

UNIVERSIDAD SAN PABLO - CEU
ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA EN INFORMÁTICA



PROYECTO FINAL DE CARRERA

**<TÍTULO DEL
PROYECTO FINAL DE CARRERA>**

Autor: **José Carlos Jiménez Gómez**

Director: **Raúl García García**

junio de 2016

Versión GitHub

Revision Branch: master @ 4ad8812 • Release: (2016-06-28) • Head tags: No tags?

Hash 4ad8812

Autor Carlos

Fecha 2016-06-28 03:31:11 +0200

Committer Carlos

Fecha 2016-06-28 03:31:11 +0200

Calificación

Página reservada para la calificación del proyecto

Resumen

Abstract

Abstract in English.

Agradecimientos

Es de bien nacidos ser agradecidos.

Índice general

Calificación	III
Resumen	IV
Abstract	V
Agradecimientos	VI
Índice General	XI
Índice de Figuras	XII
Índice de Tablas	XIII
1. Introducción	14
1.1. Motivación del Proyecto	16
1.2. Antecedentes	16
1.3. Organización de la memoria del PFC	18
1.4. Metodología	19
1.4.1. Documentación	19
1.4.2. Metodología de desarrollo	19
2. Estado de la cuestión	21
2.1. Voto electrónico	21
2.1.1. Niveles	21
2.1.2. *****Dificultad del voto electrónico*****	25
2.1.3. Requisitos del voto electrónico	26
2.2. Experiencias de Voto por Internet	30
2.2.1. Estonia	32
2.2.2. Noruega	35
2.2.3. Suiza	36

2.2.4. UNED	37
2.2.5. Universidad del País Vasco	37
2.2.6. Votescript	37
2.2.7. Online E-Voting Prototype with PTC Web Services	38
2.2.8. SELES	38
2.2.9. SEVI	38
2.2.10. Civitas	39
2.2.11. Online Voting NON IEEE Projects	40
2.3. E2E Auditable Voting Systems	40
2.3.1. ADDER	41
2.3.2. Ágora Ciudadana - Ágora Voting	44
2.3.3. Helios	44
2.4. Voto por Internet en la EPS	46
2.5. Primitivas de criptografía	47
2.5.1. Firma ciega	48
2.5.2. Secreto compartido	48
2.5.3. Pruebas de conocimiento nulo	49
2.5.4. Mixnets	50
2.5.5. Cifrado homomórfico	50
2.5.5.1. ElGamal / ElGamal Exponencial	50
2.6. Esquemas de Voto Electrónico	51
2.6.1. Prueba de conocimiento cero	55
2.7. Estado actual de las tecnologías	55
2.7.1. Certificados Digitales	55
2.7.2. NFC	55
2.7.3. Smart Cards	56
2.7.4. DNIe	56
2.7.5. Tarjeta Universitaria Inteligente - TUI	56
2.7.6. Python	56
2.7.7. Django	56
2.7.8. Android	56
3. Planteamiento	57
3.1. Objetivos finales del proyecto	57
3.2. Descripción del sistema real	59
3.2.1. Elecciones a la Junta de Escuela de la EPS	59
3.2.1.1. Definición de la Junta de Escuela	59
3.2.1.2. Proceso electoral	60

3.2.1.2.1. Plazos	60
3.2.2. Elecciones de delegados y subdelegados de curso en la EPS	61
3.3. Helios Voting	61
3.3.1. Fases de la elección en Helios	62
3.3.2. Auditorías	64
3.3.3. Protocolo criptográfico	66
3.4. Alcance del proyecto	66
3.5. Fases del proceso electoral	66
3.5.1. Fase preelectoral	68
3.5.1.1. Definición de los límites o reglas de la elección	68
3.5.1.2. Elaboración del censo	68
3.5.1.3. Registro de votantes	69
3.5.1.4. Presentación de las candidaturas	70
3.5.1.5. Generación de claves de encriptado	71
3.5.2. Fase electoral	71
3.5.2.1. Identificación del votante	71
3.5.2.2. Votación	75
3.5.3. Fase postelectoral	76
3.6. Logs	76
3.7. ggggggggggggggggggggggggg	78
3.7.1. Diagrama Entidad-Relación	81
3.7.2. Flujo oAuth DNle	83
4. Riesgos	84
4.1. Identificación y gestión de riesgos	84
4.1.1. Identificación de riesgos	84
5. Análisis del sistema	88
5.1. Especificación de requisitos	88
5.1.1. Introducción	88
5.1.2. Ámbito del sistema	89
5.1.3. Restricciones generales	91
5.1.4. Requisitos funcionales	91
5.1.5. Requisitos propios del voto electrónico	92
5.1.6. Requisitos del proceso electoral	93
5.1.7. Requisitos no funcionales	94
5.1.8. Necesidades del esquema de voto electrónico	94
5.1.9. Restricciones de diseño	98

5.1.10. Requisitos funcionales	98
5.1.11. Requisitos de la interfaz	98
5.1.12. Requisitos de calidad	98
5.1.13. Requisitos de evolución	98
5.1.14. Requisitos del proyecto	98
5.1.15. Requisitos de soporte	98
5.2. Roles / Actores	98
5.3. Modelo Conceptual	100
5.4. Modelo de Casos de Uso	101
5.4.1. Actores	101
5.5. Modelo de Comportamiento	101
5.6. Modelo de Interfaz de Usuario	101
5.7. Esquema de Voto Electrónico	101
6. Solución	105
6.1. Diseño	106
6.1.1. Diseño del esquema de votación	106
6.1.1.1. Registro	106
6.1.1.2. Identificación	107
6.1.1.3. Elección de candidatura	108
6.1.1.4. Votación	108
6.1.1.5. Escrutinio	108
6.1.1.6. Difusión de resultados	108
6.1.2. Diseño de la arquitectura	108
6.1.3. Diseño de la capa de datos	108
6.1.4. Diseño de la red	108
6.1.5. Diseño de la interfaz de usuario	108
6.1.5.1. Estructura de la página web	108
6.1.5.2. Estructura de la aplicación móvil	108
6.1.5.3. Colores	108
6.1.5.4. Logo de la elección	108
6.1.5.5. Ergonomía	108
6.1.6. Protocolo	109
6.1.6.1. Descripción del sistema	111
6.2. ESTO ES EL PFC	111
7. Plan de pruebas	118

8. Líneas futuras	119
9. Conclusiones	120
 Bibliografía	 121
 Notas (para borrador)	 125

Índice de figuras

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	17
1.2. Electrographic Vote-Recorder: Fotografía del invento de Thomas A. Edison. Fuente: Rutgers.edu	17
2.1. Tipos de e-Voting [12,39]	22
2.2. Categorización de los sistemas de voto	22
2.3. Primera aproximación de funcionalidad de SEVI	39
2.4. Diagrama de secuencia del procedimiento para una elección con ADDER [24].	42
3.1. Fases de una elección en Helios Voting	63
3.2. Diagrama ER del sistema Helios Voting	81
3.3. Flujo oAuth adaptado para permitir el uso del DNIe	83
5.1. DFD Contexto	101
5.2. DFD 0	102
5.3. DFD 1. Gestionar votante	103
5.4. Caso de uso 1. Votante	104
6.1. Diagrama de flujo del Sistema	105
6.2. Esquema del flujo que sigue el votante	105
6.3. Esquema del flujo del Sistema	106

Índice de tablas

2.1. Evolución del voto por Internet en Estonia	32
2.2. Comparativa de la evaluación de los sistemas de Votos por Internet de Estonia y Noruega conforme al criterio de Seguridad de la Información	35
2.3. Comparativa de la evaluación de los sistemas de Votos por Internet de Estonia y Noruega conforme a los criterios de verificación, auditoría y procedimiento	36
2.4. Resumen de ventajas y desventajas de los esquemas de voto electrónico según Morales Rocha [27] (p. 109)	54

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

1.2. Antecedentes

Breve Historia del voto electrónico

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:

If there is any invention on Earth that we don't want down here, that is it.

