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

24 de septiembre de 2014

# Versión SVN

Rev: **-2**

por

URL : https://pfc-carlosjg.googlecode.com/svn/trunk/doc/memoria/pfc.tex

# 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

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

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*".

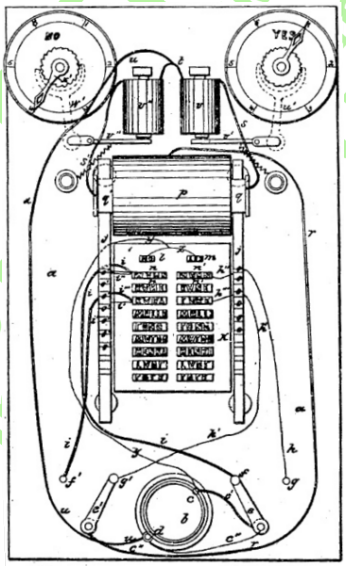

Figura 1.1: *U.S. Patent 0,090,646 – Electrographic Vote-Recorder: Primera patente de Thomas A. Edison. Permitía un voto de tipo 'A favor' o 'En contra' a través de dos interruptores. (1869). Fuente: Wikipedia*

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

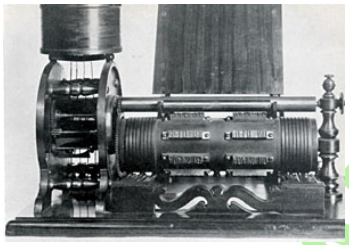

Figura 1.2: *Electrographic Vote-Recorder: Fotografía del invento de Thomas A. Edison. Fuente: Rutgers.edu*

datado en 1964, año en el que site condados de EEUU utilizaron un sistema de voto electrónico para las Elecciones Presidenciales.

## 1.3. Estado de la cuestión

### 1.3.1. Voto electrónico

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 elemenos 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 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, dependidendo 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 miebros 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.

Los sistemas de voto electrónico deberían tener como base antes de la implementación 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* [**?**], un sistema de voto secreto es *seguro* si cumple con los siguientes requisitos:

**Completitud** : Todos los votos válidos son contados de correctamente.

**Solidez** : Un votante deshonesto no puede interrumpir la votación.

**Privacidad** : Todos los votos deben ser secretos.

**Unreusability** : Ningún votante puede votar dos veces.

**Elegibilidad** : Nadie que no tenga permitido el voto puede votar.

**Fairness** : Nada debe afectar la votación.

**Verificabilidad** : Nafie puede falsificar el resultado de la votación.

### 1.3.2. Certificados Digitales

La propia web de la Fábrica Nacional de Moneda y Timbre [**?**] 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*.

para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los certificados digitales.

### 1.3.3. Smart Cards

### 1.3.4. DNIe

### 1.3.5. Tarjeta Universitaria Inteligente - TUI

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 (**??**), 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).

### 1.3.6. 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.

#### 1.3.6.1. 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 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 comnucicación 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 posibilida 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 [**?**], 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 caulquier 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 miecanismos 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 existenetes en el voto tradicional (¿?) **********

#### 1.3.6.2. ¿¿¿¿¿**********Noruega**********????

#### 1.3.6.3. Suiza

#### 1.3.6.4. UNED

#### 1.3.6.5. Votescript

El esquema de votación telemática Votescript tiene su origen en el proyecto de investigación *Votación Electrónica Segura basada en criptografía avanzada* [**?**], 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 [**?**] 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 **??**. 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 equipamentos 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.

******** 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

#### 1.3.6.6. SELES

#### 1.3.6.7. SEVI

### 1.3.7. 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 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.

### 1.3.8. 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 criptogafía es el núcleo de la solución.
Los requerimientos que se tratan de satisfacer con el uso de la criptografía son [**?**]:

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

Antes de entrar en los diferentes esquemas de voto electrónico (**??**), introducimos una serie de primitivas criptográficas que se utilizan en ellos.

