.7. Online E-Voting Prototype with PTC Web Services

Este proyecto, realizado por Brett Wilson y continuado por Hakan Evecek para la Universidad **********. El sistema diseñado consiste en un sistema web que comunica los diferentes módulos del mismo a través de servicios webs. El esquema criptográfico utilizado para cumplir con los requisitos básicos del voto electrónico se basa en el uso del criptosistema de Paillier. Este criptosistema, desarrollado en 1999 consiste en un algoritmo probabilístico asimétrico de criptografía de clave pública. Básicamente, permite que un mensaje emitido puede ser cifrado en

******** ME HE QUEDADO POR AQUÍ ******* Las razones por las que eligen este precepto en el diseño del sistema es para poder reducir el problema derivado de la coacción del votante. Tal y como apuntan en su documentación, la justificación a esta decisión de diseño del esquema se debe a que para

1.3.8.8. SELES

1.3.8.9. SEVI

El Sistema Electrónico de Votación por Internet (SEVI) [15] es una propuesta de sistema software de voto electrónico para reemplazar el canal que constituye el correo postal certificado en el proceso electoral de México.

La idea del sistema es que los ciudadanos con derecho a voto que no puedan hacer uso del mismo el día del proceso tengan un canal de votación disponible a través de Internet. Este canal sustituiría al proporcionado por el correo posta, por lo que debe asegurar, como mínimo, los mismos servicios que ya proporcionaba éste en procesos electorales anteriores.

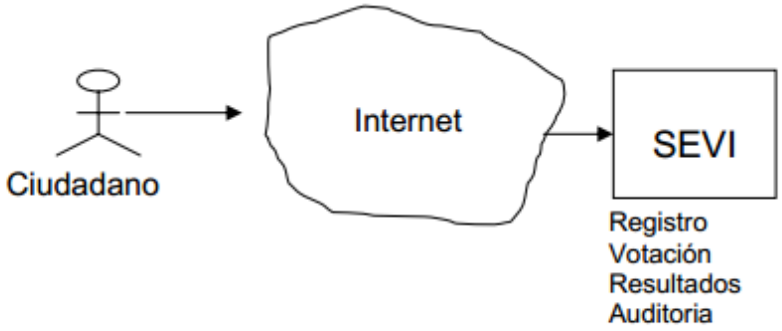

Fig. 4.1 Primera aproximación de funcionalidad de SEVI

Figura 1.4: *Primera aproximación de funcionalidad de SEVI*

El esquema de votación utilizado en SEVI divide el proceso electoral en cuatro fases:

- Registro
- Votación
- Resultados
- Auditoría

Al igual que en SELES 1.3.8.8, el protocolo de seguridad en el que se basa SEVI es una variante del de Lin-Hwang-Chang, el cual se compone de tres fases que cubren la seguridad del esquema en los módulos de votación y generación de resultados. También con este protocolo, el acuse de recibo dado a los votantes sirve para cumplir con los requisitos de auditoría. Otra de las necesidades

resueltas es la de la democracia del proceso, pues el hecho de que se puedan identificar los votantes no honestos al emitir el voto aumenta la confianza en el proceso.

No obstante el protocolo de seguridad respalda la mayor parte de la interacción con el sistema, no cubre la fase de registro. Precisamente esta es la fase con la que comienza el sistema y donde se basa parte de la suposición de honestidad esperada por el protocolo para el resto del proceso. Para resolver el problema, en SEVI optan por establecer un canal seguro entre la máquina cliente y la máquina servidor a través de un protocolo de transferencia segura SSL (Secure Sockets Layer)

1.3.9. Voto por Internet en la EPS

En la Escuela Politécnica Superior de la Universidad San Pablo-CEU ya se realizó una elección por medio de voto electrónico. Sucedió en 2005, cuando en una colaboración entre la Universidad y la multinacional española Indra se celebró la primera elección de delegados de clase a través de voto electrónico con motivo del Día de Internet, celebrado el 25 de octubre del mismo año.

En esta experiencia, más de 600 alumnos de los últimos cursos de la Escuela Politécnica eligieron a sus delegados de clase a través de este sistema.

En la fecha de la elección, cada alumno emitió su voto a través de un nombre de usuario y una clave personal. Por motivos divulgativos, los organizadores de la elección determinaron que una parte del alumnado censado realizara la votación desde un aula de votación concreta, perteneciente al centro y adecuada para ello; mientras que el resto del alumnado debía elegir sus representantes desde algún equipo personal fuera del dominio de la Universidad.

Para que estas elecciones a través de Internet pudiesen llevarse a cabo la Universidad San Pablo-CEU tuvo que adaptar su normativa de régimen interno, pues la que tenía originalmente establecía únicamente la posibilidad de un sistema de voto presencial.

1.3.10. Primitivas de criptografía

Dentro de los retos tecnológicos que propone el voto electrónico, uno de los más importantes es la seguridad. Para poder implementar un sistema seguro que

pueda soportar toda la infraestructura necesaria para poder poner en marcha un sistema de voto electrónico confiable hay que hacer uso de herramientas que sean capaces de asegurar las comunicaciones y el secreto de estas. Es en este escenario donde la criptografía es el núcleo de la solución.
Los requerimientos que se tratan de satisfacer con el uso de la criptografía son [17]:

- Privacidad del voto
- Autenticación del votante
- Integridad de los elementos de la elección

********** PRIMITIVAS CRIPTOGRÁFICAS O ESQUEMAS DE VOTO ELECTRÓNICO ??? ********** ********** EL TEMA ES QUE EXISTEN ESTAS PRIMITIVAS BÁSICAS Y LUEGO LOS ESQUEMAS SE BASAN EN ELLAS PARA SER DISEÑADOS ********** Antes de entrar en los diferentes esquemas de voto electrónico (1.3.11), introducimos una serie de primitivas criptográficas que se utilizan en ellos.
****

Primitivas Operaciones matemáticas, usadas como bloques constructores en la realización de esquemas. Su caracterización depende de los problemas matemáticos que sustentan su uso criptográfico. Ej: DES, RSA.

Esquemas Combinación de primitivas y métodos adicionales para la realización de tareas criptográficas como la firma y el cifrado digital. Ej: DES-CBC-PKCS5Padding; RSA-OAQEP-MGF1-SHA1

Protocolos Secuencias de operaciones, a realizar por dos o más entidades,que contienen esquemas y primiticas con el propósito de dotar a una aplicación de características de seguridad. Ej: TLS con

****

1.3.10.1. Firma ciega

Los protocolos criptográficos de firma ciega se dan lugar entre dos agentes, un usuario U y un firmante F de forma que F firma digitalmente una serie de datos comunicados por U sin conocer el contenido de estos.
El objetivo de este tipo de protocolos es proporcionar una serie de datos firmados

cuyo contenido solamente sea conocido por el actor que envía, siendo completamente desconocidos para el actor que los firma.
Los protocolos de firma ciega se basan en dos componentes [2]:

1.3.10.2. Secreto compartido

Los protocolos criptográficos de secreto compartido dividen un mensaje (secreto) determinado en diferentes fragmentos que se reparten entre los participantes de la comunicación. El reparto de información consiste en los siguientes preceptos:

1. El mensaje (secreto) original únicamente puede ser reconstruido por un cierto grupo de participantes autorizados.

2. Los participantes no autorizados no pueden obtener información sobre el contenido del mensaje original.

1.3.10.3. Pruebas de conocimiento nulo

Los protocolos basados en pruebas de conocimiento cero o nulo son protocolos criptográficos que se basan en la necesidad de una de las partes en poder demostrar a otra que un enunciado es cierto sin revelar nada más que la veracidad del mismo. Uno de los mejores y más sencillos ejemplos para entender el concepto de este tipo de protocolos lo encontramos en una publicación de Pablo Della Paolera, astrónomo de la Universidad Nacional de La Plata (Argentina), en su blog personal [8]. En ella explica que se puede demostrar que se enuncia algo correctamente sin necesidad de demostrar por qué. Basándonos en el ejemplo publicado, supongamos dos actores A y B, en el que B quiere demostrar que A tiene la misma cantidad (o no) de monedas en su bolsillo izquierdo que en el derecho. Para ello, la forma más simple es que B le pida a A las monedas de cada bolsillo y las cuente. Para demostrar la afirmación de que A realmente tiene (o no) las mismas monedas en cada bolsillo basta con que las enseñe. En este caso, el problema es que B está violando la privacidad de A, pues no debería ser necesario que B conozca cuántas monedas tiene A y, mucho menos, tener que enseñarlas a la audiencia para demostrar la veracidad de sus investigaciones. Esta violación de la privacidad se puede superar aplicando de forma simple una solución basada en prueba de conocimiento cero. Supongamos que A tiene X monedas en el bolsillo derecho e Y monedas en el derecho. Para no conocer el número de monedas que posee A, B le pide que piense en un número Z, entero

y mayor que X e Y. A continuación le pide que le diga la diferencia entre Z y X y entre Z e Y. Si ambas diferencias son iguales, A tiene el mismo número de monedas en ambos bolsillos, del mismo modo que si las diferencias no coinciden, se puede afirmar lo contrario, incluso sabiendo en qué bolsillo hay un mayor número de monedas. Y todo esto sin que B llegue a conocer en ningún momento cuántas monedas posee A. Matemáticamente, se trataría de un sistema de 2 ecuaciones con 3 incógnitas, por lo que no se puede resolver y no se pueden obtener los valores de X e Y:

$$Z - X = C$$

$$Z - Y = D$$

Pese a que no es resoluble, sabiendo los valores de C y D se puede demostrar en qué bosillo tiene más monedas ($C > D$ ó $D > C$) o si se tienen las mismas ($C = D$), sin necesidad de conocer los valores reales.

La importancia de este esquema criptográfico es tal que se ha implementado de forma satisfactoria en campos tan esenciales como la verificación de armas nucleares, permitiendo a los observadores internacionales medir la veracidad de una nación al cuantificar su fuerza nuclear sin necesidad de conocer la tecnología o cabezas u otros detalles clasificados que no quieren que sean sacados a la luz.

1.3.10.4. Mixnets

1.3.10.5. Cifrado homomórfico

1.3.11. Esquemas de Voto Electrónico

Los sistemas de voto electrónico están formados por un diseño conceptual y el llamado esquema o paradigma de voto electrónico (E-Voting Schemes - EVS). El esquema es el núcleo del sistema, lo que asegura que los requisitos se cumplan.

La práctica totalidad de estos esquemas usan mecanismos y principios criptográficos.

Los esquemas de voto electronico se basan en una primitiva criptográfica o en un conjunto de ellas. Por eso, hay una serie de esquemas publicados apoyados sobre alguna de las primitivas introducidas en el apartado anterior. Podemos clasificar varios tipos de esquemas de voto electrónico entre los más usados según las publicaciones de una serie de expertos en el campo del voto electrónico criptográfico:

- Esquema de Voto Electrónico basado en Cifrado Homomórfico El votante emite su voto codificado y el recuento se realiza sin descodificar los votos. De esta forma se consigue que no se vulnere el secreto del voto. Para poder realizar esta descodificación, el elector debe instalar algún software desarrollado por la autoridad electoral para realizar las operaciones criptográficas.

- Esquema de Voto Electrónico basado en Canales Anónimos Se trata de un esquema bastante seguro, aunque complejo al mismo tiempo. Se trata el anonimato del votante ocultando el origen de los votos que recibe el sistema.

- Esquema de Voto Electrónico basado en Mixnets El esquema basado en mixnets (redes mixtas) define la existencia de una serie de servidores enlazados. Cada uno de estos servidores recibe un grupo de mensajes encriptados, los reordena, los vuelve a encriptar de forma aleatoria y los envía al siguiente servidor. Con este proceso se consigue que no sea posible asociar la información de los mensajes de entrada con los de salida, rompiendo la relación votante-voto del sistema.
  La desencriptación de los votos se puede realizar tanto en cada servidor (por medio de su propia clave) como al finalizar el proceso utilizando una clave distribuida entre varios de los servidores.
  ********** LITERAL ******** La principal crítica a este esquema es que las pruebas de correctitud son voluminosas. Existen algunas implementaciones comerciales de sistemas de elección electrónica basadas en este esquema.

- Esquema de Voto Electrónico basado en Secreto Compartido En el esquema de voto electrónico basado en secreto compartido, también llamado Paradigma de Benaloh [***** CITA *****], el votante comparte su voto entre varias autoridades electorales. Una vez finalizado el proceso de votación, cada autoridad computa los votos que ha recibido y los pone en común con el resto de autoridades electorales que toman parte en la elección. Así se obtiene el resultado total del proceso.
  ********** LITERAL ********** La implementación de este esquema posee altos costos en términos de comunicación, ya que cada voto debe enviarse por varios canales diferentes (tantos como autoridades electorales haya).