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 tecnológicamente y socialmente, logrando herramientas más sofisticadas y seguras en conjunción con un

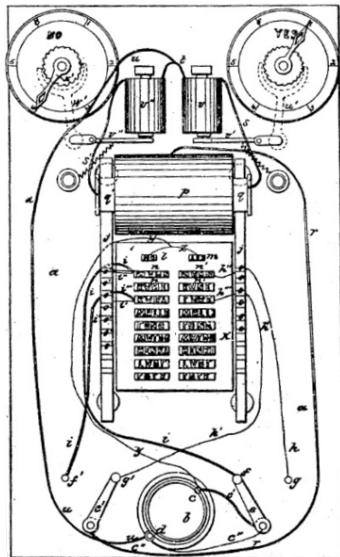


Figura 1.1: U.S. Patent 0,090,646 – *Electrographic Vote-Recorder*: Primera patente de Thomas A. Edison. Permitía un voto de tipo 'A favor' o 'En contra' a través de dos interruptores. (1869).
Fuente: Wikipedia

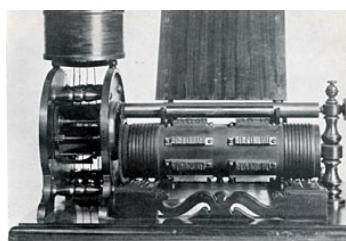


Figura 1.2: *Electrographic Vote-Recorder*: Fotografía del invento de Thomas A. Edison. Fuente: Rutgers.edu

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 los 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 [10] 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 [35] - 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 [37], referente a nivel mundial en proyectos de voto electrónico, tanto presencial como remoto.

1.3. Organización de la memoria del PFC

En el Capítulo 3 ... En el Capítulo 4 ... En el Capítulo 5 ... En el Capítulo 6 ...
En el Capítulo 7 ... En el Capítulo 8 ... En el Capítulo 9 ...

1.4. Metodología

1.4.1. Documentación

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

1.4.2. 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 proyectos. 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

Estado de la cuestión

2.1. 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.

2.1.1. Niveles

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

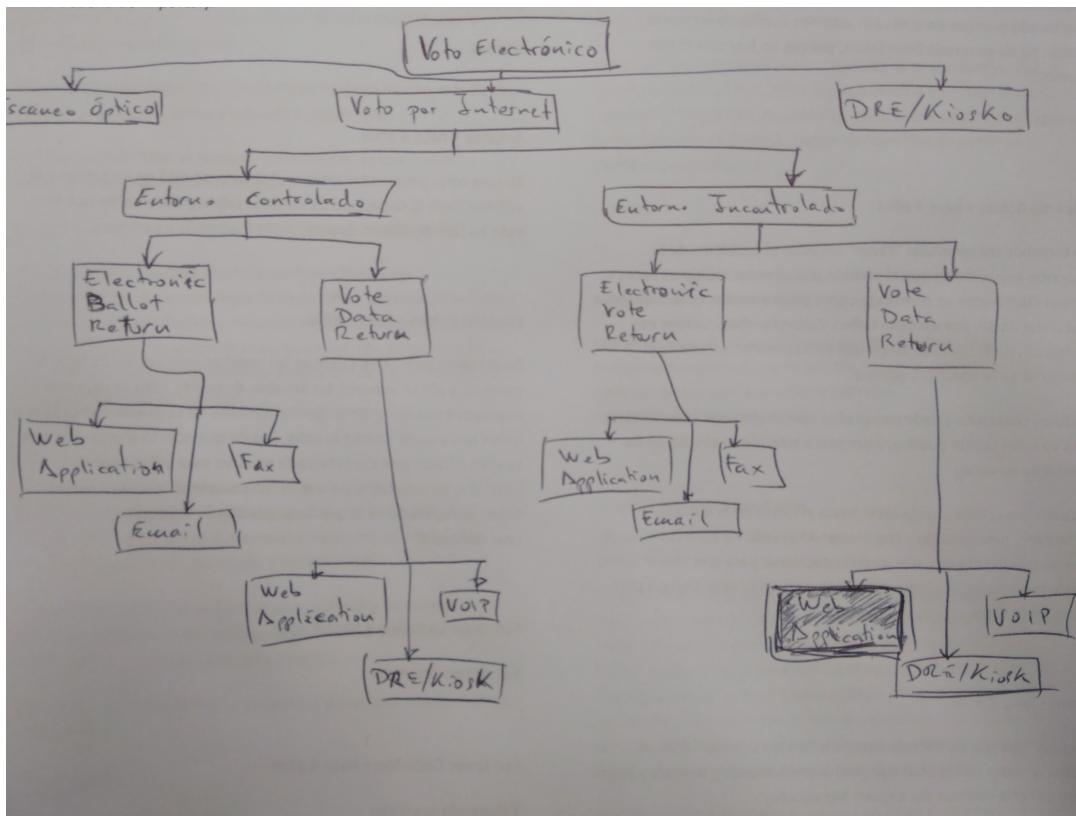


Figura 2.1: Tipos de e-Voting [12, 39]



Figura 2.2: Categorización de los sistemas de voto

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.

2.1.2. ***Dificultad del voto electrónico*******

El voto electrónico es uno de los retos más importantes y complejos del mundo tecnológico hoy en día. Aunque pueda parecer que en otras áreas más modernas hay desarrollos mucho más complejos, el problema del voto electrónico sigue teniendo factores de difícil resolución. Quizá el concepto más complicado para resolver para los desarrolladores de estos protocolos y sistemas es el de la dualidad Verificabilidad-Secreto. Aquí se enfrentan dos requisitos básicos de un sistema de voto electrónico, por un lado, la posibilidad de un elector de verificar que el voto que ha emitido ha sido correctamente incluido en el escrutinio y el derecho fundamental del secreto de voto del propio elector. Para exemplificar y visualizar el problema, introduciremos una serie de actores:

Blanca y Begoña : dos votantes.

Juan : quiere influenciar el voto de Blanca.

Carnívoros y Herbívoros : las dos opciones entre las que los votantes han de elegir en la Elección.

Blanca tiene intención de votar por los Carnívoros, mientras que Begoña desea votar a los Herbívoros. Por su parte, Juan tiene un gran interés en que Blanca vote por los Herbívoros.

Como hemos avanzado, en cualquier proceso electoral hay un conflicto entre la verificabilidad y el secreto. Cualquier votante querría verificar que el proceso de su voto ocurre correctamente, desde su inclusión en la urna hasta el preciso conteo en el escrutinio. De forma particular, Blanca quiere verificar que su voto es apropiadamente escrutado como Carnívoros. No obstante, si Blanca consigue suficiente información del proceso de voto como para poder convencer a Juan de la opción a la que votó, nace la amenaza de la compraventa de votos. En este caso en el que Blanca puede demostrar a Juan su voto, éste podría ofrecer dinero u otros recursos a Blanca a cambio de que su voto sea para los Herbívoros en vez de para los Carnívoros.

De todos modos, de alguna forma, el voto electrónico lo que quiere es que Blanca consiga la información suficiente para verificar personalmente que su voto a Carnívoros ha sido efectivamente emitido y escrutado como Carnívoros, pero que no consiga la información necesaria como para probar a Juan el sentido de su voto.