#### 1.3.8.1. Firma ciega

#### 1.3.8.2. Secreto compartido

#### 1.3.8.3. Pruebas de conocimiento nulo

#### 1.3.8.4. Mixnets

#### 1.3.8.5. Cifrado homomórfico

### 1.3.9. Esquemas de Voto Electrónico

Según la teoría, 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 mayoría de ellos usan mecanismos y principios criptográficos. Podemos discernir varios tipos de esquemas de voto electrónico entre los más usados según publican diversos expertos en este campo:

- 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 [**?**], 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 **********

********** Según [**?**] ********** 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 [**?**], en la cual se expone una recopilación de información muy concisa sobre multitud de esquemas y sistemas que los implmentan, según las necesidades que se necesiten cubrir.

## 1.4. Descripción del sistema real

### 1.4.1. Elecciones a la Junta de Escuela de la EPS

#### 1.4.1.1. Definición de la Junta de Escuela

Según el documento **NORMAS DE ORGANIZACIÓN Y FUNCIONAMIENTO DE LA UNIVERSIDAD SAN PABLO-CEU** [**?**], 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.

#### 1.4.1.2. Proceso electoral

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

##### 1.4.1.2.1. Plazos

- Convocatoria
- Presentación de candidaturas
- Publicación del censo
- Constitución de la Junta Electoral

- Designación de las mesas electorales

### 1.4.2. Elecciones de delegados y subdelegados de curso en la EPS

## 1.5. Organización de la memoria del PFC

En el Capítulo 1 ...

## 1.6. Metodología

### 1.6.1. Documentación

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

### 1.6.2. Metodología de desarrollo

BDD - Behavior Driven Development

********** Hablar de la evolución en los procesos de desarrollo de software, llegando a TDD. Escribir sobre la diferencia (evolución) de TDD hacia BDD y ATDD (Acceptance Test driven Development). A partir de aquí, comentar un poco sobre BDD. Los motivos por los que se adaptaría bien a este tipo de proyecto (un proyecto en el que debe probarse todo lo posible, por ejemplo) y la forma de introducirlo. **********

# Capítulo 2

# Planteamiento

## 2.1. Objetivos finales del proyecto

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

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

Este 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, que 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 puediera ser escalable hasta un nivel superior al ámbito de la Escuela o la Universidad.

**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 era la búsqueda de soluciones para elecciones generales, autonómicas, municipales, etc. Elecciones que afectan a la población y de los motivos por los cuales todavia 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.

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. Alcance del proyecto

Como se indica en el apartado **??**...

## 2.3. 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 elaboriación 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**

- 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.

### 2.3.1. Fase preelectoral

#### 2.3.1.1. 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. (...)

#### 2.3.1.2. 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 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.

#### 2.3.1.3. Registro de votantes

Pese a que el censo tiene que ser elaborado antes de cada elección, puede ser que la forma que tiene un organismo de conformarlo es a través de un registro de votantes.

Así, en lugar de tener una institución dedicada a definir el censo del país, como en España puede ser el INE, a partir del cual se extrae el censo electoral según el comicio (éste dependerá del tipo de elección y de la circunscipción electoral ******** ¿Ejemplo censo diferente en Buenos Aires para Jefe de Gobierno y para Legislativas? *******); se da el caso de que el Estado no contabiliza automáticamente como votantes a sus ciudadanos al cumplir los 18 años (o la edad mínima para votar, dependiendo del país / territorio), sino que es responsabilidad del propio ciudadano el inscribirse en el registro de votantes. ******* Esto hay que cambiarlo, no vale *********

********** Registro de votantes como mecanismo para la posterior identificación??? Si no podemos usar DNIe, pero se usa una smartcard, habría que realizar el mapeo de la Id del votante con los certificados de la smartcard.... **********

#### 2.3.1.4. Presentación de las candidaturas

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

### 2.3.2. 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.

### 2.3.3. Fase electoral

#### 2.3.3.1. 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 cotejación, 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 metodo de identificación es el mejor

para cumplir con los requisitos de la elección, incluídos 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 estatates 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 poíticos 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 desacnoseja 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 implatación 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 podríamo 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 herramietna 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 indentificación 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).