- Esquema de Voto Electrónico basado en Pruebas de Conocimiento Nulo

- Esquema de Voto Electrónico basado en Firma Ciega En un Esquema de Firma Ciega, el firmante no conoce el contenido del mensaje que firma, ya que el emisor del mismo realiza un proceso previo para ocultar su contenido, lo que se conoce por *cegar* el mensaje.
  Se caracteriza porque la entidad firmante no adquiere ningún conocimiento sobre el contenido del mensaje que está firmando, aunque, con posterioridad, la firma obtenida puede ser verificada como válida tanto por esta entidad firmante como cualquier otra entidad que disponga de la información necesaria.
  Se caracteriza porque la entidad firmante no adquiere ningún conocimiento sobre el contenido del mensaje que está firmando, aunque, con posterioridad, la firma obtenida puede ser verificada como válida tanto por esta entidad firmante como cualquier otra entidad que disponga de la información necesaria.
  ********* Explicación del proceso (Chaum??) ********** Los esquemas que se basan en protocolos con firma ciega suelen usar canales anónimos para enviar tanto la firma como el voto cifrado a la autoridad electoral, con lo que protege el anonimato del votante.
  Podemos encontrar este esquema en soluciones como la propuesta en 1992 por Fujioka en [10], la cual sirvió de base a Cranor para la implementación de un prototipo (Sensus).
  El esquema desarrollado en Sensus divide el proceso en cuatro etapas: *inicialización*, *registro*, *votación* y *recuento*. A su vez, registra dos autoridades: *Administrador* y *Contador*. ********* VER BELLEBONI **********

- Esquema de Voto Electrónico basado en papeletas precifradas Este esquema de voto electrónico aparece en la tesis [17]

********** Según [17] ********** Podemos definir cuatro grupos de esquemas de voto electrónico remoto. Estos se diferencian en la forma en la que usan los elementos criptográficos para tratar de resolver los requisitos de seguridad de un sistema electoral:

- Esquemas basados en firma ciega
- Esquemas basados en mixnets
- Esquemas basados en cifrado homomórfico
- Esquemas basados en papeletas precifradas

Junto con estos esquemas básicos en cuanto a solucionar problemas determinados de los procesos electorales electrónicos, nos centramos en resumir algunos de los esquemas desarrollados concretamente para elecciones mediante voto por Internet.
Está fuera del alcance de este proyecto el estudio de estos esquemas y sus evoluciones, pero nos basamos en esta información para el desarrollo del sistema que se implementa. Para ahondar en ellos. recomiendo la lectura del capítulo 4 de la tesis de la Dra. Emilia Pérez Belleboni [22], en la cual se expone una recopilación de información muy concisa sobre multitud de esquemas y sistemas que los implementan, según las necesidades que se necesiten cubrir.

1.3.11.1. Prueba de conocimiento cero

La técnica de Prueba de Conocimiento Cero (Zero Knowledge Proof - ZKP) en criptografía permite a un actor probar un mensaje a otro actor verificador sin revelar el contenido del mismo.

1.4. Organización de la memoria del PFC

En el Capítulo 2 ... En el Capítulo 3 ... En el Capítulo 4 ... En el Capítulo 5 ... En el Capítulo 6 ... En el Capítulo 7 ... En el Capítulo 8 ...

1.5. Metodología

1.5.1. Documentación

Para la redacción del documento del PFC se hizo uso de LaTeX, a través del IDE TexnicCenter.

1.5.2. Metodología de desarrollo

Fases de la ingeniería de software En el desarrollo de proyectos de software existen múltiples de metodologías. Una de ellas basa el desarrollo en 5+2 etapas:

1. Análisis
2. Especificación

3. Diseño
4. Implementación
5. Prueba
6. Documentación
7. Mantenimiento

Aunque para este proyecto, la metodología a emplear se basa en estas fases, por las características el mismo habrá diferencias, sobre todo en cuanto a la distribución de recursos y tiempo entre ellas.
A diferencia de los proyectos de software evolutivos o mantenidos en el tiempo, este proyecto está diseñado para ser puesto en producción durante un relativamente corto espacio de tiempo. Por esto, la fase de Mantenimiento no merece disponer de recursos abundantes, puesto que se limitaría al tiempo en el que el sistema está en producción, lo cual será desde un día a unos pocos, lo que la Autoridad Electoral considere oportuno que estén las urnas abiertas junto con el tiempo empleado para el conteo de resultados y su difusión.
Las fases de análisis y diseño, como en todos los proyectos son realmente importantes, en este caso, además, porque tratan datos muy sensibles, como es la elección de representantes y tienen que lidiar con problemas como el anonimato del votante rompiendo la asociación voto-votante, la autenticidad del votante, verificabilidad del voto, etc.
******** Aquí referencia a los requisitos del voto electrónico **********
La fase de implementación, si el diseño ha sido bien desarrollado debería llevar el tiempo necesario para realizar el software y la integración de los diferentes módulos y sistemas. Sin embargo, la fase de Pruebas cobra una importancia capital en este tipo de proyectas. Al tener una vida tan corta y una importancia en cuanto a datos tan alta, el margen de error del sistema durante el breve período que estará en producción debe ser residual. Este tipo de sistemas deben tener una tolerancia a fallos de prácticamente el 100 %. No hay opción a realizar sistemas evolutivos, por lo que hay que tratar de que no lleguen errores a producción, ya que los que se encuentren durante la jornada electoral se tendrían que arreglar en el momento, con las implicaciones que esto acarrea en cuanto a riesgo de una mala solución y compromiso con los datos o, incluso, con la transparencia del proceso (técnicos modificando código fuente durante la jornada electoral no es una buena práctica de cara a auditorías externas en un sistema electrónico de voto). Por ello, la única forma en la que se

Capítulo 2

Planteamiento

2.1. Objetivos finales del proyecto

El objetivo principal de este Proyecto de Fin de Carrera es la implementación de un sistema de votación electrónica remota (i-voting) diseñada de forma ad-hoc para dos de los procesos electorales que se llevan a cabo en la Escuela Politécnica Superior de la Universidad San Pablo CEU.
Estos procesos están definidos en las *Normas de Organización y Funcionamiento de la Universidad San Pablo-CEU* [20] y son:

- Elecciones de Delegados y Subdelegados
- Elecciones de Miembros de la Junta Electoral

El sistema que se propone en esta memoria es un sistema **robusto**, **fiable**, **verificable** y **auditable**, buscando satisfacer las exigencias de seguridad de procesos electorales más ambiciosos que los que tratamos en este proyecto, los cuales abarcan el ámbito universitario. Por tanto, intención de este PFC, no es la de simplemente realizar estos comicios de forma electrónica, sino tratar de diseñar un sistema con idea de que pudiera ser escalable para niveles superiores al ámbito de la Escuela o la Universidad.
Como se ha avanzado al inicio de esta sección, el sistema propuesto busca tener estas características:

Robusto El sistema debe ser tolerante tanto a fallos como ataques externos e internos.

Fiable El sistema cumple con requisitos de seguridad que satisfacen la privacidad y la precisión de votos y votantes.

Verificable Se puede verificar que los votos han sido contados y forman parte del resultado del escrutinio.

Auditable El sistema debe proporcionar mecanismos para que pueda llevarse una auditoría del mismo antes, durante y después del proceso.

El germen de la idea del proyecto, como se comenta en las Motivaciones del proyecto 1.1 era la búsqueda de soluciones para elecciones generales, autonómicas, municipales, etc. Elecciones que afectan a la población. Junto a la idea de desarrollar soluciones para este tipo de comicios, también está el estudio de las circunstancias por las que todavía no se han implementado sistemas de este tipo en España de carácter general.
Al realizar el estudio del estado del arte actual, se puede recopilar una ingente documentación teórica sobre diferentes sistemas, paradigmas y esquemas de todo tipo de votación electrónica. Hay muchos artículos y tesis muy importantes que tratan de desarrollar sistemas de este tipo, desde el punto de vista teórico hasta el prototipo práctico. Incluso tenemos estados que han implementado una solución con carácter vinculante. En este PFC, lejos de tratar de encontrar una solución novedosa y revolucionaria, vamos a tratar de plasmar un conjunto de ideas y proposiciones de diferentes autores para implementar un sistema propio para la escuela que cumpla con el mayor número de requisitos básicos y deseables para el voto electrónico, teniendo en cuenta además, la variante del factor remoto, es decir, que cumpla, además con los requisitos de control, confiabilidad y seguridad que hagan viable el voto a través de Internet. Así pues, el objetivo general del PFC será:

- Diseñar un esquema y un sistema de voto electrónico remoto a través de Internet que sea robusto, fiable, verificable y auditable**********, además de un coste ajustado,********** para que se puedan llevar a cabo las Elecciones a Delegado y Subdelegado de Curso y las Elecciones a Miembro de la Junta Electoral de la Escuela Politécnica Superior de la Universidad San Pablo CEU.

Teniendo en cuenta el objetivo general, vamos a definir una serie de objetivos intermedios que habrá que cumplir:

OBJETIVO 1 Definir un esquema de voto electrónico que soporte la implementación del sistema en base a los requisitos del mismo.

OBJETIVO 2 Especificar el mecanismo y los protocolos para la identificación de votantes en el sistema y la emisión de los votos sin coacción.

OBJETIVO 3 Especificar los mecanismos y protocolos para una segura recepción de los votos, así como un correcto escrutinio y una veraz publicación de resultados.

OBJETIVO 4 ...

OBJETIVO 5 ...

2.2. Descripción del sistema real

2.2.1. Elecciones a la Junta de Escuela de la EPS

2.2.1.1. Definición de la Junta de Escuela

Según el documento **NORMAS DE ORGANIZACIÓN Y FUNCIONAMIENTO DE LA UNIVERSIDAD SAN PABLO-CEU** [20], en su Artículo 9, *"Las Facultades, Escuelas y Centros integrados o adscritos son las instancias responsables de la organización de la enseñanza e investigación, de acuerdo con las directrices emanadas de los órganos superiores de la Universidad, y de los procesos académicos, administrativos y de gestión conducentes a la obtención de títulos de carácter oficial y validez en todo el territorio nacional, así como de aquellas otras funciones que determinen las presentes Normas de Organización y Funcionamiento y los restantes reglamentos universitarios."*

A partir de esta definición, en el *Capítulo II. De los órganos académicos*, encontramos el Artículo 22, *Tipos de órganos*, donde se establece *"(1c) que las Juntas de Facultad, Escuela o Centro son órganos colegiados"*. Y encontramos su definición en el Artículo 31, *Las Juntas de Centros*, donde podemos leer que *"La Junta de Facultad, Escuela o Centro es el órgano colegiado de gobierno del mismo, que ejerce sus funciones con vinculación a los acuerdos del Patronato, Consejo de Gobierno y resoluciones del Rector."*

También podemos destacar los artículos 32 y 33, donde se establece la composición y funciones de las Juntas de Facultad, Centro o Escuela:

- Artículo 32: Composición de las Juntas

  La Junta de Facultad, Escuela o Centro estará compuesta por miembros natos y electos.

Son miembros natos: El Decano o Director, que presidirá sus reuniones; los Vicedecanos o Subdirectores, el Secretario académico, que levantará acta de sus sesiones y los Directores de los Departamentos integrados en la Facultad o Escuela.

Son miembros electos: Quienes resulten elegidos en representación del profesorado y de los alumnos de acuerdo con la normativa que reglamentariamente se establezca.

- Artículo 33: Funciones de las Juntas Las competencias de la Junta de Facultad, Escuela o Centro son:

  a) Colaborar con el Decano o Director en la gestión de la Facultad, Escuela o Centro.

  b) Promover el perfeccionamiento de los planes de estudio y de la metodología docente, así como el establecimiento de nuevos títulos tanto propios como oficiales.

  c) Participar en la programación de las actividades de extensión universitaria.

  d) Velar por la adecuada dotación de los servicios necesarios para su correcto funcionamiento.

  e) Cualquier otra competencia que le pueda ser atribuida en el desarrollo de estas Normas de Organización y Funcionamiento.

2.2.1.2. Proceso electoral

******** AQUÍ HACE FALTA ENCONTRAR UN TEXTO LEGAL EXPLICANDO EL PROCEDIMIENTO DE LAS ELECCIONES **********

2.2.1.2.1. Plazos

- Convocatoria
- Presentación de candidaturas
- Publicación del censo
- Constitución de la Junta Electoral
- Designación de las mesas electorales

2.2.2. Elecciones de delegados y subdelegados de curso en la EPS

2.3. Alcance del proyecto

Como se indica en el apartado 2.1...

2.4. Fases del proceso electoral

- Fase Preelectoral

  Definición de los límites o reglas de la elección : Deben definirse de forma que no parezca ambigua las reglas electorales. Qué se vota, a quién se vota, de qué forma, cómo se cuentan los votos o se asignan los cargos. Quiénes pueden votar, cuándo comienza y finaliza el sufragio.

  Elaboración del censo : Las autoridades de la Elección deben realizar un proceso de elaboración del censo electoral, para identificar qué votantes tienen derecho a ejercer el voto y dónde (con qué opciones de voto).

  Registro de votantes : Puede ser necesario que, según los mecanismos de identificación a utilizar, el votante deba registrarse previamente a la elección frente a la Autoridad Electoral, con el fin de, si no existe censo electoral formalizado, introducirse en el censo de la elección o, si existe ese censo previo, obtener la acreditación identificativa necesaria para poder votar de forma remota con las garantías avaladas por la autoridad electoral. ********** EN LA TESIS DE VMMR, CAPÍTULO 5, VIENE MUCHA INFORMACIÓN. DE CARA A LA SOLUCIÓN, PODEMOS CITARLE, HABLAR DE QUE LO QUE HAY QUE CONSEGUIR ES IDENTIFICAR A UNA PERSONA DE FORMA INCORRUPTIBLE Y RELACIONARLA CON UN SISTEMA DIGITAL (FIRMA!!!!). HABLA DE LA HUELLA DACTILAR, LA FIRMA MANUSCRITA Y LA VOZ **********

  Presentación de candidaturas : A efectos del sistema informático que desarrollamos es el proceso en el que la autoridad electoral define qué candidaturas pueden ser elegidas por cada votante en cada circunscripción (lógica).