Si Blanca vota a Carnívoros y Begoña a Herbívoros, ambas deberían tener la seguridad de que sus votos han sido correctamente incluidos en el escrutinio según sus opciones elegidas. Las dos pueden decirle a Juan que han votado a Herbívoros, con lo que Blanca estará mintiendo y Begoña dirá la verdad, pero Juan no notará la diferencia. Quizá al ver Juan que no tiene seguridad para incentivar a Blanca, desista de tratar de comprar su voto y se acabe así con la amenaza.

Hay que arreglar este párrafo.

Voting systems are hard to make trustworthy because they have strong, conflicting security requirements: - Integrity of election results must be assured so that all voters are convinced that votes are counted correctly. Any attempt to corrupt the integrity of an election must be detected and correctly attributed. - Confidentiality of votes must be assured to protect voters' privacy, to prevent selling of votes, and to defend voters from coercion. Integrity is easy to obtain through a public show of hands, but this destroys confidentiality. Confidentiality can be obtained by secret ballots, but this fails to assure integrity. Because of the civic importance of elections, violations of these requirements can have dramatic consequences. https://www.cs.cornell.edu/projects/civitas/papers/clarkson_civitas_tr.pdf

2.1.3. Requisitos del voto electrónico

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* [19], un sistema de voto secreto es seguro si cumple con los siguientes requisitos:

- **Completitud (Completeness)** : Todos los votos válidos son contados 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:

- **Robustez (Robustness)** : El sistema debe ser capaz de tolerar una cierta cantidad de condiciones de fallas, a la vez que debe ser capaz de manejar y responder a estas situaciones.
- **Verificabilidad Universal (Universal Verifiability)** : Cualquier actor debe poder verificar el resultado de las votaciones.
- **Sin recibo (Receipt Freeness)** : El votante no necesita una prueba del voto realizado, debe ser incapaz de probar a un tercero el contenido de su voto
- **Incoercebilidad (Incoercibility)** : El votante no puede ser coercido por un tercero para que vote por una opción en concreto. Se debe asegurar la libertad del voto.
- **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)** : El votante tiene la capacidad de 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 [13] 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 continuación, añaden una serie de propiedades ligadas al voto electrónico:

- **Autenticación** 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 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.

2.2. Experiencias de Voto por Internet

En lo referente al voto electrónico hay muchos proyectos llevados a cabo, tanto desde el mundo empresarial como estatal o universitario.

Muchas de ellas se utilizan hoy en día. Se pueden destacar a niveles estatales todas las elecciones en la que se usan urnas electrónicas o máquinas cuenta-votos, como ocurre en países como Venezuela, Estados Unidos, India y muchos más. Incluso hay otros que tienen como prioridad el estudio de la implantación de este tipo de herramientas para sus procesos electorales, como es el caso

actual de Argentina. Lo mismo ocurre con muchos proyectos surgidos desde ámbitos académicos o empresariales, donde se desarrollan sistemas que permiten el uso de tecnología para la fase de votación. Incluso algunos permiten el volcado de información de los votos de la urna en el sistema de recuento de voto, pero una vez la urna ha sido cerrada, no de forma interactiva con el momento en el que el votante introduce su voto en el Sistema.

No obstante, la naturaleza de este proyecto implica que nos centremos en aquellos procesos que utilizan la variante del voto electrónico consistente en el voto por Internet, siendo éste de transmisión al sistema de recuento en el momento en el que se introduce el voto.

En este sentido, 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 (2.2.1) que, desde el año 2005, proveen de un sistema de voto por Internet a la totalidad del censo que desee hacer uso del sistema.

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 la dirección de UPyD (Unión Progreso y Democracia).

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

Según un estudio de un ente holandés, recogido en []

Hay que citar el documento que hay en <https://www.jbisa.nl/download/?id=17700076&download=1>

, once países han desarrollado pruebas piloto para elecciones a través de voto electrónico por Internet a nivel nacional, aunque cuatro de ellas ya habían abandonado sus proyectos. Los países que quedaban probando de distinta forma soluciones de voto por Internet y que recoge dicho estudio serían Australia, Canadá, Estonia, Francia, India, Noruega y Suiza. Las motivaciones de los países en desarrollar herramientas de votación remota difieren en cada uno de ellos, dependiendo del tipo de votantes al que va dirigido este tipo de votación. Indica como ejemplo el de Francia, motivado por la necesidad de incrementar la participación electoral de los expatriados o el de Estonia, país que ha apostado por un

desarrollo tecnológico en la mayoría de entornos gubernamentales, motivado por incrementar la participación tanto de los votantes ocasionales como de acercar a los que se suelen abstener.

2.2.1. 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 y 2015, este porcentaje superó el 30 % de los sufragistas.

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

Elección	Tipo	IV	% 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 %
2015	Elecciones Parlamentarias	176.491	30,05 %

Tabla 2.1: Evolución del voto por Internet en Estonia

IV: Votantes que votaron a través de Internet.

%tv: % de votantes que votaron a través de Internet sobre el total de votantes.

Hay que marcar que la fuente de estos datos provienen del Tribunal Electoral de Estonia (o como se diga), concretamente de la web <http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics>

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 año 2000 un despliegue técnico importante para la implantación del documento de identidad electrónico, junto con mecanismos de comunicación con la Admi-

nistración 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 coerción, 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 coerción. Otra necesidad importante del sistema es su acceso, que debe ser prácticamente universal, lo cual implica que ha de ser accesible y sencillo de entender para los usuarios, además de que debe funcionar en la mayoría de las plataformas tecnológicas.

Hay una serie de puntos, recogidos en [29], 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 coerción, 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 nivel nacional y vinculante. - Aceptación nacional, con n° 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 un 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.

INTERESANTE – <http://elecciones.smartmatic.com/estonia-y-el-voto-por-internet/>

2.2.2. Noruega

¿Hay que hablar de Noruega?

	SISTEMA DE VOTACIÓN	
	ESTONIA	NORUEGA
Identificación digital de votantes	•••	••
Protección frente a la suplantación de votantes	••	••
Usabilidad de la interfaz de votante	•	•
Seguridad criptográfica de la información intercambiada	•••	•••
Protección frente a ruptura del secreto del voto por una sola entidad	•••	••
Protección frente a ruptura del secreto del voto por colusión entre entidades	•	•
Protección frente a contabilización indebida de votos	••	••
Protección frente a denegación arbitraria de derecho a voto	•••	•••

Tabla 2.2: Comparativa de la evaluación de los sistemas de Votos por Internet de Estonia y Noruega conforme al criterio de Seguridad de la Información

Destacar que estas tablas vienen de una ponencia de Justo Carracedo, presentación en Posibilidades del voto telemático en la democracia digital <http://www.criptored.upm.es/descarga/ConferenciaJustoCarracedoTASSI2014.pdf>

	SISTEMA DE VOTACIÓN	
	ESTONIA	NORUEGA
Identificación robusta de gestores del sistema	•••	•••
Verificación individual de voto	•	•
Verificabilidad de resultados	•	••
Protección frente a la coacción	•	•
Protección del sistema frente a falsas acusaciones	••	••
Capacidad de supervisión de los intervenidores	••	••
Uso de software público	•	•••
Auditabilidad del sistema	••	••

Tabla 2.3: *Comparativa de la evaluación de los sistemas de Votos por Internet de Estonia y Noruega conforme a los criterios de verificación, auditoría y procedimiento*

2.2.3. 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. [5] 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

seguir?...