#### 2.3.3.2. 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 habe 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 implatación 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.

### 2.3.4. Fase postelectoral

## 2.4. 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 desccrifrar o los propios auditores.
No obstante, un exahustivo registro de información acerca del proceso podría suponer 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 descrifrado.

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

## 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 especificación de requisitos 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. Descripción del sistema

**Título:** AQUÍ VA EL TÍTULO **********

**Descripción:** El sistema consiste en una plataforma de voto eléctronico 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. (********** DNI? 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 sistema 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 descrifrados 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.

### 4.1.3. 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.

**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.

### 4.1.4. 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

### 4.1.5. Requisitos del proceso electoral

**Ejemplo** : Aquí va un requisito.

### 4.1.6. Requisitos no funcionales

**Bajo coste** : El coste del sistema debe ser relativamente bajo.

**Soporte a usuarios** : El sistema debe proporcionar unas herramientas de soporte a usuarios de cualquier rol que hagan uso del mismo.

### 4.1.7. Necesidades del esquema de voto electrónico

1. Identificación y autenticación remota
2. ...

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

**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.

**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.

**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) *********

**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.

**Bajo coste** : El coste del sistema debe ser relativamente bajo.

**Soporte a usuarios** : El sistema debe proporcionar unas herramientas de soporte a usuarios de cualquier rol que hagan uso del mismo.

**Voto múltiple:** El sisteme 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 **********)

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

Como primera fase a la hora de analizar un sistema que se pretende desarrollar es necesario la realización de una especificación de los requisitos que se van a exigir al sistema. Estos requisistos son las bases que tendrá que satisfacer el diseño del sistema para la correcta consecución del proyecto.

En el sector de la ingeniería existen muchos protocolos para llevar a cabo una

especificación de requisitos. En este proyecto vamos a basarnos en el estándar IEEE 830-1998. Este documento es el que estandariza la redacción de un documento completo como es una Estandarización de Requisitos de Software de manera formal. Por la tipología de documento que estamos redactando en este PFC, no se requiere de un documento anexo dedicado únicamente a este proceso. Por ello, no vamos a utilizar la totalidad el estándar, sino sólo aquellas partes que podamos integrar en la memoria de forma correcta.
El estándar, en el momento del análisis de este proyecto, cuenta ya con dieciséis años de vigencia (1998), por lo que el formato que vamos a utilizar se basa en su estructura, pero con modificaciones para poder adaptarlo a las necesidades de este PFC.
Algunas de las modificaciones vienen inspiradas en este proyecto [**?**] y en este post al respecto [**?**], 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, usailidad, 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.

**********

## 4.2. 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

- 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
  - Apertura de los canales de difusión de resultados.

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

- 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 puede 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 puede 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).