- Fase Electoral (Votación)

  Identificación : El primer paso del proceso de votación es el de la identificación del votante. Como ya se ha planteado, la identificación del votante es uno de los procesos críticos de una elección, pues, el sistema debe cumplir con varios requisitos básicos del voto electrónico, como puede ser el principio de autenticidad (en el que sólo los votantes autorizados pueden votar) o el democrático (por el cual el votante que tiene derecho a votar es sólo para hacerlo una vez).

  Votación : El momento en el que el votante ya identificado, observa las opciones que puede elegir y ejerce su voto a una o varias de ellas (dependiendo del tipo de elección).

- Fase postelectoral

  Difusión de resultados : La difusión de resultados es la fase que tiene la responsabilidad de publicar los resultados de forma oficial u oficiosa. En los sistemas de conteo

- Auditoría No es una fase propiamente dicha en el sentido cronológico en el que se han definido las anteriores. La fase de auditoría abarca todas las etapas del proceso, en mayor o menor medida, puesto que debe permitir la vigilancia del correcto funcionamiento del mismo en todas ellas.

2.4.1. Fase preelectoral

2.4.1.1. Definición de los límites o reglas de la elección

Para ejercer la democracia de forma correcta las ”reglas del juego” deben estar bien definidas, de forma clara y concisa, estableciendo los límites, los mecanismos, las fechas y todo lo necesario para una correcta interpretación, sin lugar a ambigüedades. (...)

Estas reglas de la elección son responsabilidad de la Autoridad Electoral encargada de la organización de los comicios, así como del organismo que los convoca. De cara al sistema informático, esta fase preelectoral es la que sienta las bases de la lógica de negocio del sistema. Ya que define las reglas que el sistema deberá cumplir para llevar a cabo correctamente la elección. (...)

2.4.1.2. Elaboración del censo

Uno de los cometidos de la Autoridad Electoral previamente a la celebración de unos comicios es la elaboración de un censo electoral completo y fiable que les permita tener un control de cuánta gente y quiénes disfrutan del derecho a votar. Además, este censo debe recoger a qué circunscripción pertenece cada votante y la mesa/urna donde debe realizar su voto.

Una circunscripción es una división electoral. Pensando en elecciones legislativas de España, por ejemplo, casi todas las provincias son unicircunscripcionales, excepto el Principado de Asturias, que se conforma con 3 circunscripciones y la Región de Murcia, compuesta por 5 circunscripciones. Sin embargo, para las Elecciones al Parlamento Europeo, España registra sus votos como una única circunscripción.

Al asignar cargos basándose en circunscripciones, es básico que en el censo esté definido en cuál de ellas vota cada votante. Además, en cada circunscripción, los candidatos varían, por lo que las papeletas entre las que cada votante puede elegir no serán iguales de unas circunscripciones a otras.

Extrapolando a las Elecciones a la Junta de Escuela de la EPS, podemos identificar varias de estas circunscripciones, a saber:

- Alumnos, por titulación: Arquitectura, Ingeniería Informática, Ingeniería de Telecomunicaciones e Ingeniería de la Edificación
- Profesores, por categoría: colaboradores, adjuntos, agregados y catedráticos.

Podemos asumir, entonces que hay 8 circunscripciones. Por las normas de estas elecciones, para cada circunscripción se eligen 2 representantes que serán los que acaben formando la Junta de Escuela, con 16 cargos electos.
********** **CREO QUE ESTÁ MAL. REALMENTE, LOS ALUMNOS SON UNA ÚNICA CIRCUNSCRIPCIÓN: SU CENSO LO FORMAN LOS DELEGADOS Y SUBSELEGADOS DE CADA UNO DE LOS GRUPOS, QUE COMPONEN TAMBIÉN LOS CANDIDATOS. CANDIDATOS = CENSO EN ESTA ”CIRCUNSCRIPCIÓN”**

La Universidad deberá elaborar un censo con los alumnos y profesores que tienen derecho a votar en las Elecciones, así como definir en qué circunscripción lo harán, para que tengan conocimiento de entre qué candidatos pueden elegir a sus representantes. De cara al sistema, es importante conocer estas divisiones, tanto para el conteo de los votos, como para la gestión de los candidatos en el momento en el que se presentan al votante.

Por tanto, es necesario tener un sistema que cargue el censo electoral elaborado por la Universidad, así como la definición de las circunscripciones y la relación entre estas y el propio censo de votantes.

2.4.1.3. Registro de votantes

En muchos procesos electorales no existe un censo oficial elaborado por la Autoridad Electoral o alguna otra institución relacionada (como puede ser el INE en España). En ese caso, en multitud de estados se procede a una fase de registro en la cual se permite (en algunos casos, se obliga) a los ciudadanos a que se registren en un listado de votantes. Es el paso previo para poder votar. Una vez finalizada esta fase de registro, la Autoridad Electoral posee un censo *oficial* de votantes.

En el caso de las Elecciones dentro de la Escuela Politécnica, el censo lo proveerá la propia Autoridad Electoral a través de los datos de profesores, alumnos y empleados del Centro. Al realizar la carga de estos datos para conformar el censo electrónico, el sistema tendrá conocimiento de qué potenciales votantes tendrán permiso o no para votar y qué opciones de voto deberá presentarles para que conformen su boleta electrónica.

Dependiendo del mecanismo digital de identificación y votación que se adopte para el sistema, la fase de registro puede ser tan simple como la correcta carga del censo en el sistema o puede aumentar ligeramente su complejidad. Si se decide utilizar una identificación basada en base de datos, habría que asignar a cada votante un nombre de usuario y una contraseña, al menos para ingresar en el sistema, ya que podría generarse otro par para la votación. En cualquier caso, en una situación como esta, además de la carga del censo resulta necesario una asociación de cada votante incluido en este con los nombres de usuarios y contraseñas generados para cada uno.

La Universidad proporciona a cada alumno, profesor y empleado un carnet universitario para su identificación. Entre otros servicios, estos carnets poseen la funcionalidad de identidad y firma digitales. Puede una buena opción hacer uso de estos servicios y evitar la asociación anterior, la cual, además del paso extra, no proporciona un nivel de seguridad aceptable. El servicio de esta tarjeta (TUI) o del DNIe español permite una identificación digital unívoca y confiable entre el votante y el sistema. Haciendo uso del servicio de firma digital, también se varía el esquema de votación del sistema, pues no requeriría de un módulo de generación de firmas electrónicas para votantes, pues cada uno llevaría el suyo propio en su TUI personal.

2.4.1.4. Presentación de las candidaturas

Una vez definido tanto el censo como las divisiones electorales, tienen que presentarse las candidaturas. (...)

2.4.2. Generación de claves de encriptado

Es necesario que en esta fase se generen las claves que se utilizarán tanto para encriptar el voto que deposita el votante en la urna digital como las necesarias para que los miembros de mesa puedan descifrarlo para poder realizar el escrutinio.

2.4.3. Fase electoral

2.4.3.1. Identificación del votante

El primer paso de un votante a la hora de emitir su voto, en el sistema de voto tradicional es identificarse ante los miembros de la mesa electoral. Para ello, en elecciones como las que organizan el Ministerio de Interior en España o las diferentes Comunidades Autónomas, el votante hace uso de un documento que verifique su identidad. En España, este documento es el DNI, aunque también se puede hacer uso del Pasaporte. En otros países en los que se carece de un documento oficial de identidad expedido por las autoridades del Estado, se realiza un registro biométrico de los votantes con, por ejemplo, las huellas dactilares de los mismos.
En el caso de las Elecciones a la Junta de Escuela de la EPS CEU, la identificación de los votantes...

Una vez identificado al votante, se le tiene que cotejar con el censo de la elección o de la mesa en la que ha sido identificado. En países como España, la elaboración del censo corre a cargo del INE (Instituto Nacional de Estadística) y reparte a los votantes en diferentes mesas repartidas en locales electorales. En otros estados, este censo no existe y se requiere que sea la ciudadanía la que se registre en un Registro de Votantes, con lo que si no se ha acudido a tiempo de realizar este trámite, la persona pierde su derecho al voto.
En el caso de estudio de las elecciones de la EPS, este censo debe ser proporcionado por la propia Escuela. Los datos son suyos y la cesión debe ser temporal y, simplemente, para ser cotejado, nunca para publicación de ningún tipo de resultado o listado con la información proporcionada.

********* LOPD ?? ? ? ? **********

Para dejar constancia de que un votante ya ha ejercido su derecho al voto, en países como España es tan simple como que los miembros de la mesa electoral lo reflejen en una lista con el censo de su mesa. En otros territorios, sin embargo, la costumbre es marcar de alguna forma a aquellas personas que han votado, como puede ser manchar algún dedo de la mano con tinta indeleble, para que, si volviese a intentar votar en otra mesa, se pueda comprobar que ya lo había hecho previamente.

En un sistema de voto por Internet no hay una interacción directa entre el votante y la autoridad electoral, que es quien debe permitirle votar. Por ello, es muy importante que los mecanismos para identificar al votante sean precisos y confiables. Por ello, hay que valorar qué método de identificación es el mejor para cumplir con los requisitos de la elección, incluidos ahí los inherentes al voto electrónico telemático y remoto.

- Usuario / contraseña.

  Para las elecciones de la Junta de Escuela de la EPS, el método de usar un par usuario / contraseña sería una solución sencilla. El censo está bastante acotado y, al ser todos los potenciales votantes miembros de la Universidad, poseen una cuenta de correo electrónico corporativa proporcionada por ésta. El proceso sería tan fácil como, por ejemplo, usar la dirección de correo electrónico de cada alumno / profesor / trabajador de la Escuela como nombre de usuario y enviarles un email a cada uno con una clave aleatoria generada por la autoridad electoral.
  Esta solución, no obstante, sería inviable para elecciones más ambiciosas, como lo son las legislativas estatales o autonómicas, ya que carecemos de elementos como direcciones de correo electrónico de todo el censo. Se podría utilizar el correo ordinario como método para hacer llegar estas credenciales, de la misma forma en que los partidos políticos hacen llegar la propaganda electoral o la Junta Electoral hace llegar la información del censo electoral a cada votante. Considero que sería un gasto extra de recursos económicos, humanos y medioambientales que no se sostiene para la utilización de este servicio. Tampoco se asegura la recepción del correo si aprovechamos el envío de la información del censo electoral, pues el envío, al contrario que cuando hemos solicitado el voto por correo y nos hacen llegar las papeletas, no es certificado. Realizar este envío de credenciales con garantía de recibo, resultaría muy costoso y lenta.
  Otro motivo que desaconseja el envío de credenciales por correo es éstas podrían ser interceptadas por otra persona distinta a quien identifican de

forma no muy complicada, lo cual supone una brecha de seguridad bastante importante.

- DNIe

  Lo ideal para una elección por el sistema de voto por Internet es implementar un proceso que resulte sencillo al votante, ya que si resulta ser más complicado que el voto tradicional, el votante no le verá sentido y no hará uso de él. Con este planteamiento, parece que el uso del DNIe es una buena idea. Por un lado, es un documento oficial que llevamos normalmente con nosotros en todo momento. Además es el mismo documento que nos identifica en las elecciones tradicionales, con lo que para el votante no debería suponer ninguna suspicacia ni trauma, al estar completamente insertado en la sociedad su uso para este cometido (asumimos en este supuesto que la implantación del DNIe en España es casi completo, que el votante ya no necesita acudir a una comisaría a solicitarlo y que los certificados no están caducados).
  Ventajas del uso del DNIe como identificador del votante:

  - Documento expedido por las propias Autoridades del Estado, quienes lo avalan.
  - Seguridad.
  - La gente lo lleva consigo constantemente y está acostumbrada a usarlo para identificarse o, incluso, para realizar otro tipo de actividades en Internet, como obtener certificados de Organismos Públicos, banca por Internet, etc.
  - Es el mismo documento que ya se utiliza para identificarse en las elecciones presenciales tradicionales.

  Inconvenientes del DNIe:

  - Extranjeros con derecho a voto pueden no tener DNIe, pero deberían poder votar con el pasaporte.
  - Certificados caducados. Que los certificados que lleva consigo el DNIe no tengan la misma fecha de caducidad que el propio documento es un punto en contra, ya que los usuarios no lo renuevan al ver que no tienen que hacerlo con el documento físico.
  - Rotura del chip que contiene los certificados.