2.2.4. UNED

Indra

2.2.5. Universidad del País Vasco

(Scytel)

2.2.6. Votescript

El esquema de votación telemática Votescript tiene su origen en el proyecto de investigación *Votación Electrónica Segura basada en criptografía avanzada* [7], 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 [33] 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 (2.2.1). 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 coerción.

2.2.7. 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

Nombre
de la
Universi-
dad!!

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 coerción del votante. Tal y como apuntan en su documentación, la justificación a esta decisión de diseño del esquema se debe a que para

2.2.8. SELES

SELES

2.2.9. SEVI

El Sistema Electrónico de Votación por Internet (SEVI) [25] 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 postal, por lo que debe asegurar, como mínimo, los mismos servicios que ya proporcionaba éste en procesos electorales anteriores.

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

Quitar el
pie que
viene
implí-
cito en
la ima-
gen!!!

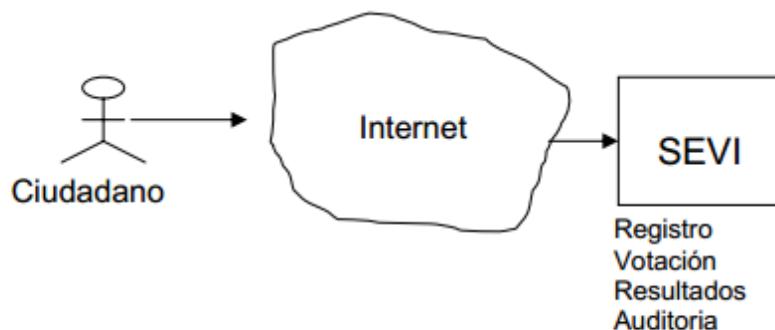


Fig. 4.1 Primera aproximación de funcionalidad de SEVI

Figura 2.3: *Primera aproximación de funcionalidad de SEVI*

- Registro
- Votación
- Resultados
- Auditoría

Al igual que en SELES (2.2.8), 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)

2.2.10. Civitas

<http://www.cs.cornell.edu/projects/civitas/>

Civitas is a new, secure voting system. Civitas is the first voting system implementation that allows voters to vote securely from the remote client of their choice, while provably providing universal verifiability, voter verifiability, anonymity, and coercion resistance. Civitas scales up to a large number of voters, with a low marginal computational cost per voter.

aaaaaa

2.2.11. Online Voting NON IEEE Projects

On-line Voting System is a web based system that facilitates the running of elections and surveys online. This system has been developed to simplify the process of organizing elections and make it convenient for voters to vote remotely from their home computers while taking into consideration security, anonymity and providing auditing capabilities. Users are individuals who interact with the system. All user interaction is performed remotely through the user's web browser. Users are categorized into three classes: Administrator, returning Officers and Voters. A running version of the system will have only one Administrator but it typically has multiple returning officers and voters. The administrator is responsible for managing user accounts, polls, system resources and logs and for the health and safekeeping of the system. Returning officers have the responsibility of managing a poll as assigned by the administrator, whereas voters only have the ability to submit ballots on polls in which they are admitted.

quitar esto, que no va a ir aquí

2.2.12. 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 realizará 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.

2.3. E2E Auditable Voting Systems

Una propiedad bastante útil para el desarrollo de esquemas para votación por Internet es la llamada **verificabilidad punto a punto** (o punta a cabo según otros autores hispanohablantes) (en la literatura inglesa: end-to-end verifiability;

E2E-verifiability). Con ella se puede solucionar el problema de la necesidad de confiar en el proceso que recoge, almacena y cuenta los votos.

Se considera a Josh Benaloh [3] como el precursor del concepto de verificabilidad E2E. Según su propia definición del término, se considera que los requisitos de un sistema completamente verificable E2E son [3, 15, 38]:

En [15] se recoge un resumen sobre sistemas E2E del cual se puede extraer que los sistemas utilizados para las votaciones en Estonia (2.2.1) y en Noruega (2.2.2) son casi completamente E2E verificables.

1. **Verificabilidad individual:** los votantes pueden comprobar que sus votos se han registrado con la opción que han elegido.
2. **Verificabilidad universal:** Cualquiera puede comprobar que todos los votos han sido escrutados con precisión.

Para cumplir el requisito de la verificabilidad individual, el sistema estonio se apoya en una app para smartphones que gestiona la verificación del voto, mientras que en la solución noruega apuestan por una sistema de retorno de código por SMS. A través de ambos protocolos, se permite al votante una herramienta a través de la cual puede asegurarse de que su voto ha sido correctamente incluido en la votación. Los problemas para cumplir con los requisitos de Benaloh aparecen cuando se estudian las herramientas para cumplir con la verificabilidad universal. El método tradicional para garantizar este requisito es utilizar las pruebas de conocimiento zero (2.5.3, 2.6.1). Con estas pruebas se trata de convencer a un verificador de que el proceso se ha llevado a cabo correctamente con una alta probabilidad, sin necesidad de que el verificador tenga conocimiento del contenido de los votos incluidos en la elección. En los sistemas implementados en Estonia y Noruega, aunque parecen tener herramientas que incluyen estas pruebas de conocimiento nulo en todas las etapas del proceso, según algunos informes postelectorales [8], esto no ocurría en la totalidad del proceso. Según estos mismos informes [8], un ejemplo de sistema electoral por Internet E2E-verificable es Helios2.3.3, del que dicen que es un reconocido “estándar en verificabilidad de voto por Internet”. La visión de este sistema es que proporciona al proceso todas las garantías que aporta la verificabilidad E2E, como la capacidad de observar pruebas de conocimiento cero no interactivas que verifican que cada voto fue incluido correctamente y que el escrutinio completo fue computado con precisión. No obstante, hay que remarcar que, como su propio desarrollador indica, Helios es un sistema pensado en elecciones con bajo riesgo de coerción, lo cual no es válido para elecciones nacionales como el modelo estonio o noruego.

Las garantías que ofrecen los esquemas de verificabilidad E2E eliminan la necesidad de los votantes de confiar tanto en los propios clientes (dispositivos, navegadores, sistemas operativos) que utilizan para votar, como los servidores y los trabajadores oficiales que administran los sistemas asociados a la recepción, descifrado y conteo de votos, que son los pilares críticos en los que se basa un sistema de voto por Internet.

Falta decir el porque!! Porqué se olvidan los votantes de la amenaza? pues porque el E2E consigue que se demuestre la invariabilidad del voto emitido frente al contado...E2E

2.3.1. ADDER

ADDER [24] se define como un sistema de voto electrónico basado en Internet, libre y de código abierto. Desarrollado por la Universidad de Connecticut (EEUU) en 2006, supone una plataforma de eVoting completamente funcional con una serie de características de seguridad como robustez, privacidad del voto, auditabilidad y verificabilidad.

Los desarrolladores de ADDER dividen el voto por Internet en 3 escenarios:

Remoto En el escenario del voto por Internet remoto, un actor diferente a la autoridad electoral, ya sea el votante o un tercero, es el que tiene el control sobre el cliente de voto y el entorno operativo.

Kiosko En el escenario del voto por Internet en modo kiosko, el cliente de voto puede ser instalado por las autoridades de la elección, pero entorno de la votación está fuera de su control.

Cabina de voto En este escenario, las autoridades electorales tienen control tanto del cliente de voto como del entorno en el que se lleva a cabo.

ADDER fue diseñado para el primero de los escenarios, el voto telemático remoto, pero dependiendo de los requisitos de seguridad, es adaptable a los otros dos. Además, es un sistema capaz de llevar a cabo elecciones tanto a pequeña como a gran escala.