**** 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

# Capítulo 5

# Solución

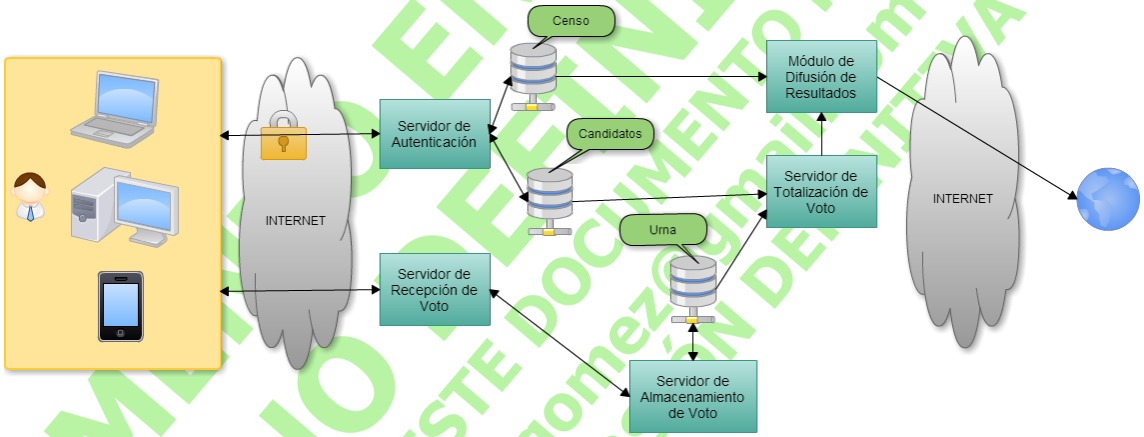


Figura 5.1: *Diagrama de flujo del Sistema*

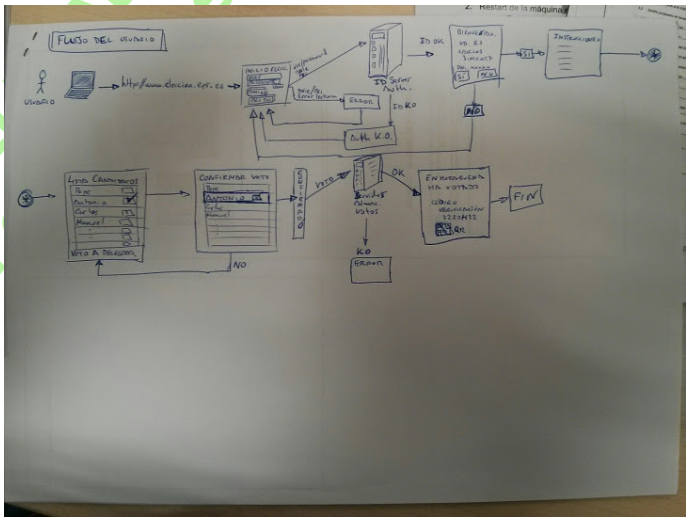

Figura 5.2: *Esquema del flujo que sigue el votante*

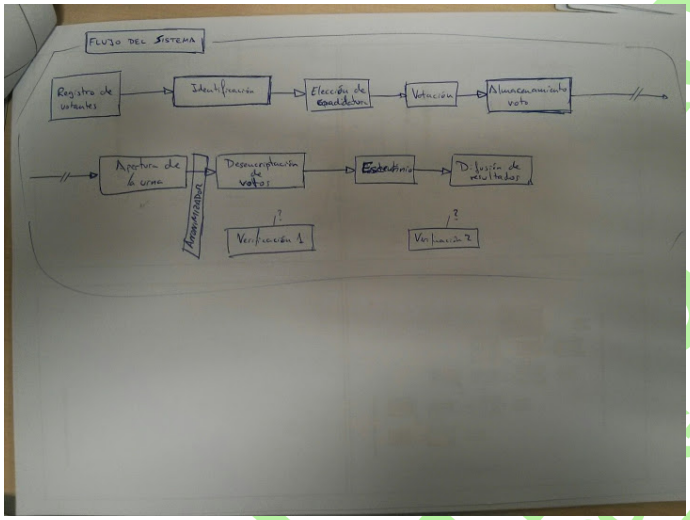


Figura 5.3: *Esquema del flujo del Sistema*

## 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

# Capítulo 6

# Plan de pruebas

# Capítulo 7

# Líneas futuras

# Capítulo 8

# Conclusiones

# Bibliografía


[1] 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.

[2] 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.

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

[4] 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.

[5] 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.

[6] Garcia Mondaray, S. Especificación de requisitos software con IEEE 830-1998, Noviembre 2012.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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