- Limitaciones técnicas para las aplicaciones web. En el estado actual de la tecnología, es necesario hacer uso de un applet de Java para poder firmar con el DNIe. De cara a la identificación, ya hay software Javascript que se salta este paso, aunque no a la hora de firmar, para lo cual, hoy por hoy, no hay alternativa. Este detalle es una limitación importante, quizá no para el oto electrónico, pero sí para el voto universal por Internet, ya que requiere de más tecnología que simplemente un dispositivo conectado a Internet y un lector. Además, el uso de applets está cada vez peor visto en Internet y se recomienda no implementar alternativas basadas en el estándar W3C. Por desgracia, este organismo todavía no tiene definido de una manera versátil cómo afrontar el problema de la criptografía en los nuevos estándares web.
- Necesidad de HW externo, como son los lectores de Smartcard. Para poder utilizar el DNIe como identificador, el sistema tiene que poder leer los datos que le indica. Si hacemos uso de los certificados que contiene, necesitamos un lector externo, lo cual quizás no sea un problema si usamos un PC que tenemos en casa, pero sí que puede serlo cuando queremos votar desde otro ordenador o incluso desde un dispositivo móvil, donde ya no es tan simple que tengamos este lector y que sea compatible. Cierto es que podríamos hacer uso de la banda MRZ del documento escaneándola pero... (******** no estoy seguro, qué pasa con fotocopias??, yo me fiaría de los certificados).

- MobID

  El Gobierno de Estonia, para sus comicios por Internet está desarrollando una tecnología en la que el propio smartphone es la herramienta que sirve para identificarnos. Parece una buena opción, pues hoy por hoy, es bastante común que llevemos el smartphone con nosotros de la misma forma que llevamos el DNI. Además, es un dispositivo muy personal, que no se suele compartir, por lo que podría realizarse una identificación unívoca entre el usuario-votante y su registro en el censo electoral. (******** hay que mirar bien esto, pues no sé si habrá algo desarrollado, de todos modos, en España esto ni se contempla)

- Smartcard

  Otra opción posible es el uso de una smartcard que contenga certificados emitidos por la Autoridad Electoral para cada votante. Los inconvenientes de este método son varios: - Por un lado, requiere un registro previo de los

votantes, pues hay que generarles los certificados. - Un problema logístico ya que, una vez generados los certificados e introducidos en las tarjetas, éstas deben hacerse llegar a los votantes que las van a utilizar. Este paso, en unas elecciones a gran escala puede suponer un esfuerzo injustificado.

En el caso de las Elecciones a la Junta de Escuela de la EPS, podemos pensar en la primera opción. No obstante, como se explica en próximos capítulos, el hecho de necesitar certificados de firma para cifrar y firmar el voto por seguridad, nos hace que tengamos que plantearnos una solución para este problema. Con una simple identificación de usuario / contraseña no lo vamos a poder resolver, así que se tiene que buscar una alternativa. Sería inteligente tratar de buscar una alternativa que sirva tanto para el paso de votación como para el de identificación, por seguridad, así que podríamos pensar en DNIe. Pero en la Universidad podemos tener miembros del censo que no posean este documento (estropeado, caducado, extranjeros). La forma que tiene la Universidad de acreditar que un alumno forma parte de ella es con un carnet universitario que se entrega tanto a alumnos como a profesionales. Podría ser este documento, el oficial en la Escuela, el que se use como identificador de votante, con lo que estamos hablando de utilizar una smartcard especial, emitida por la propia Autoridad Electoral de forma previa. (********** Lo que pasa es que me temo que estas tarjetas no tienen certificados, con lo que tampoco van a valer para la votación).

2.4.3.2. Votación

En el sistema tradicional, el momento de la votación es aquel en el que el votante deposita su voto en la urna tras haber escogido la papeleta o marcado la boleta de candidatos y haber sido identificado correctamente por los miembros de la mesa electoral.
Este proceso es al que estamos habituados en los territorios con una cierta historia democrática. En principio, parece bastante transparente, en cuanto a que el votante puede confirmar sin ninguna duda que su voto, efectivamente, se encuentra dentro de la urna sellada, junto con el resto de votos de la mesa.
Aquí encontramos el primer detalle controvertido con respecto al voto por Internet. El votante no tiene constancia física de que su voto se ha depositado en la urna correcta, ni siquiera de si está en alguna urna. No ”se ve”.
Es más, sabe que ha introducido en la urna la papeleta que tenía en su mano, que sabe cuál es porque él mismo la ha elegido. Pero en el sistema informático, no sabe si ocurre lo mismo. Puede pensar que aunque haya seleccionado un

candidato y el sistema le diga que ha contabilizado su voto por éste, realmente, por detrás esté cambiando el voto y registrando a otro candidato diferente.
Es misión del sistema informático proveer al votante de mecanismos que le permitan verificar todas estas cuestiones. Hay que diseñar el sistema para que haya confianza en él. Quizá esta sea la mayor de las barreras existentes en la actualidad para la implantación del voto por Internet, la falta de confianza.
No es por falta de métodos seguros o carencia de medios criptográficos. El problema es que no es fácil que el elector, opinión pública u organismos de control o auditoría confíen en el proceso, ya que, a priori, parece una gran caja negra, ante la cual es complicado asegurar una verificación de datos de forma transparente.

2.4.4. Fase postelectoral

2.5. Logs

********** Esto no va aquí, pero lo pongo para acordarme. Ya veremos si va en planteamiento, en solución o en... **********
********** Probablemente tenga que ir en un capítulo dedicado a la AUDITORÍA, ahora que lo pienso **********
Con la trascendencia que tiene un sistema de votación electrónico, es básico procurar de sistemas precisos y confiables para una auditoría interna o externa. Se trata de desarrollar herramientas y procedimientos que permitan corroborar el perfecto funcionamiento del sistema sin interferir en el mismo ni violar los principios de privacidad del voto secreto.

Una de las herramientas que se usan para este caso, son los logs del sistema.

Con los logs, se va escribiendo uno o varios ficheros con trazas que indican los pasos que se han llevado a cabo en cada momento o elementos que han afectado al sistema de una u otra forma.

En el caso de este sistema, es muy importante tener registrada la mayor parte de las acciones que ocurren en el mismo. Desde los accesos a web, intentos de autenticación, votaciones, hasta las acciones de los administradores del comicio, los miembros de la Junta Electoral encargados de proporcionar las claves para descifrar o los propios auditores.
No obstante, un exhaustivo registro de información acerca del proceso podría su-

poner un peligro para el secreto de voto. Esto puede ocurrir porque cuanto más información se registre, si no se hace con cuidado, mayor probabilidad de incurrir en un problema de trazabilidad del voto.

Pongamos un ejemplo, sencillo y burdo, de trazabilidad del voto por medio de registros de log independientes: Diseñamos el sistema con servidores de autenticación y votación independientes.

1. El servidor web guarda los accesos al sistema a través del portal web, con IP incluida.
2. El sistema de autenticación, registra el momento en que un votante se autentica, guardando la identidad del mismo.
3. El sistema registra qué votante y en qué momento introduce su voto en la urna digital, anotando el identificador del voto.
4. Otro log de registro es el que relaciona el identificador del voto cifrado con el contenido del mismo una vez descifrado.

En este ejemplo podemos observar claros fallos de diseño que comprometen la privacidad del votante, como el de guardar la relación entre un voto descifrado y el identificador del voto cifrado (pero para desarrollo o una prueba de caja blanca no es descabellado este tipo de registros).

Se observa que si un atacante tuviese acceso a los logs del sistema, podría, sin mucha dificultad llegar a relacionar al votante con el contenido de su voto, con lo que se pierde el anonimato del proceso. Todo ello incluso usando diferentes servidores y diferentes elementos de registro de log.

El argumento es que, al igual que en prácticamente cualquier sistema, es muy importante tener un servicio de logs que nos informen del funcionamiento del sistema, ya que así se puede estudiar en producción o a posteriori cómo se ha comportado el mismo y poder actuar ante ataques al mismo o responder con datos ante fallos en el mismo. Pero en un sistema de voto electrónico, además de la importancia que ya como sistema electrónico tienen, es muy importante centrarse en su diseño, ya que no es simplemente un servicio en el que añadimos trazas, sino que tenemos que asegurar que estas trazas no van a interferir en la seguridad del sistema, comprometiendo, como hemos visto en el ejemplo, el principio de anonimato en el voto que se le exige al sistema.

Capítulo 3

Riesgos

3.1. Identificación y gestión de riesgos

(Uno de los riesgos que hay que tener en cuenta en este tipo de elecciones es la fecha límite. Tiene que funcionar durante un cierto período de tiempo, sin fallo y sin posibilidad de modificación -relativamente-)

3.1.1. Identificación de riesgos

Miembros de una conocida empresa española líder en procesos de voto electrónico publicaron un artículo de buenas prácticas al implementar un sistema de voto electrónico por Internet. En el mismo exponen una lista de riesgos generales de seguridad inherentes al voto electrónico. Su intención era usarlos como referencia para poder comparar diferentes sistemas de voto sin tener en cuenta la tecnología que los implementen.
En este PFC van a tenerse en cuenta de cara al diseño de un sistema robusto de voto por Internet.

Votos por parte de votantes sin autorización : El sistema de voto debe poseer un mecanismo robusto y confiable para identificar correctamente de forma remota a los votantes, ya que personas sin autorización podrían intentar emitir su voto.

Suplantación del voto : Un votante o un atacante podrían intentar suplantar la identidad de un votante autorizado para votar en su lugar. El sistema debe proporcionar un mecanismo que detecte este tipo de intentos de suplantación.

Inyección de votos : El sistema debe prevenir la aceptación de votos *inyectados*. Un atacante puede intentar introducir en la urna votos de votantes que no han participado en el proceso electoral (por ejemplo, por abstención) y que, por tanto, no deberían contabilizarse.

Privacidad del voto comprometida : Un atacante podría intentar quebrar la privacidad del voto de un votante, identificando al mismo con su opción elegida, con lo que se pierde el requisito del derecho al voto secreto. El sistema debe implementar mecanismos que eviten completamente que, durante cualquier fase del proceso, la intención de voto de cualquier votante pueda dejar de ser secreta.

Coacción y compra de votos : Una persona u organización puede comprar a un votante u obligarle a votar por una candidatura específica. El sistema de voto debe evitar que un votante pueda probar a un tercero su intención de voto de forma irrefutable.

Modificación del voto : Los votos emitidos pueden ser modificados para cambiar el resultado de la elección. El sistema debe detectar cualquier manipulación en los votos válidos ya emitidos.

Borrado de votos : Relacionado con el anterior, un atacante podría intentar borrar votos que ya han sido emitidos. La urna debe estar protegida ante cambios no autorizados, como puede ser un intento de borrado.

Publicación de resultados intermedios no autorizados : Los resultados intermedios podrían ser divulgados antes del cierre de la elección, con lo que se puede influir en los votantes que todavía no hayan emitido su voto. El sistema debe preservar el secreto de los votos sufragados hasta el proceso de escrutinio y evitar la difusión de resultados parciales antes de la finalización del periodo de votación.

Desconfianza del votante : Un votante puede no tener ningún medio para verificar la correcta recepción y cuenta de su voto por parte del sistema. Debido a esto, el votante podría desconfiar del proceso. El sistema debe permitir al votante verificar si su voto ha sido correctamente recibido por el sistema y si ha sido incluido en el proceso de escrutinio con la opción con la que fue emitido.

Ataque DoS : Un atacante podría interrumpir la disponibilidad del canal de votación realizando un ataque DoS (*Denial o Service - Denegación de Servicio*).

El sistema debe detectar una eventual congestión de los servicios de votación para poder reaccionar tan pronto como sea posible y evitar una caída de los mismos que no permita a los electores sufragar su voto.

dddd : Una insuficiente trazabilidad de los eventos de la elección o una manifiesta facilidad para modificar los datos auditables puede permitir a un atacante esconder cualquier comportamiento no autorizado en el sistema. El sistema debe proporcionar medios para implementar un proceso de auditoría que permita detectar cualquier manipulación de estos datos.

Capítulo 4

Análisis del sistema

Una vez ha sido presentado el proyecto, planteados los objetivos y estudiado el estado de la cuestión, la siguiente fase en el desarrollo es el Análisis. En esta etapa se analiza el problema con el cliente, llegando a un acuerdo en el alcance del proyecto y los requisitos que deben ser satisfechos.

4.1. Especificación de requisitos

4.1.1. Introducción

En esta sección de la memoria vamos a desarrollar la especificación de requisitos de software. Con esta técnica lo que se consigue es una descripción completa del sistema que se va a desarrollar.

Los requisitos se organizan en tres tipos diferentes:

Funcionales : Son los requisitos que el sistema debe cumplir para su correcto funcionamiento. Son requisitos fundamentales de cara al usuario, ya que responden a la pregunta *¿qué hace?*, por lo que implican directamente en la funcionalidad que el sistema proporciona al usuario.

No funcionales : Usualmente son los requisitos que responden a la pregunta *¿cómo lo hace?*. Definen las necesidades de recursos para el funcionamiento del sistema, como protocolos, infraestructura, tecnología...