— System overview — El procedimiento del proceso electoral comienza permitiendo al administrador del mismo alimentar al sistema con la lista de usuarios (votantes y autoridades) y de candidatos. Las autoridades ingresan al sistema y participan en el protocolo de generación de claves criptográficas. Aquí, se genera una clave pública para el sistema y claves privadas únicas para cada una de las autoridades. Cada votante se loguea y descarga la clave pública del sistema, la cual usa para cifrar el voto. Este voto cifrado se guarda en un área de almacenamiento público reservada específicamente para el votante. Cuando el período

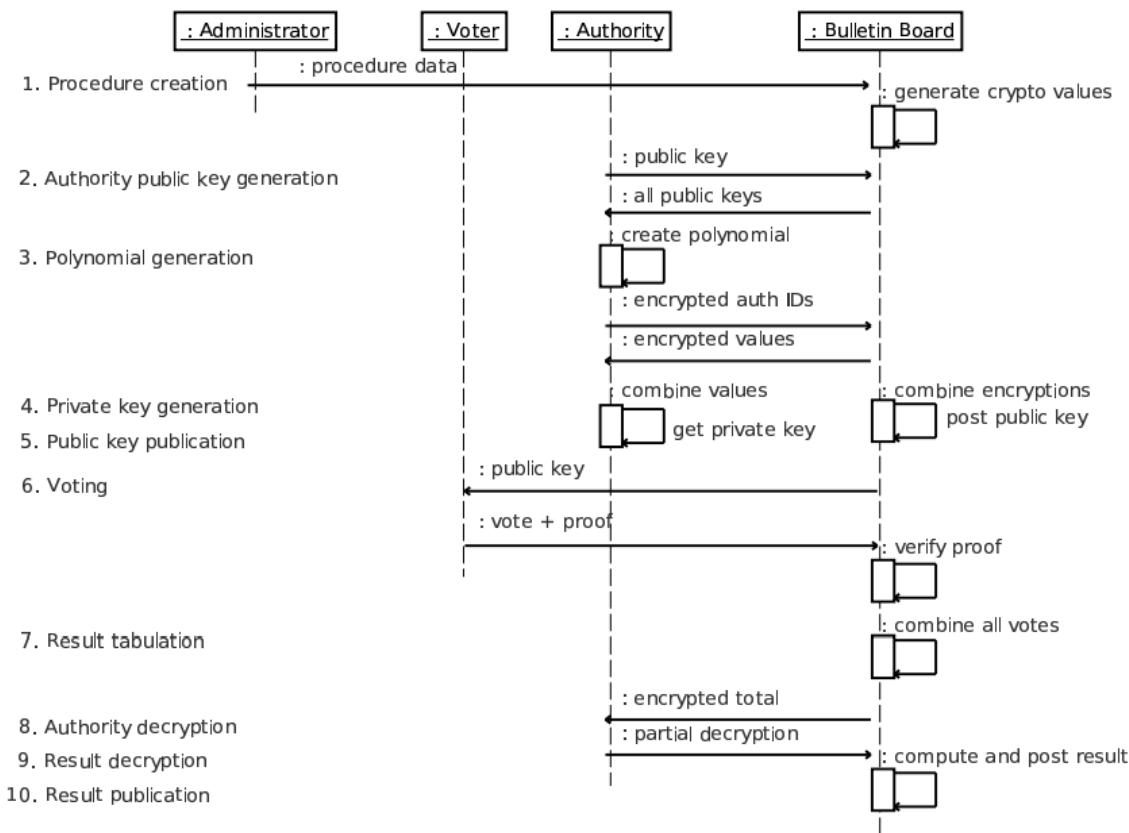


Figura 2.4: Diagrama de secuencia del procedimiento para una elección con ADDER [24].

de votación finaliza, el servidor cuenta los votos y publica el resultado encriptado. A continuación, las autoridades proveen cierta información para decodificar, basada en el resultado encriptado y es sus claves privadas. Cuando se consigue suficiente de esta información, el servidor combina las piezas individuales para componer el resultado electoral, que es publicado. El sistema se implementa con una arquitectura basada en un tablón de anuncios, un servidor de autenticación (*gatekeeper*) y un cliente (puede ser tanto un programa de escritorio como un applet de Java).

Aquí va la imagen de la arquitectura de ADDER.

Los objetivos que persigue el sistema ADDER son:

1. *Transparencia*. Toda la información del tablón de anuncios es pública y puede ser consultada por cualquier observador. Aquí se incluyen votos cifrados, claves públicas y escrutinios.
2. *Verificabilidad universal*- Cualquier resultado electoral obtenido por el sistema debería ser verificado por cualquier observador. A través de los logs y trazas del sistema se puede realizar una auditoría de cualquiera de los

procesos.

3. *Privacidad*. Todos los votantes pueden confiar en que sus votos se mantienen secretos. Sólo el recuento es accesible al público.
4. *Confianza distribuida*. Cada procedimiento del proceso electoral está supervisado por varias autoridades. El recuento no puede llevarse a cabo sin la cooperación de un determinado número de autoridades.

Soluciones propuestas por ADDER:

1. *Autenticación de usuarios*. Para la autenticación de usuarios, ADDER emplea un sistema análogo a Kerberos que denominan *gatekeeper* (guardián de la puerta). (...)
2. *Privacidad del voto*. Para contrarrestar el conflicto entre privacidad del voto y verificabilidad universal y la necesidad de acceso al contenido del voto para asegurar el correcto conteo, el sistema utiliza técnicas de cifrado homomórfico.
3. *Verificabilidad universal*. Para cumplir con este requisito, el sistema se apoya en un tablón de anuncios, en el que se publica información relevante al proceso. Junto al sistema, se han implementado una serie de herramientas libres y de código abierto que permiten hacer uso de los datos publicados en el tablón y realizar una serie de tareas:
 - a) *Recuento de los votos encriptados*. Gracias a las propiedades del cifrado homomórfico, no necesita usar claves privadas para contar los votos, pues no es necesario que los descifre para realizar el recuento. El programa puede repetir el proceso ejecutado en el servidor.
 - b) *Verificación de todas las pruebas*. Cada votante puede comprobar las pruebas de validación de su voto.
 - c) *Descifrado del recuento final*. Una vez que todas las autoridades han terminado sus descifrados parciales, la suite de verificación recalcula los coeficientes de Lagrange y desencripta la suma final.
 - d) *Verificación del hash*.
4. Verificabilidad del votante.

esta
no es-
tá muy
bien ex-
plicado

2.3.2. Ágora Ciudadana - Ágora Voting

2.3.3. Helios

Helios es un sistema de voto por Internet cuyos desarrolladores consideran que es el primer sistema de voto con auditoría abierta (open-audit) basado en web. Actualmente es un proyecto en desarrollo, funcional y públicamente accesible. Cualquier organismo interesado puede descargar el código fuente, configurar un proceso electoral y llevar a término la elección, junto con que cualquier observador puede auditar todo el proceso.

Este proyecto es apropiado para realizar procesos electorales para organismos que necesiten que estos sean confiables y con voto secreto, eso sí, siempre que los comicios se celebren en un ambiente en el que la coerción del voto no sea una amenaza. Este detalle es importante, ya que muestra una de las *debilidades* de esta implementación con respecto a un proceso electoral de gran escala.

Helios trata de ser un sistema de voto por Internet simple comparado con otros protocolos criptográficos, centrándose en la *auditabilidad pública* como elemento diferencial. Con esta propiedad, cualquier organismo puede apoyarse en Helios para llevar a cabo la elección y, aunque resultase que Helios estuviera corrupto, la integridad de la elección puede ser verificada por los observadores.