Organizacionales : ********** NOTA: yo esto lo considero de otra forma ..., según wikipedia: son el marco contextual en el cual se implantará el sistema para conseguir un objetivo macro **********

4.1.2. Ámbito del sistema

El sistema que se va a desarrollar tiene como finalidad que los alumnos, profesores y empleados de la Escuela Politécnica Superior de la Universidad San Pablo CEU puedan votar remotamente en las Elecciones a la Junta de Escuela. Para ello, el sistema debe ser distribuido y dirigido hacia un entorno web, permitiendo que los votantes puedan emitir su voto desde cualquier lugar donde tengan conexión a Internet. Con el auge de los teléfonos móviles inteligentes y de las redes móviles (GPRS, 3G, 4G, HSDP...), se puede permitir la votación desde cualquier lugar en la que el proveedor de telefonía móvil provea de cobertura al votante. Este enfoque ubicuo del voto debe asegurar, no obstante, las mismas garantías que proporciona un sistema de voto tradicional o uno de voto electrónico presencial. El sistema dispone, por un lado, del servidor web que permite la interacción tanto con el votante como la difusión de los resultados electorales. Este servidor web tendrá comunicación con Internet y debe tener una seguridad acorde con el nivel de peligro ante ataques que se espere para este tipo de elección. Por otro lado, la parte de la lógica de negocio del sistema se basa en subsistemas independientes, aunque modulares, dependiendo del servicio que tengan que ofrecer. La independencia de estos subsistemas responde a cuestiones de seguridad y para proporcionar mayor transparencia del proceso en cuanto al *flujo del voto* a través del software.

Título: AQUÍ VA EL TÍTULO **********

Descripción: El sistema consiste en una plataforma de voto electrónico remoto por Internet, seguro, anónimo y tratando de implementar el máximo de requisitos exigibles al voto electrónico que cumplan con el objetivo. El desarrollo es ad-hoc según las normas de las elecciones que van a tomar parte. (**********)Pese a ser un diseño dirigido a unos tipos de elecciones concretas, se puede modularizar el sistema para que, implementando unas nuevas reglas, el sistema sirva de base a otros procesos.(**********). Los votantes dispondrán de unas credenciales digitales que servirán para que se puedan identificar unívocamente en el sistema, sin suplantaciones. (********** DNIe? TUI? user/password? **********). Estas credenciales se implementan basándose en certificados digitales que aseguran la autenticidad del votante. Una vez el votante se autentica contra el sistema y el censo (proporcionado por la Universidad y cargado previamente en el sistema), se le presenta el surtido de papeletas entre las que puede elegir a sus representantes. Este conjunto de papeletas ha de ser calculado por el sis-

tema teniendo en cuenta el tipo de votante con el que interacciona (estudiante/profesor/empleado, carrera, grupo/clase...).Una vez seleccionada la papeleta, emite el voto. El voto consiste en que el votante firma digitalmente un sobre lógico en el que va la papeleta cifrada. Este sobre se envía al sistema, donde un módulo urna digital se encarga de almacenarlo hasta la finalización del periodo de votación. Una vez llega el fin de este periodo, los administradores de la elección abren la urna. Para ello, requieren de una clave criptográfica que estará troceada y repartida entre varios miembros. La apertura de la urna implica la anonimización de los votos, rompiendo la relación entre un votante y el voto que ha emitido. Una vez cumplido con el requisito del voto anónimo y eliminada la trazabilidad del voto, estos tienen que ser descifrados para, a continuación, ser contados. Al finalizar el escrutinio, se publican los resultados. Junto a la publicación de los resultados, se deben publicar unas listas para que los votantes puedan verificar que el voto digital que emitieron no ha sido alterado y, además, ha formado parte del escrutinio.

El sistema consiste en una plataforma de voto electrónico remoto por Internet, seguro, anónimo y tratando de implementar el máximo de requisitos exigibles al voto electrónico que cumplan con el objetivo. El desarrollo es ad-hoc según las normas de las elecciones que van a tomar parte. La identificación de los votantes en el sistema ha de ser unívoca, evitando que un votante pueda ver su identidad suplantada por otro. Los usuarios que intenten acceder al sistema de voto y no pertenezcan al censo oficial, proporcionado por la Autoridad Electoral de la Universidad, han de ser identificados y su acceso al mismo rechazado, pues hay que cumplir el requisito de Autenticidad del voto/votante. El sistema debe proporcionar al votante las distintas opciones entre las que puede elegir para ejercer su voto teniendo en cuenta el tipo de votante registrado y las reglas de le elección que le aplican. Una vez seleccionado el voto que quiere ingresar en la urna electrónica, el sistema debe asegurar que éste es correcto, para avisar al votante que lo corrija en caso contrario y no emitir un voto incoherente en el sistema. En el caso de un voto coherente (votos válidos y votos nulos), el sistema debe, en primer lugar destruir la relación entre el voto y el votante, cumpliendo con el requisito de privacidad del voto o anonimato del votante, el voto es secreto, por lo que hay que asegurar que no existe una trazabilidad que pudiese llegar a relacionar un voto con la identidad del votante que lo sufragó. El sistema debe proporcionar un mecanismo por el cual un votante tenga la capacidad de confirmar que su voto ha sido correctamente incluido en la urna electrónica. Debe poder asegurarse

de que *ha votado*. Del mismo modo, el sistema ha de asegurar que los votos, ya desligados de la identidad del votante, son correctamente almacenados en la urna electrónica y correctamente contados en la fase de recuento o consolidación de votos. Teniendo en cuenta las reglas de la elección, debe asegurar que todos los votos son correctamente contados y que sólo lo son una vez. Una vez finalizado el recuento, y difundidos los resultados, el sistema debe proporcionar un mecanismo para que un votante pueda confirmar que su voto ha sido incluido correctamente en los resultados ofrecidos por el sistema sin que se viole la privacidad de su voto.

Adicionalmente, el sistema debe proporcionar funcionalidades externas al proceso de voto. Debe tener un sistema de carga y gestión de los datos electorales (reglas de la elección, urnas, circunscripciones, candidatos, censo). Debe proporcionar herramientas que permitan la monitorización del proceso para comprobar el estado del mismo, además de herramientas de transparencia para que pueda ser auditado en tiempo real por las autoridades competentes.

4.1.3. Restricciones generales

1. Primera restricción **********
2. Segunda restricción **********

4.1.4. Requisitos funcionales

Votación por Internet : El sistema de votación debe funcionar de forma remota en sus fases de registro, identificación, votación y consulta de resultados. Cualquier votante puede acceder a las funcionalidades del sistema a las que tiene autorización desde cualquier punto conectado a Internet.

Permitir votación presencial : El sistema debe proporcionar los mecanismos necesarios para permitir el voto a aquellos votantes con derecho al mismo que quieran emitirlo de forma presencial en el periodo habilitado para ello. ******* NOTA: (Analizando este requisito, la mejor forma es habilitando un horario en la sala de ordenadores de la Escuela destinados a que las personas que quieran puedan votar de forma remota desde estos puestos) *********

Disponibilidad total : El sistema debe estar disponible para proporcionar servicio de voto durante todo el periodo estipulado en las normas que se fijen

para la elección. ******* NOTA: (24/7, un día, varios días... depende de cómo se defina el proceso) *********

Identificación remota : El sistema debe implementar un mecanismo que sea capaz de asegurar la identificación de un votante en el sistema de forma remota, digitalmente, sin posibilidad de error ********** NOTA: Esto de sin posibilidad de error ni me gusta ni queda correcto **********.

Autenticación remota : El sistema debe poder autenticar a los votantes que tratan de usar su identificación digital para ingresar en el sistema de forma remota. El sistema no debe errar en esta autenticación, permitiendo la entrada de los votantes autorizados y revocando el acceso a los atacantes, suplantadores o desautorizados.

Papeleta/boleta digital : El sistema debe mostrar al votante la papeleta o boleta (dependiendo del tipo de elección) correspondiente a la elección y el censo que le corresponda. Debe contener las opciones correctas por las que puede optar y mantener correctamente la/s opción/es seleccionadas.

Voto anónimo : El sistema debe poder romper la relación existente entre el voto y el votante. Deben desarrollarse los protocolos criptográficos y de infraestructura necesarios para que nadie pueda vincular el contenido del voto a un votante determinado.

4.1.5. Requisitos propios del voto electrónico

******** AQUÍ HAY QUE DEFINIR LOS REQUISITOS DEL VOTO ELECTRÓNICO. DEPENDE DEL AUTOR, HAY UNOS U OTROS. HABRÁ QUE DEFINIR CUÁLES SON LOS QUE VAMOS A TENER EN CUENTA PARA ESTE PROYECTO. ESTÁN EN –TEMP– ESPERANDO A QUE TOME LA DECISIÓN A partir de los requisitos estudiados al estudiar el estado actual del voto electrónico en 1.3.1, consideramos los siguientes requisitos como los implícitos al voto electrónico:

Autenticidad : Sólo los votantes autorizados pueden votar. La autorización de un votante para ejercer su derecho al voto está expresada en el censo electoral conformado por la Autoridad Electoral competente. El sistema debe comprobar que el votante que quiere realizar un voto debe estar inscrito correctamente en el censo electoral y que en éste no se indique que tiene vetada su participación en el proceso.

Anonimato : El voto es secreto. Ningún votante, observador o manipulador del sistema puede tener la habilidad o herramienta de poder conocer el voto que ha sufragado otro votante en ningún momento del proceso electoral.

Verificabilidad : El votante puede asegurarse de que su voto se ha contado adecuadamente. El sistema debe ase El sistema tiene que proporcionar una herramienta que permita a un votante poder verificar que la opción por la que ha votado ha sido correctamente añadida a los resultados consolidados del proceso electoral, sin que por ello pueda violarse el requisito de Anonimato, asegurando que ningún actor del sistema pueda tener acceso al contenido de dicho voto.

Imposibilidad de coacción : El voto emitido no puede ser mostrado. El sistema debe evitar que el voto emitido pueda ser mostrado a un tercer actor con el fin de evitar la coacción al votante por medio de éste. **********
NO ESTOY DE ACUERDO CON ESTO. ALGUNOS AUTORES INDICAN LO CONTRARIO, QUE ES PRIMORDIAL QUE EL VOTANTE SE QUEDE CON UNA PRUEBA DE SU VOTO. DE TODOS MODOS CONSIDERO QUE SI SE CUMPLE EL REQUISITO DE VERIFICABILIDAD, ES MEJOR CUMPLIR ESTE, PERO NO POR HACERLO VAMOS A CONSEGUIR REBAJAR EL RIESGO DE COACCIÓN, ¿O SÍ? **********

Posibilidad de emitir un voto nulo . El sistema debe dar la opción al votante de que pueda realizar un voto nulo, al igual que puede realizarlo en un proceso electoral no electrónico.

Fiabilidad : el sistema debe asegurar que no se producen alteraciones de los resultados. Es esencial que el sistema asegure que, aunque existan riesgos inherentes a cualquier sistema informático, estos no van a afectar los resultados del proceso electoral.

Auditabilidad : se debe poder comprobar que el funcionamiento de los elementos que intervienen en el proceso es correcto. Para favorecer la transparencia del proceso, es muy importante que el sistema proporcione unas herramientas que permitan tanto la monitorización del proceso como auditorías del mismo. Estas herramientas deben ser fiables y demostrar tanto su correcto funcionamiento como el del proceso electoral en si mismo a una serie de actores designados (operadores, auditores, observadores).

Usabilidad : cualquier votante debe ser capaz de emitir un voto en un tiempo

razonable. El sistema debe ser usable y accesible, debe facilitar el proceso de emisión de voto a prácticamente la totalidad del electorado.

4.1.6. Requisitos del proceso electoral

Ejemplo : Aquí va un requisito.

4.1.7. Requisitos no funcionales

Bajo coste : El coste del sistema debe ser relativamente bajo. Teniendo en cuenta las características del cliente, una Escuela o Universidad y los potenciales desarrolladores del proyecto, estudiantes, es importante procurar que el espíritu del sistema a implementar se base en ek bajo coste. Con este principio, se pueden ahorrar recursos económicos a la institución que podría destinar a otras necesidades. Por ello, se considera importante promover la utilización de software libre o sin licencia, así como reducir el número de responsables en la gestión del proceso electoral a nivel de control del sistema informático y la utilización de tecnologías hardware que reduzcan el desembolso de capital, como es la utilización de software de virtualización frente a la inversión en máquinas, mucho más costosas.

Soporte a usuarios : El sistema debe proporcionar unas herramientas de soporte a usuarios de cualquier rol que hagan uso del mismo. Al ser un sistema de votación nuevo, diferente al tradicional y con una característica tecnológica por medio, es fundamental que se ofrezca soporte, tanto técnico como de procedimiento a los usuarios del sistema en la jornada electoral, ya sean votantes activos como responsables de la autoridad electoral, auditores u observadores del proceso. Hay que procurar que puedan disponer de la información y el soporte necesario para que todos puedan realizar sus funciones durante la jornada electoral sin problemas o, al menos, minimizándolos.

4.1.8. Necesidades del esquema de voto electrónico

Votación por Internet : ~~El sistema de votación debe funcionar de forma remota en sus fases de registro, identificación, votación y consulta de resultados. Cualquier votante puede acceder a las funcionalidades del sistema a las que tiene autorización desde cualquier punto conectado a Internet.~~

Identificación remota : El sistema debe implementar un mecanismo que sea capaz de asegurar la identificación de un votante en el sistema de forma remota, digitalmente, sin posibilidad de error. Existen varias soluciones para solventar este requisito, como son los certificados digitales electrónicos externos (contenidos en tarjetas de soporte físico como una smartcard, el DNI o la TUI de la Universidad), la identificación biométrica, acceso por usuario y contraseña con pasos extras para aumentar la seguridad.

Autenticación remota : El sistema debe poder autenticar a los votantes que tratan de usar su identificación digital para ingresar en el sistema de forma remota. El sistema no debe errar en esta autenticación, permitiendo la entrada de los votantes autorizados y revocando el acceso a los atacantes, suplantadores o desautorizados. No sólo debe ser capaz de permitir que un votante pueda asegurar la veracidad de su identidad, sino que debe permitir la autenticación del mismo de cara al sistema y a la Autoridad Electoral.

Firma digital : Para poder cumplir con el voto remoto, es necesario que el sistema permita el uso de la firma digital, ya que es una herramienta clave para poder verificar la identidad y autenticidad de un votante, así como la validez del voto que emite.

Permitir votación presencial : El sistema debe proporcionar los mecanismos necesarios para facilitar el voto a aquellos votantes con derecho al mismo que quieran emitirlo de forma presencial en el periodo habilitado para ello. Este requisito trata de preservar la tradición de estos procesos electorales en los que se fijaba una fecha para el sufragio y se acudía a la urna. Así, del mismo modo, hay que adecuar una serie de equipos en los centros de votación habituales que, aunque estén conectados a Internet y el voto siga siendo remoto, permitan a los votantes que lo deseen hacer uso de su derecho al voto sin tener que salir de la Escuela. ******* NOTA: (Analizando este requisito, la mejor forma es habilitando un horario en la sala de ordenadores de la Escuela destinados a que las personas que quieran puedan votar de forma remota desde estos puestos) *********

Disponibilidad total : El sistema debe estar disponible para proporcionar servicio de voto durante todo el periodo estipulado en las normas que se fijen para la elección. Aunque el sistema entra en producción para llevar a cabo funciones que se realizan en la llamada fase preelectoral, el momento más crítico e importante se presupone que es la propia jornada electoral.

El sistema debe estar preparado para su uso al comienzo de ésta y debe estar activo, accesible a los votantes y sin caídas durante la duración de la misma.

Voto anónimo : Este es un requisito implícito del voto electrónico. Por ello, para el esquema de votación que se ha de utilizar es fundamental tenerlo en cuenta. Han de integrarse los protocolos criptográficos y de infraestructura necesarios para que nadie pueda vincular el contenido de un coto a un votante determinado. ********** ESTO QUIZÁ DEBERÍA QUEDARSE DIRECTAMENTE EN LOS REQUISITOS IMPLÍCITOS AL VOTO ELECTRÓNICO. DE HECHO, A PARTIR DE ELLOS Y PINCELADAS DE ESTA SUBSECCIÓN SE HAN DE SENTAR LAS BASES DEL ESQUEMA DE VOTO ELECTRÓNICO A IMPLEMENTAR **********

Papeleta/boleta digital : El sistema debe mostrar al votante la papeleta o boleta (dependiendo del tipo de elección) correspondiente a la elección y el censo que le corresponda. Debe contener las opciones o candidatos entre las que puede seleccionar o elegir y mantener correctamente la/s opción/es seleccionada/s.

Voto múltiple: ~~El sistema debe permitir a los votantes votar más de una vez, invalidando cada vez que emite un voto, los votos anteriores que hubiese introducido en el sistema. (********** ¿QUEREMOS ESTO? TOTAL, EL RIESGO DE COACCIÓN ES MUY BAJO EN ESTAS ELECCIONES... PERO SI QUEREMOS ACERCARNOS A UNAS GENERALES, QUIZÁS SEA IMPEPINABLE, SIGUIENDO EL MODELO ESTONIO **********)~~

********** ESTO ES TEMPORAL. VOY A IR HACIENDO UNA LISTA DE REQUISITOS SEGÚN LOS VOY CONOCIENDO. ESTA LISTA ES EL BATIBURRILLO, CUANDO ESTÉN CLAROS, LOS VOY COLOCANDO EN SUS TIPOS CORRESPONDIENTES Y LOS DEFINIMOS FORMALMENTE SEGÚN LA PLANTILLA **********

********** OTRA FORMA EN LA QUE PODEMOS ORDENAR LA ESPECIFICACIÓN DE REQUISITOS HAY QUE RE-REDACTARLO **********

Para la especificación de los requisitos que ha de satisfacer el sistema, se van a seguir algunas de las recomendaciones del IEEE en el estándar IEEE 830-1998 [14], ya que éste establece las normas para la realización de un documento formal y completo de especificación de requisitos (SRS en inglés).

Algunas de las modificaciones vienen inspiradas en este proyecto [18] y en este post al respecto [12], determinando una serie de tipos de requisitos más

específica que los que define el estándar original.
Con esto, vamos a describir los requisitos necesarios para la consecución del proyecto según la siguiente tipología:

Restricciones de diseño : requisitos que limitan el desarrollo al crear el producto. Se etiquetan como RD.x, siendo x el número del requisito.

Requisitos funcionales : Conjunto de requisitos que reflejan la funcionalidad que debe prestar el sistema. Se etiquetan como RF.x, siendo x el número del requisito.

Requisitos de la interfaz : Conjunto de requisitos que definen las necesidades de la interacción del software con otros sistemas y usuarios. Se etiquetan como IN.x, siendo x el número del requisito.

Requisitos de calidad : Exigencias en la calidad que se piden explícitamente para el producto. En esta categoría se engloban los requisitos de rendimiento, escalabilidad, accesibilidad, usabilidad, etc. Se etiquetan como CA.x, siendo x el número del requisito.

Requisitos de evolución : Requisitos para el diseño del producto con el objetivo de facilitar la adaptación a exigencias o condiciones que puedan surgir en el futuro. Se etiquetan como EV.x, siendo x el número del requisito.

Requisitos del proyecto : Requisitos que afectan y condicionan el proceso de desarrollo del proyecto. Se etiquetan como PR.x, siendo x el número del requisito.

Requisitos de soporte : Requisitos que deben ser cumplidos por el cliente. Se etiquetan como SO.x, siendo x el número del requisito.

Dentro de la clasificación anterior, cada requisito debe especificarse formalmente, empleando para ello la siguiente plantilla:

Descripción : Descripción corta del requisito.

Importancia : La importancia del requisito, con tres valores:

Esencial El incumplimiento de este requisito provocaría el fracaso del proyecto.

Condicional El requisito mejoraría el resultado final del desarrollo.

Opcional El requisito no tiene que ser implementado, pero se puede tener en cuenta al realizar el diseño del producto).

Validez : Este apartado demuestra la validez del requisito. tiene cuatro secciones, que estarían presentes sólo en el caso de ser relevantes para ese requisito concreto.

Medible : Describe cómo comprobar el grado de cumplimiento del requisito.

Alcanzable : Propone, de un modo general, un camino para lograr su consecución.

Relevante : Justifica la presencia del requisito en el documento, indicando cómo ayuda a definir la entidad global del producto.

Específico : Extiende la descripción del requisito, con referencia a los casos de uso, si fuesen relevantes.

4.1.9. Restricciones de diseño

4.1.10. Requisitos funcionales

4.1.11. Requisitos de la interfaz

4.1.12. Requisitos de calidad

4.1.13. Requisitos de evolución

4.1.14. Requisitos del proyecto

4.1.15. Requisitos de soporte

****

**** LO QUE HAY QUE DESARROLLAR **** Requisitos de Usuarios: Necesidades que los usuarios expresan verbalmente Requisitos del Sistema: Son los componentes que el sistema debe tener para realizar determinadas tareas Requisitos Funcionales: Servicios que el sistema debe proporcionar Requisitos no funcionales: Restricciones que afectan al sistema

4.2. Roles / Actores

Considerando el flujo del votante en el sistema, identificamos cuatro roles en el sistema que deben ser tenidos en cuenta de cara a las funcionalidades,

privilegios y responsabilidades que tienen que encontrar en el uso del mismo.

Votante

El votante es el actor principal del sistema, pues es al que va dirigido el proceso de votación. Es el único rol que tiene la capacidad de votar. Las acciones que puede realizar son:

- Consultar su presencia en el censo.
- Identificarse unívocamente en el sistema.
- Elegir la papeleta con su voto.
- Capacidad de poder emitir un voto nulo.
- Firmar el voto.
- Votar preservando el carácter anónimo del voto.
- Consultar que su voto ha sido contabilizado.

Administrador

El administrador es el rol encargado de gestión de las fases electorales. Tiene responsabilidad y potestad de:

- Iniciar el proceso electoral.
- Iniciar el proceso de votación.
- Terminar el proceso de votación.
- Apertura de la urna
- Inicio del escrutinio
- Apertura de los canales de difusión de resultados.
- Finalizar el proceso electoral.

Miembro de la Junta Electoral

********** CAMBIAR EL NOMBRE ********** Una vez el administrador de la elección dé por finalizado el proceso electoral, se requerirá que varios miembros de la Junta Electoral proporcionen unas claves personales que, juntando varias de ellas, servirán como llave lógica para la apertura de la urna que contiene los votos.

Los usuarios con este rol no pueden votar. El miembro de la Junta Electoral no forma parte del censo de votantes acreditados para votar en las elecciones, por lo que no puede tener acceso al módulo de votación.

Auditor

El auditor debe tener acceso a una serie de funcionalidades del sistema. Su función es velar porque el desarrollo del proceso electoral se realiza sin ningún tipo de fallo o de interferencia por parte de algún atacante.
Los usuarios con este rol no pueden votar. El auditor no forma parte del censo de votantes acreditados para votar en las elecciones, por lo que no puede tener acceso al módulo de votación.
Su misión es de control, por lo que ninguna acción que realice en el sistema puede afectar al desarrollo de la elección.

Autoridad Certificadora

Junto con los cuatro roles expuestos, encontramos un quinto actor en la figura de la Autoridad Certificadora. Esta entidad es la encargada de generar, administrar, validar y verificar las credenciales que han de usar cada uno de los votantes para emitir el voto, así como los de cada uno de los actores del proceso (administradores, miembros de la Junta Electoral, auditores o incluso los sistemas y sus comunicaciones).

Los usuarios cuyo rol sea Votante son los únicos que tienen capacidad para poder votar en la elección. Hay usuarios que pueden ejercer varios roles en el sistema. Tanto un Administrador como, sobre todo, un Miembro de la Autoridad Electoral, perteneciendo a la Universidad pueden tener derecho al voto. En estos casos, para mantener la transparencia y fiabilidad del proceso, las persona que ejerzan estos roles, a la hora de votar deberán hacerlo accediendo al sistema con un usuario distinto, con un rol asignado de Votante, garantizando que no pueden acceder con éste a ningún otro módulo del sistema. Se entiende que los roles de Auditor ~~o de Observador~~ están destinados a personas ajenas a la votación que tienen como objetivo vigilar y asegurar que la elección se lleva a cabo de forma limpia y correcta. Por ende, se entiende que las personas con usuarios asociados a estos roles no deben acceder al sistema de votación en ningún caso, además de que no deberían aparecer acreditados en el censo electoral.

4.3. Modelo Conceptual

**********A partir de los requisitos de información, se desarrollará un diagrama conceptual de clases UML, identificando las clases, atributos, relaciones, restricciones adicionales y reglas de derivación necesarias.**********

4.4. Modelo de Casos de Uso

********** A partir de los requisitos funcionales descritos anteriormente, se emplearan los casos de uso como mecanismo para representar las interacciones entre los actores y el sistema bajo estudio. Para cada caso de uso deberá indicarse los actores implicados, las precondiciones y postcondiciones, los pasos que conforman el escenario principal y el conjunto de posibles escenarios alternativos. **********

4.4.1. Actores

********** En este apartado se describirán los diferentes roles que juegan los usuarios que interactúan con el sistema. Los actores pueden ser roles de personas físicas, sistemas externos o incluso el tiempo (eventos temporales). **********

4.5. Modelo de Comportamiento

********** A partir de los casos de uso anteriores, se crea el modelo de comportamiento. Para ello, se realizarán los diagramas de secuencia del sistema, donde se identificarán las operaciones o servicios del sistema. Luego, se detallará el contrato de las operaciones identificadas. **********

4.6. Modelo de Interfaz de Usuario

********** En esta sección se deberá incluir un prototipo de baja fidelidad o mockup de la interfaz de usuario del sistema. Además, es preciso elaborar un diagrama de navegación, reflejando la secuencia de pantallas a las que tienen acceso los diferentes roles de usuario y la conexión entre éstas. **********