El protocolo de voto de Helios se basa en la aproximación de emisión de voto de Benaloh y en la mixnet de Sako-Killian. [2]

Ver una descripción de Helios v4 en [38]

Primitivas criptográficas en Helios: <https://securewww.esat.kuleuven.be/cosic/publications/thesis-249.pdf> ElGamal Homomorphic encryption Threshold Encryption (+Secret Sharing)

la siguiente info para analizar está sacada de <https://eprint.iacr.org/2015/942.pdf>

TEMPORAL————— 6 Case Study:
Helios Helios is an open-source, web-based electronic voting system,¹⁸ which has been deployed in the real-world: the International Association of Cryptologic Research (IACR) has used Helios annually since 2010 to elect board members [BVQ10,HBH10],¹⁹ the Catholic University of Louvain used Helios to elect their university president in 2009 [AMPQ09], and Princeton University has used Helios since 2009 to elect student governments [Adi09].²⁰ Informally, Helios can be modelled as an election scheme (Setup, Vote,Tally) such that: Setup generates a key pair for an asymmetric homomorphic encryption scheme, proves correct key generation in zero-knowledge, and outputs the public key coupled with the proof.

Vote enciphers the vote to a ciphertext, proves correct ciphertext construction in zero-knowledge, and outputs the ciphertext coupled with the proof. Tally proceeds as follows. First, any ballots on the bulletin board for which proofs do not hold are discarded. Secondly, the ciphertexts in the remaining ballots are homomorphically combined,²¹ the homomorphic combination is decrypted to reveal the election outcome, and correctness of decryption is proved in zero-knowledge. Finally, the election outcome and proof of correct decryption are output. The original Helios scheme [AMPQ09] is vulnerable to attacks against ballot secrecy [CS13, CS11, SC11]. The current version of Helios is intended to mitigate against these attacks.²² In particular, it incorporates Smyth's recommendation to reject ballots containing zero-knowledge proofs that have been previously observed [Smy12, §4]. For clarity, we write Helios 3.1.4 for the current version of Helios. Bernhard [Ber14, §6.11] and Bernhard et al. [BCG+15a, §D.3] show that variants of Helios 3.1.4 using the strong Fiat-Shamir heuristic satisfy notions of ballot secrecy.²³ These notions assume ballots are recorded-as-cast, i.e., cast ballots are preserved with integrity through the ballot collection process [AN06, §2]. Unfortunately, ballot secrecy is not satisfied without this assumption, because Helios 3.1.4 uses malleable ballots (as do the variants studied by Bernhard [Ber14] and Bernhard et al. [BCG+15a]), which are incompatible with ballot secrecy (§5). Theorem 9. Helios 3.1.4 does not satisfy ballot secrecy. Proof sketch. Suppose an adversary calls the left-right oracle to derive a ballot, exploits malleability to derive a related ballot, and outputs a bulletin board containing the related ballot.²⁴ The board is balanced, because it does not contain the ballot output by the left-right oracle. And the election outcome will allow the adversary to win the game. We omit a formal proof of Theorem 9. The proof sketch of Theorem 9 does not immediately give way to a real-world attack against Helios. Nevertheless, we can derive an attack (as the following example demonstrates) by extrapolating from the proof sketch and Cortier & Smyth's permutation attack, which asserts: given a ballot b for vote v , we can exploit malleability to derive a ballot b' for vote v' [CS13, §3.2.2]. Suppose Alice, Bob and Charlie are voters, and Mallory is an adversary that wants to convince herself that Alice did not vote for a candidate v . Further suppose Alice casts a ballot b_1 for vote v_1 , Bob casts a ballot b_2 , and Charlie casts a ballot b_3 . Moreover, suppose that either Bob or Charlie voted for v . (Thus, we exclude election outcomes without any votes for candidate v , which would permit Mallory to trivially convince herself that Alice did not vote for candidate v .) Let us assume that votes for v_0 are not expected. Mallory proceeds as follows: she intercepts ballot b_1 , exploits malleability to derive a ballot b such that $v = v_1$ implies b is a

vote for v_0 , and casts ballot b . It follows that the tallier will compute the election outcome from bulletin board b, b_2, b_3 . If the outcome does not contain any votes for v_0 , then Mallory is convinced that Alice did not vote for v . This attack also works against the variants of Helios 3.1.4 studied by Bernhard and Bernhard et al., however, neither Bernhard [Ber14, §6.11] nor Bernhard et al. [BCG+15a, §D.3] were able to detect the attack,²⁵ because interception is not possible when ballots are recorded-as-cast.²⁶ Recommendation: adopt non-malleable ballots. We have seen that nonmalleable ballots are necessary for ballot secrecy (§5), hence, future Helios releases should adopt non-malleable ballots. The specification for the next Helios release [Adi14] makes some progress in this direction. Moreover, a liberal interpretation of that specification by Smyth, Frink & Clarkson [SFC15] leads to a variant of Helios, named Helios 4.0, which defines non-malleable ballots [SHM15]. Proving whether Helios 4.0 satisfies ballot secrecy is a direction for future work. And a successful proof would provide strong motivation for future Helios releases being based upon Helios 4.0.

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.

2.4. 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 [27]:

- 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 (2.6), 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 primitivas con el propósito de dotar a una aplicación de características de seguridad. Ej: TLS con

2.4.1. 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 [6]:

2.4.2. 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.

2.4.3. 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. Un sencillo ejemplo 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 [14]. 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 bolsillo 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.

2.4.4. Mixnets

2.4.5. Cifrado homomórfico

Hablamos del cifrado homomórfico

2.4.5.1. ElGamal / ElGamal Exponencial

Uno de los algoritmos más utilizados para realizar un cifrado homomórfico es el de ElGamal. Este algoritmo es un sistema de cifrado homomórfico respecto de la operación multiplicación. Con esto, se obtiene un proceso en el que el producto de dos mensajes cifrados equivale al cifrado del producto de ambos mensajes.

$$\varepsilon(x_1) \cdot \varepsilon(x_2) = \varepsilon(x_1 \cdot x_2)$$

La propiedad de ElGamal en cuanto a homomorfismo es muy interesante, pero de cara al voto por Internet, presenta ciertos problemas. El principal es que la operación en la que se basa es el producto. Sería mucho más útil que el homomorfismo fuera sobre la suma, ya que el escrutinio no es otra cosa que la suma (totalización) de votos.

Así, existe una variante de ElGamal que se denomina ElGamal Exponencial. En esta variante, en lugar de encriptar el mensaje

$$m$$

como en ElGamal tradicional, se cifra

$$g^m$$

- donde g es un generador, normalmente se suele reutilizar el mismo que se utiliza para generar la clave pública -, transformando el sistema en un homomorfismo aditivo, es decir, sobre la operación suma.

$$\varepsilon(g^{x_1}) \cdot \varepsilon(g^{x_2}) = \varepsilon(g^{x_1+x_2})$$

Ahondar un poco en la criptografía, pero sólo la parte que entiendo.

2.5. 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 cumplen.

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

Los esquemas de voto electrónico 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 imple-

mentaciones comerciales de sistemas de elección electrónica basadas en este esquema.

LITERAL

- 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).

LITERAL

- 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 [19], 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 [27]

Según la tesis de Morales Rocha [27], 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:

Según
[27] *****

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

El propio autor de la tesis citada [27], incorpora (en la página 109) un resumen con las ventajas y desventajas que ofrece cada uno de estos esquemas (tabla 2.4).

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.

Estoy diciendo cosas contradictorias. Arreglar.