Capítulo 5

Solución

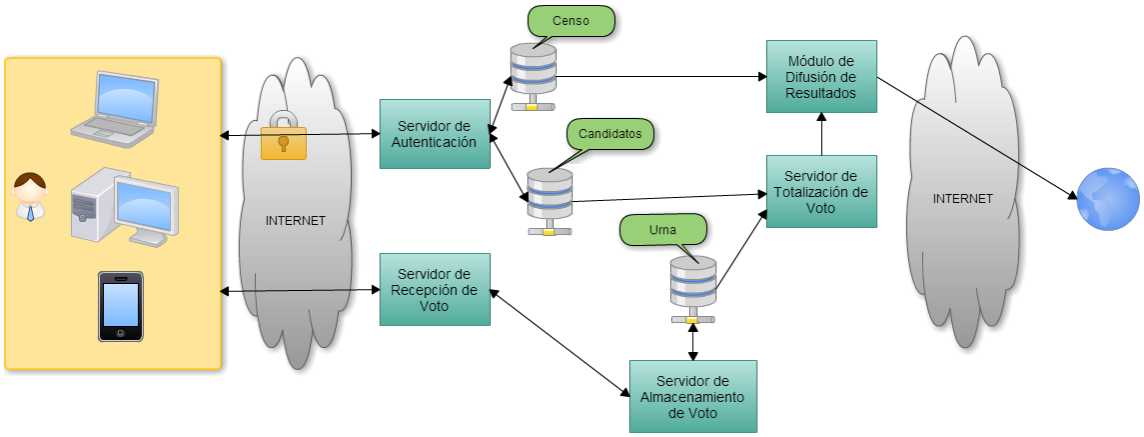

Figura 5.1: *Diagrama de flujo del Sistema*

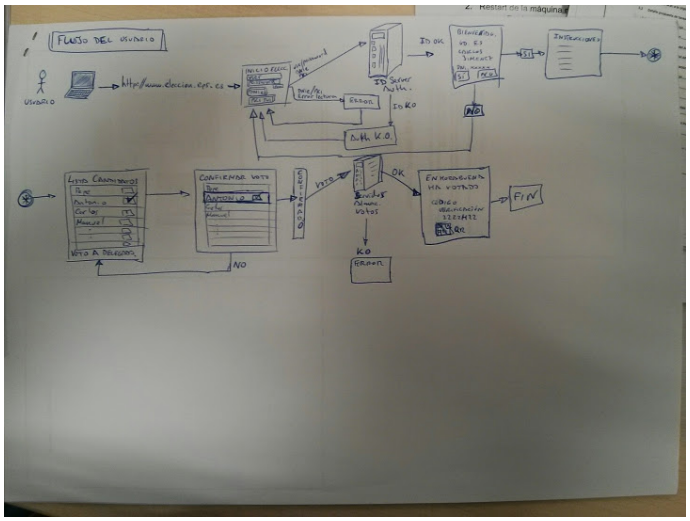

Figura 5.2: *Esquema del flujo que sigue el votante*

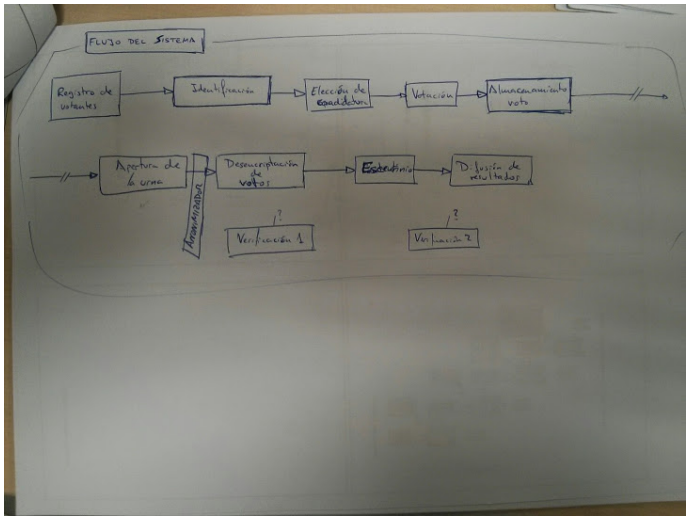

Figura 5.3: *Esquema del flujo del Sistema*

5.1. Diseño

5.1.1. Diseño del esquema de votación

5.1.1.1. Registro

5.1.1.2. Identificación

5.1.1.3. Elección de candidatura

5.1.1.4. Votación

5.1.1.5. Escrutinio

5.1.1.6. Difusión de resultados

5.1.2. Diseño de la arquitectura

5.1.3. Diseño de la capa de datos

5.1.4. Diseño de la red

5.1.5. Diseño de la interfaz de usuario

5.1.5.1. Estructura de la página web

5.1.5.2. Estructura de la aplicación móvil

5.1.5.3. Colores

5.1.5.4. Logo de la elección

5.1.5.5. Ergonomía

En varios de los sistemas estudiados que se han desarrollado para intentar implantar el voto electrónico a un nivel medio, como pueden ser los mexicanos SELES 1.3.8.8 y SEVI 1.3.8.9 o los españoles de Víctor Moreno [18] *****o Votescript 1.3.8.6??????******** se observa que se realiza una división del proceso electoral en cuatro fases (Registro, Votación, Consolidación de resultados y Auditoría). En el desarrollo de este sistema vamos a identificar las mismas fases, pero con matices.

Así, en una primera visión global del sistema, en este se definen cuatro fases:

- Preelectoral

- Votación
- Consolidación de resultados
- Postelectoral

Realmente, la mayor diferencia con las fases definidas en los esquemas anteriores se corresponden con el alcance de la primera y la última fase. La fase Preelectoral, denominada comúnmente en los ejemplos estudiados en la Introducción como fase de Registro, en este sistema tiene un alcance mayor. En este proceso electoral no se requiere que el votante se registre para poder votar. El censo lo proporciona la Autoridad Electoral y se carga en el sistema. Igualmente, en los días previos a la jornada electoral el sistema permitirá a los votantes comprobar si están en el censo y qué información contiene éste, tanto personal - para asegurarse de que podrán identificarse - como de permisos de cara a realizar la votación.

La fase postelectoral, que denominan de Auditoría, preferimos dejarla como postelectoral al considerar que la auditoría del sistema es una operativa que se realiza durante toda la jornada electoral, no sólo al finalizar ésta. No obstante, es cierto que al final se llevarán a cabo auditorías de los resultados y el funcionamiento. Además de las auditorías llevadas a cabo por los auditores *oficiales*, se va a implementar un mecanismo que permita a los propios votante auditar que su voto ha sido correctamente incluido y contado en el proceso. Esta fase postelectoral también tiene más operativas ... **********

Las fase de votación también tiene un alcance diferente. En primer lugar, empieza con la identificación del votante en el sistema electoral. Una vez el votante ha sido correctamente identificado por el sistema (tal como lo haría contra los miembros de la mesa en el voto tradicional), debe recibir una boleta electrónica que le ofrezca las opciones entre las que, por su circunscripción, deba elegir la que desea votar. Una vez seleccionado, es el momento en el que realmente el votante realiza la votación, traspasando el voto de forma digital al sistema, a la *urna digital* donde se anonimizarán y almacenarán hasta la fase de consolidación.

En la fase de consolidación de resultados, el sistema se encargará del conteo de los votos que han sido emitidos

******** Antes de este punto hay que hacer un resumen de los diferentes esquemas de votación, teniendo estos como Firma ciega, mixnets, etc...**********

5.1.6. Protocolo

Como se ha comentado en capítulos anteriores, hay una multitud de soluciones propuestas para el voto telemático.

Teniendo en cuenta el objetivo de este Proyecto Fin de Carrera, de los sistemas implementados a gran escala, a nivel nacional o regional, podemos destacar Estonia, Noruega y los cantones suizos como las tres experiencias más exitosas y aquellas de las que se pueden estudiar las soluciones, esquemas y protocolos utilizados. No obstante, el alcance de las mismas supera sobremanera el de este proyecto. Igualmente, muchas decisiones las toman en base a satisfacer requisitos que resultan muy importantes en su análisis, pero que en este trabajo no se ha considerado que tengan igual trascendencia, y viceversa, por lo que se han de tomar diferentes consideraciones frente a los mismos problemas dependiendo del impacto que suponen en cada proyecto.

También se han presentado casos de proyectos de voto telemático pensados a menor escala. Entre ellos, hay muchas soluciones que, en parte, podrían satisfacer los requisitos de este proyecto. No obstante en ninguno de ellos encontramos un protocolo que se adapte completamente a los requerimientos planteados, ya que, en algún momento, se analiza un elemento que los hace diferir. Por ejemplo, un proyecto ya maduro como Votescript 1.3.8.6 realiza un estudio académico y técnico muy profundo acerca del voto telemático pero, por su propia definición, el modelo de identificación y emisión del voto lo sitúan físicamente en centros de votación. Este elemento es diferencial para este proyecto, pensado en el voto telemático remoto, aunque puede integrarse cuando se estudian alternativas para que aquellos votantes que, por algún motivo, no pueden o quieren votar por Internet de forma remota tengan la oportunidad de ejercer su derecho de sufragio desde un lugar habilitado para ello por la propia Escuela.

A partir de los esquemas criptográficos estudiados y con ayuda de algunos protocolos ya publicados en otros proyectos, el siguiente paso es diseñar el protocolo de votación que se adapte a las necesidades del Proyecto, cumpliendo con los requisitos y asegurando los niveles de seguridad planteados.

En muchas de las soluciones estudiadas se observa que no recibe la importancia necesaria la fase de identificación del votante. Los mecanismos de identificación y autenticación del mismo resultan laxos desde el punto de vista de la seguridad ante el fraude electoral. Por ello han sido descartadas las soluciones basadas en identificación por medio de bases de datos con el típico protocolo de usuario/contraseña o incluso con elementos de seguridad de una generación algo posterior, como pin, patrones, captchas, operaciones aritméticas o métodos

similares con mayor o menor complejidad. Igualmente, se han descartado aquellos métodos de identificación que requieran la presencia física del votante frente a los responsables de la mesa de votación, ya que se busca el diseño de un sistema remoto. Así descartamos protocolos de identificación como los publicados por Votescript, en el que el votante acude a un centro o local de votación, se identifica ante la mesa electoral y recibe un token criptográfico personalizado con el que se le permite ejercer el sufragio.

La mayoría de las soluciones estudiadas previamente a la realización de esta memoria centran sus esfuerzos en la fase de votación. Buscan la elaboración de un protocolo robusto, basado en esquemas criptográficos, que permita la mayor seguridad posible al cumplimiento de los requisitos fundamentales del voto electrónico, dotando al sistema de privacidad del votante, **********

5.1.6.1. Descripción del sistema

El sistema contará de cinco fases, determinadas por el flujo temporal de la votación. Preelectoral, Identificación, Votación, Escrutinio y publicación de resultados. Adicionalmente, se tendrá en cuenta un sistema de auditoría, de carácter transversal a este flujo, ya que debe estar disponible durante todo el proceso de votación.

********** No he podido conseguir reglamentación oficial de la elección, así que, básicamente, propongo yo las fases y la problemática ... esto, con palabras aquí escrito y bien puesto **********

El sistema que se propone en este PFC es un sistema integral. Busca sostener el proceso electoral desde el comienzo hasta el final del mismo. Por ello empieza en el momento mismo de definición del censo y no termina hasta que la publicación de resultados y su auditoría son oficializadas por el órgano rector de la Elección.

La primera fase, preelectoral, es aquella previa al día electoral, en la cual se definen las bases en las que se rige el proceso electoral. Así, es imprescindible cumplimentar varias acciones por parte de los desarrolladores, administradores y órgano electoral. En primer lugar, es fundamental la elaboración de un censo electoral. En éste se recogen los potenciales votantes, aquellos con derecho a voto, identificando, además, la circunscripción ********** ??¿¿??¿¿ no hay mejor nombre ??? ********** a la que pertenece. En unas elecciones legislativas, una circunscripción electoral se puede definir como el conjunto de electores a partir del cual se procede la distribución de los escaños asignados, en función de la distribución del los votos sufragados. En

las elecciones legislativas españolas, las circunscripciones se corresponden con las provincias españolas (excepto en el caso de Aturias, que está subdividida en 3 distritos electorales, y la Región de Murcia, que lo hace en 5). Esto significa que del total de diputados que se eligen en este proceso para la totalidad de España, en vez de repartirlos con el recuento total de los votos, se reparten los cargos por cada circunscripción, dependiendo del número de electores de cada una, con lo que los votantes censados en una circunscripción, digamos por ejemplo la provincia de Málaga, elegirán a un número determinado de diputados que serán quienes les representen en el Congreso junto a los elegidos en el resto de territorios españoles. En las Elecciones al Parlamento Europeo, sin embargo, España actúa como una única circunscripción, por lo que los diputados que representarán al país en la cámara supranacional se obtendrán a base de repatir los escaños con respecto al total de votos recogidos en todo el territorio español. Algo parecido es lo que se va a definir en el censo electoral. Además de recoger de forma unívoca a los electores con derecho al voto, se tendrán que sumar las ********** necesarias para su correcta identificación, así como la "circunscripción" a la que pertenece, es decir, el grupo sobre el que debe escoger a sus representantes, con el fin de que la opción de voto que el sistema le presente y la que introduzca en el sistema sea correcta. Se vislumbran aquí dos requisitos del voto electrónico que necesitan ser satisfechos para la integridad del proceso electoral. En primer lugar, es básico que el censo defina claramente los votantes con derecho al voto y provea de la información necesaria para que se pueda comprobar la identidad del votante en el momento en el que se disponga a votar. En las elecciones con voto tradicional esto se conseguía añadiendo datos personales tales como el número del DNI, del Pasaporte o, en caso de estas elecciones, el número de identificación del alumno. Así, al acudir a la mesa electoral todos los votantes tenían estos datos con los que se podían identificar frente a los miembros de la misma, los cuales tienen la potestad de permitirles votar o no. Integridad del voto. El hecho de relacionar cada votante con una "circunscripción" es esencial a la hora de mantener la integridad de la votación, pues hay que tener en cuenta los candidatos a los que cada votante puede votar, ya que no son los mismos para todos. Igual que en unas legislativas españolas un votante de Málaga no elige entre los mismos candidatos que lo hace un votante de Lugo, en estas elecciones, un alumno elige sus representantes entre los delegados de curso, mientras que los profesores, por su parte, lo hacen entre otros colegas profesores. Es indispensable, pues, gestionar correctamente estas relaciones ya que no se deben recoger votos de votantes a candidatos a los que

no tiene derecho a elegir.