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 de la citada tesis de Morales Rocha [27], así como el capítulo 4 de la tesis de la Dra. Emilia Pérez Belleboni [33], 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.

Clasificación	Ventajas	Desventajas
Esquemas basados en firma ciega	<ul style="list-style-type: none"> Protegen la privacidad del votante al separar los procesos de autenticación y voto. 	<ul style="list-style-type: none"> La protección del anonimato puede verse afectada si un atacante monitorea el canal de comunicación. Con el conocimiento de la clave privada de la autoridad de autenticación se pueden añadir votos no legítimos.
Esquemas basados en mixnets	<ul style="list-style-type: none"> Protegen la privacidad del votante a través de las permutaciones llevadas a cabo. 	<ul style="list-style-type: none"> Difícil verificación de que los servidores mix han actuado correctamente. En el caso de mixnets de descifrado, el terminal de votación requiere de alta capacidad de cómputo.
Esquemas basados en cifrado homomórfico	<ul style="list-style-type: none"> Protegen la privacidad del votante al no tener que descifrar los votos individualmente para llevar a cabo el escrutinio. 	<ul style="list-style-type: none"> No soportan todo tipo de elecciones. Son susceptibles a ataques en donde votantes deshonestos pueden enviar un mensaje que represente más de un voto para un candidato.
Esquemas basados en papeletas precifradas	<ul style="list-style-type: none"> Protegen la privacidad del votante ya que este envía como voto un código cuya relación con el candidato es desconocida para el servidor de votación. Evitan ataques de código malicioso que trate de alterar o conocer el contenido del voto. El voto puede ser enviado desde un dispositivo con baja capacidad de cómputo. Permiten al votante verificar que su voto se ha recibido correctamente en el servidor de votación. 	<ul style="list-style-type: none"> Posibles alteraciones en las papeletas precifradas sin detección, lo cual ocasionaría que el votante envíe un voto diferente al deseado. Se pueden presentar problemas de logística en la distribución de las papeletas a los votantes. Votantes no pueden verificar que su voto fue incluido en el escrutinio sin arriesgar un ataque de coerción masiva. Poca usabilidad al tener que teclear códigos de votación.

Tabla 2.4: Resumen de ventajas y desventajas de los esquemas de voto electrónico según Morales Rocha [27] (p. 109)

2.5.1. 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.

2.6. Estado actual de las tecnologías

2.6.1. Certificados Digitales

La propia web de la Fábrica Nacional de Moneda y Timbre [9] 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 intervenientes en la comunicación están únicamente 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

2.6.2. NFC

Buena fuente de información en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_RFID.pdf

2.6.3. Smart Cards

Una SmartCard

2.6.4. DNIe

DNIe - Añadir DNIe 3.0

2.6.5. Tarjeta Universitaria Inteligente - TUI

2.6.6. Python

2.6.7. Django

2.6.8. Android

Capítulo 3

Planteamiento

3.1. 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* [30] 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 auditabile**, 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.

- **Verifiable** Se puede verificar que los votos han sido contados y forman parte del resultado del escrutinio.
- **Auditabile** 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, verifiable y auditabile 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.

?¿?¿?
además
de un
coste
ajusta-
do,

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 coerción.

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 ...

SEGUIR CON LOS OBJETIVOS

3.2. Descripción del sistema real

3.2.1. Elecciones a la Junta de Escuela de la EPS

3.2.1.1. Definición de la Junta de Escuela

Según el documento **NORMAS DE ORGANIZACIÓN Y FUNCIONAMIENTO DE LA UNIVERSIDAD SAN PABLO-CEU** [30], 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.

3.2.1.2. Proceso electoral

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

3.2.1.2.1. Plazos

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

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

3.3. Helios Voting

Tras el estudio de varias soluciones ya implementadas y de una solución diseñada desde cero, he decidido usar un sistema ya desarrollado como base para el diseño de la solución que lleve a cabo el proceso electoral en la Escuela.

Los motivos que se han tenido en cuenta para seleccionar un desarrollo de terceros frente a uno propio son los siguientes:

- Para mantener la fiabilidad de un sistema de voto por Internet es fundamental una buena base criptográfica y unos protocolos cimentados en sólidos procesos matemáticos. Este concepto tan crucial he preferido delegarlo en el sistema Helios Voting, diseñado Ben Adida¹, doctor en Ingeniería Informática en Criptografía y Seguridad de la Información por el MIT² (Massachusetts Institute of Technology). Además, el creador del sistema fue asesorado³ directamente por profesionales con muchísima experiencia acreditada en conceptos tales como el voto electrónico y criptografía como pueden ser Lessig, Benaloh⁴ o Rivest⁵, entre otros. Con esta carta de presentación, se observa que el nivel de protocolos criptográficos tiene un amplio sustento académico detrás. Igualmente, existen multitud de artículos en los que se presentan, estudian y discuten los protocolos criptográficos del sistema Helios Voting en sus diferentes versiones. Incluso en muchos de estos artículos se ofrecen alternativas a distintos elementos para aumentar la seguridad del sistema o para introducir alternativas a sistemas de voto pero manteniendo la máxima seguridad para que el sistema siga siendo E2E-verificable.
- Helios es un sistema de voto por Internet basado en desarrollo de código abierto. Está escrito en Python, utilizando Django como framework de desarrollo. Esta filosofía de software libre permite que el código pueda ser reutilizado y modificado para adaptarlo a las necesidades de la Escuela. Además, el lenguaje utilizado es bastante potente y la facilidad de integra-

¹<http://ben.adida.net/>

²<http://mit.edu/>

³<https://vote.heliosvoting.org/about>

⁴<http://research.microsoft.com/~benaloh/>

⁵<http://people.csail.mit.edu/rivest/>

ción con los recursos que provee la Escuela es un punto importante que se ha tenido en cuenta.

- El proyecto Helios Voting está activo. Aunque la frecuencia de actualizaciones en el código o las conversaciones en el grupo de Google del proyecto ha decaído este último año 2015, el proyecto está activo y los desarrolladores implicados. Además, se observa que hay mucha gente interesada en el mismo que realizan forks del código para realizar sus propias modificaciones y/o aportaciones al mismo. Asimismo, proyectos como Ágora Voting nacieron a partir de un fork de Helios Voting, aunque actualmente hayan virado a otros protocolos criptográficos.

No me gusta nada cómo está redactado esto ni me parece que esté en el sitio correcto. Cambiar.

3.3.1. Fases de la elección en Helios

Una elección con el sistema Helios Voting se desarrolla a través de una serie de fases o acciones.

Crear elección El primer paso del protocolo de Helios es la creación de la Elección. Corresponde al administrador logarse en el sistema y crear la elección. Para ello, puede poner el nombre y descripción del Proceso, seleccionar si es una elección al uso o un referéndum, si se usan los nombres de los votantes o pseudónimos, si se presentan los nombres de los candidatos a cada votante en orden aleatorio y si la elección es privada para los votantes registrados o abierta a cualquier votante.

Preparar la elección Antes de abrir el proceso de votación hay que preparar la elección. Para ello hay tres elementos que requieren ser inicializados.

Preguntas Helios funciona a base de preguntas al electorado. Con una elección creada, el primer paso debería ser formular dichas preguntas y sus posibles respuestas, así como si es multiselección o de elección simple.

Censo de votantes Es necesario incluir un censo de votantes o permitir una votación abierta. En el caso del censo, Helios permite hacer cargas de ficheros csv con la información del votante (id, email y nombre). También permite que cualquiera pueda emitir un voto.