En el caso de esta elección, es la propia Escuela Politécnica Superior la que debe proveer el censo oficial a los administradores del sistema, los cuales procederán a cargarlo en el mismo a través de los mecanismos implementados para ello. (Aquí encontramos un primer punto de auditoría importante). (En algunos países, en vez de elaborarse un censo oficial, son los propios votantes los que han de registrarse)

********** Lo he liado todo **********

Es requisito de la Institución que convoca el proceso electoral el definir las "reglas del juego". En este caso, el órgano de la EPS encargado de la celebración de las elecciones ha de definir los mecanismos de votación para que el sistema se pueda adaptar y mantener ..... **********

Candidatos. Es necesario que los candidatos puedan presentar su candidatura e incorporarse al sistema para que éste pueda gestionarlos para presentarlos como opciones a los votantes determinados, además de en el momento de consolidación de los votos y posterior publicación de resultados. En muchos procesos se realizan desarrollos que permiten a los partidos políticos registrar sus listas electorales y/o candidatos de forma remota durante el plazo determinado que la Ley Electoral les indica. Así, los partidos inscriben a sus representantes en el proceso electoral. En el caso de esta elección, debido a su carácter tan localizado no vemos necesidad de ello y corresponde a la Escuela Politécnica Superior proporcionar el listado de candidatos elegible y las circunscripciones a las que se presentan. ********** Para futuros desarrollos, pensando en la escalabilidad del sistema, se podría desarrollar este punto para que este proceso sea independiente de los órganos electorales de la EPS **********.

En las elecciones tradicionales, es también necesaria la formación de las mesas electorales, con la definición del número de ellas que son necesarias y la designación de los miembros que van a formar parte de ella. En una elección electrónica y remota, como la que hemos diseñado, el concepto de mesa se puede mantener, sobre todo para poder gestionar las circunscripciones y para continuar con las estadísticas de participación tradicionales, basadas en agrupaciones y disgregaciones de mesas. Sin embargo, al transformarse en un concepto lógico, se pierde el sentido de la designación de los miembros de mesa, por lo que no será un punto a tener en cuenta en el proceso.

********** Pasamos a la siguiente fase: Identificación **********
Una vez acometidas todas las gestiones de la fase preelectoral, pasamos a la fase correspondiente al llamado Día Electoral (aunque realmente la elección en

vez de en un día, se pueda alargar a lo largo de un período de tiempo mayor). Tratando de emular a las elecciones tradicionales, esta fase comienza con la apertura de los colegios electorales y las mesas que los componen. En el caso digital, serán los miembros designados por la Junta Electoral los que, previa identificación y requerimiento de sus credenciales digitales, pongan en marcha el sistema en su fase electoral. Será una apertura de los colegios de forma virtual, permitiendo que los votantes puedan acceder al sistema y proceder a votar. La fase de identificación del votante es una fase realmente importante. En las elecciones de voto tradicional, el proceso normal consiste en que el votante acude a la mesa electoral y muestra a los miembros de mesa alguna identificación de curso legal, respaldada por alguna institución estatal reconocida y capacitada. Los miembros de la mesa electoral contrastan la identificación presentada con la información recogida en el censo electoral de dicha mesa y deciden si es suficiente o no para permitir al votante introducir su voto en la urna. En el caso de las elecciones legislativas españolas los documentos que se pueden mostrar son DNI, pasaporte o permiso de conducir. Todos estos documentos son válidos para votar incluso estando caducados. Han de mostrar la fotografía del votante para permitir la identificación por parte de los miembros de mesa, por lo que, aunque sea válido que estén caducados, no se permite utilizar el resguardo de DNI en trámite. ********** En el caso de las elecciones de la EPS, los documentos válidos son .-..... ********** Es requisito el sustituir este sistema de identificación del elector por otro en el que no sea necesaria la presencia física de éste ni de los miembros de mesa para permitir el voto, aunque manteniendo el mismo nivel de seguridad en el proceso. Aquí se hace indispensable estudiar las opciones de identificación digital que se pueden implementar para .....

Lo ideal es disponer de documentos que contengan tokens criptográficos propios que puedan ser utilizados en los diferentes procesos de identificación y voto. Por ello, vamos a utilizar documentos que los disponen. Así, los documentos válidos para ejercer el derecho al voto serán el DNIe (tanto la primera versión como la denominada 3.0, presentada en enero de 2015) y la TUI (**********) de la Universidad San Pablo-CEU. En sendos documentos encontramos elementos criptográficos que identifican unívocamente a su dueño. Además encontramos en ellos certificados para la firma digital, que serán necesarios para la fase de votación.

El votante se identifica con su documento digital de forma remota. Es necesario que disponga de un lector de chip electrónico conectado al dispositivo desde

el que va a realizar el voto.

El siguiente paso

Capítulo 6

Plan de pruebas

Capítulo 7

Líneas futuras

Capítulo 8

Conclusiones

Bibliografía

[1] BURNAND, F. E-voting to advance slowly in 2011. http://www.swissinfo.ch/eng/e-voting-to-advance-slowly-in-2011/29138944, 2011.

[2] CABELLO PARDOS, A.B., HERNÁNDEZ ENCINAS, A., HOYA WHITE, S., MARTÍN DEL REY, A., AND RODRÍGUEZ SÁNCHEZ, G. Un protocolo de votación electrónica basado en firmas digitales ciegas. *Universidad de Sevilla. XX Congreo sde Ecuaciones Diferenciales y Aplicaciones. X Congreso de Matemática Aplicada* (Septiembre 2007).

[3] CARRACEDO VERDE, JOSÉ DAVID, GÓMEZ OLIVA, ANA, MORENO BLÁZQUEZ, JESÚS, PÉREZ BELLEBONI, EMILIA, AND CARRACEDO GALLARDO, JUSTO. Votación electrónica basada en criptografía avanzada (proyecto votescript). *Universidad Politécnica de Madrid* (2002). http://vototelematico.diatel.upm.es/articulos/articulo_venezuela_revisado.pdf.

[4] Certificados digitales - fnmt. https://www.cert.fnmt.es/curso-de-criptografia/certificados-digitales.

[5] CHAUM, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM 24*, 2 (Feb. 1981), 84–90.

[6] CHEN, X., WU, Q., ZHANG, F., TIAN, H., WEI, B., LEE, B., LEE, H., AND KIM, K. New receipt-free voting scheme using double-trapdoor commitment. *Information Sciences 181*, 8 (2011), 1493 – 1502.

[7] CORTÉS POLO, DAVID MIGUEL, HORNERO ÍNCERA, ALEXEI, MARTÍNEZ BRAVO, LORENZO, AND GONZÁLEZ-SÁNCHEZ, JOSÉ LUIS. Estudio de infraestructura par sistemas de voto electrónico. *Departamento de Informática, Escuela Politécnica. Universidad de Extremadura* (-). http://gitaca.unex.es/agila/voto/voto.pdf.

[8] DELLA PAOLERA, P. La prueba de Conocimiento Cero o Nulo. http://paolera.wordpress.com/2014/06/27/la-prueba-de-conocimiento-cero-o-nulo/, Junio 2014.

[9] Internet Voting - Voting methods in Estonia - Estonian National Electoral Committee. http://www.vvk.ee/voting-methods-in-estonia/engindex/.

[10] FUJIOKA, ATSUSHI, OKAMOTO, TATSUAKI, AND OHTA, KAZUO. A practical secret voting scheme for large scale elections. In *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology* (London, UK, UK, 1993), ASIACRIPT '92, Springer-Verlag, pp. 244–251.

[11] GARCÍA ZAMORA, C. P. Diseño y desarrollo de un sistema para elecciones electrónicas seguras (seles). Master's thesis, Centro de Investigacion y de Estudios Avanzados del Instituto Politecnico Nacional. Departamento de Ingeniería Eléctrica. Sección de Computación, Septiembre 2005. http://delta.cs.cinvestav.mx/~francisco/Repository/tesisCPGZ.pdf.

[12] GARCIA MONDARAY, S. Especificación de requisitos software con IEEE 830-1998. http://www.godtic.com/blog/2012/11/18/especificacion-de-requisitos-software-con-ieee-830-1998/, Noviembre 2012.

[13] HERSCHBERG, M. A. Secure electronic voting over the world wide web. Master's thesis, Department of Electrical Engineering and Computer Science, MIT - Massachusetts Institute of Technology, Mayo 1997.

[14] IEEE. IEEE Recommended Practice for Software Requirements Specifications. *IEEE Std 830-1998* (1998).

[15] LÓPEZ GARCIA, M. D. L. Sistema electrónico de votación. Master's thesis, Benemérita Universidad Autónoma de Puebla. Facultad de Ciencias de la Computación, Febrero 2007. http://delta.cs.cinvestav.mx/~francisco/TesisMaestriaFinal_Lourdes.pdf.

[16] LÓPEZ GARCIA, M. D. L. *Diseño de un protocolo para votaciones electrónicas basado en firmas a ciegas definidas sobre emparejamientos bilineales*. PhD thesis, Centro de Investigacion y de Estudios Avanzados del Instituto Politecnico Nacional. Departamento de Computación, Junio 2011. http://www.cs.cinvestav.mx/TesisGraduados/2011/TesisLourdesLopez.pdf.

[17] MORALES ROCHA, V. M. *Seguridad en los procesos de voto electrónico remoto: registro, votación, consolidación de resultados y auditoría*. PhD thesis, Universitat Politècnica de Catalunya. Departament d'Enginyeria Telemàtica, Marzo 2009. http://www.tdx.cat/bitstream/handle/10803/7043/01VMmr01de01.pdf.

[18] MORENO PEÑA, ADRIÁN. Portal web para la gestiómn de información de un departamento universitario en la usc. Master's thesis, Escuela Técnica Superior de Ingeniería - Universidad de Santiago de Compostela, Diciembre 2007. http://bloqnum.com/pfc/proyecto/proyecto.html.

[19] MORSHED CHOWDHURY, M J. Comparison of e-voting schemes: Estonian and norwegian solutions. *NordSecMob, University of Tartu* (2010). http://courses.cs.ut.ee/2010/security-seminar-fall/uploads/Main/chowdhury-final.pdf.

[20] Normas de organización y funcionamiento de la Universidad San Pablo-CEU. http://servicios.ceu.es/calidad/Portals/0/Dat/Doc/A.1_NORMAS_DE_ORGANIZACI%C3%93N_Y_FUNCIONAMIENTO.pdf.

[21] OCHOA JIMÉNEZ, J. E. Función picadillo determinista al grupo g2 y su aplicación en autenticación para dispositivos móviles. Master's thesis, Centro de Investigacion y de Estudios Avanzados del Instituto Politecnico Nacional. Departamento de Computación, México D.F., México, Diciembre 2013. http://www.cs.cinvestav.mx/TesisGraduados/2013/TesisJoseOchoa.pdf.

[22] PÉREZ BELLEBONI, E. Aplicación de documentos de identificación electrónica a un esquema de voto telemático a escala paneuropea, seguro, auditable y verificable. Master's thesis, Universidad Politécnica de Madrid - Escuela Universitaria de Ingeniería Técnica de Telecomunicación - Departamento de Ingeniería y Arquitecturas Telemáticas, Febrero 2013. http://oa.upm.es/14925/1/EMILIA_PEREZ_BELLEBONI.pdf.

[23] PÉREZ BELLEBONI, EMILIA, AND CARRACEDO GALLARDO, JUSTO. Uso del dnie para reforzar el anonimato en el voto telemático mediante tarjetas inteligentes. *Departamento de Ingeniería y Arquitecturas Telemáticas. Escuela Universitaria de Ingeniería Técnica de Telecomunicación. Universidad Politécnica de Madrid* (2009). http://vototelematico.diatel.upm.es/articulos/Uso_DNiIe_anonimato_voto.pdf.

[24] Indra. procesos electorales. http://www.indracompany.com/sector/procesos-electorales.

[25] PUIGGALÍ, JORDI, CHÓLIZ, JESÚS, AND GUASCH, SANDRA. Best practices in internet voting. *Scytl Secure Electronic Voting* (2010). http://www.scytl.com/wp-content/uploads/2013/05/PUIGGALI_BestPracticesInternetVoting.pdf.

[26] Scytel. http://www.scytl.com/.

[27] VENTURA BONELL-TEROL, M. A. Propuesta de implantación de votación electrónica en las elecciones a rector de la universidad politécnica de valencia. Master's thesis, Universitat Politècnica de València. Facultat d'Administració i Direcció d'Empreses, Octubre 2011. http://riunet.upv.es/bitstream/handle/10251/14584/PROPUESTA%20DE%20IMPLANTACI%C3%93N%20DE%20VOTACI%C3%93N%20ELECTR%C3%93NICA%20EN%20LAS%20ELECCIONES%20A%20RECTOR%20DE%20LA%20UNIVERSIDAD%20PO.pdf?sequence=1.

[28] Voting machines pros and cons. http://votingmachines.procon.org/view.timeline.php?timelineID=000021.

[29] WIIK ØBERG, M. Improving the norwegian internet voting protocol. Master's thesis, Department of Mathematical Sciences, NTNU - Norwegian University of Science and Technology, Junio 2011.