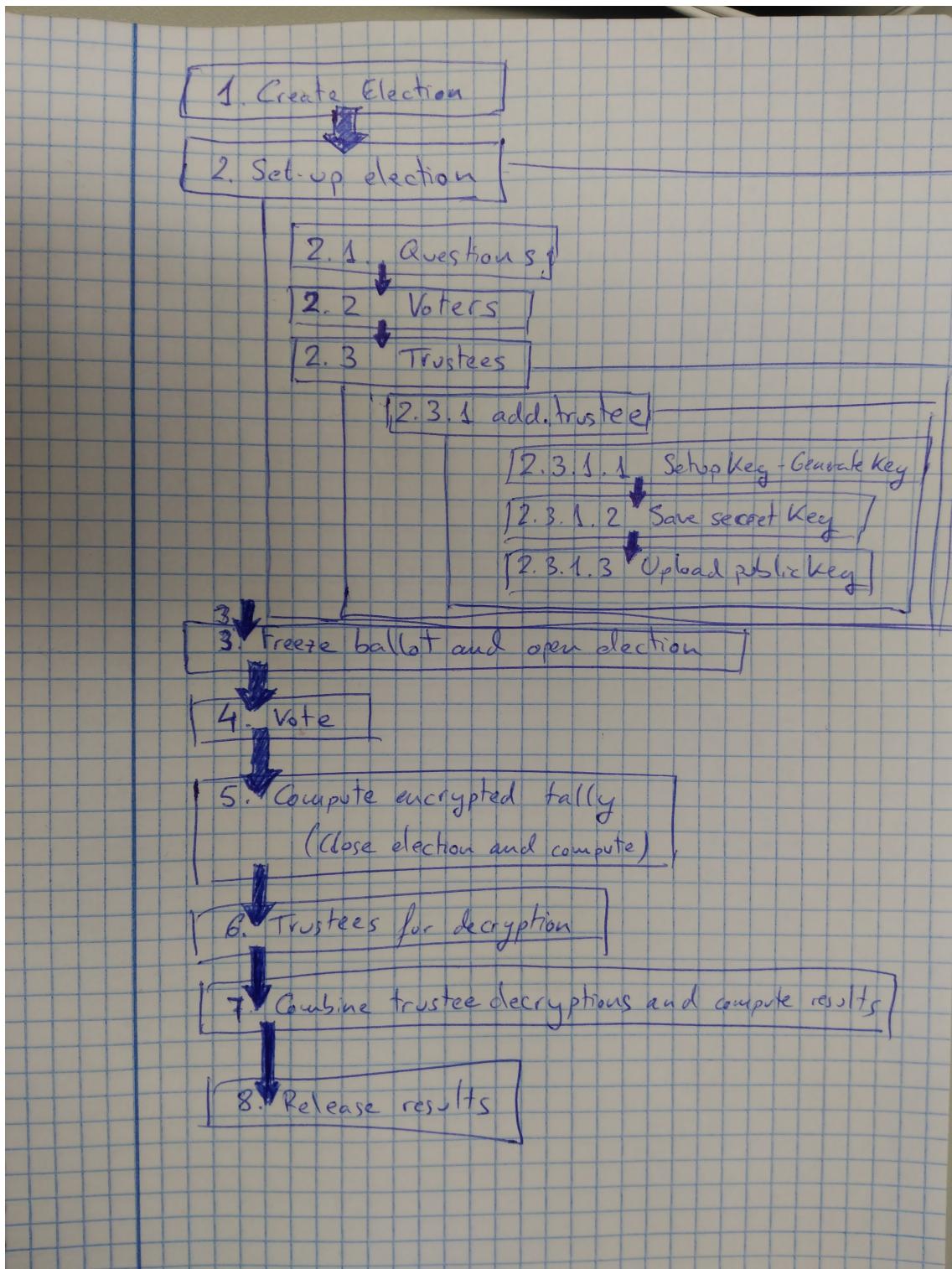


Figura 3.1: Fases de una elección en Helios Voting

Trustees En voto electrónico, es necesario tener entidades de las que poder fiarse para el correcto funcionamiento de la elección. Como es complicado que exista una entidad externa que cumpla con los requisitos, esto se emula utilizando varios trustees. Básicamente, los trustees son entidades fiables que es difícil que se puedan poner de acuerdo entre sí para falsear la elección. Estas entidades combinan sus claves públicas y privadas para formar la clave pública y privada de la elección a utilizar en la encriptación de los votos y la desencriptación del resultado del escrutinio. En Helios, el propio sistema es un trustee, suficiente para llevar a cabo los procesos criptográficos en caso de que no se defina ninguna entidad o usuario confiable adicional.

Setup key - generate key

Save secret key

Upload public key (verify private key)

Congelar papeleta y abrir la elección

Votar

Compute encrypted tally (close election and compute)

Trustees for decryption

Combine trustee decryption and compute results

Difusión de resultados

3.3.2. Auditorías

Las auditorías son procesos fundamentales para la fiabilidad de un sistema de voto por Internet. En este caso vamos a introducir aquellas que, usando pruebas de conocimiento nulo (2.5.3), permiten comprobar el correcto funcionamiento de cada proceso de la elección.

Durante el período de votación, tanto el votante como entidades externas pueden realizar una serie de pruebas o auditorías para confirmar el correcto estado del proceso. Estas auditorías se realizan a distintos niveles dependiendo del actor que deseé realizarlas, así los votantes pueden realizar auditorías de correctitud de su voto emitido, mientras que auditores externos no pueden llevar a cabo estas comprobaciones. Sin embargo, tanto los primeros como los segundos pueden realizar una auditoría al escrutinio.

La interfaz de usuario de Helios posee una zona dedicada a las pruebas de auditoría. En ellas, según se va avanzando en la Elección, van apareciendo enlaces e instrucciones según se pueden comenzar a realizar pruebas a diferentes elementos del sistema.

Las auditorías de procesos que permite Helios Voting durante el proceso de votación:

Verificación de la papeleta (antes de votar) El sistema permite verificar una papeleta cifrada previamente a su sufragio. La papeleta verificada no será la que se utilice para votar y no será, por tanto, contada sino que, por medidas para combatir la coerción, habrá que volver a encriptarla de nuevo cuando se quiera emitir el voto. Una vez el votante está en la cabina de voto virtual y ha encriptado sus opciones de voto, el sistema permite realizar una verificación para asegurarse de que la encriptación de estas ha sido correcta. Para ello, el sistema presenta al votante la información para auditar su papeleta (ballot audit info). Este texto es el que debe copiar el votante para utilizar en la herramienta de verificación de papeletas. En ésta, se incluye dicho texto y la URL de la elección datos suficientes para realizar la verificación.

Poner aquí qué significa esta información

Explicar en qué consiste la verificación

Una vez hemos auditado nuestro voto, tenemos la posibilidad de publicar la papeleta auditada en el *Helios tracking center*, permitiendo a otras entidades realizar una doble comprobación de la verificación de la papeleta.

Lista de papeletas auditadas Como hemos avanzado en el punto anterior, en el momento de realizar la votación, el votante puede realizar una verificación del contenido encriptado de su papeleta. El sistema le permite, una vez realizada la comprobación, publicar esta *papeleta abierta* en un tablón con una lista de papeletas auditadas. En cualquier momento de la elección, cualquier usuario, sea votante o no, puede acceder a esta lista y realizar la misma verificación sobre las papeletas ahí publicadas. Estas papeletas, no obstante, no son las que se han utilizado para emitir el voto, pues ya se ha comentado que una vez el votante la *abre* para su verificación, ha de reencriptar su voto para *meterlo en la urna* definitivamente.

Auditoría del escrutinio Una vez se ha realizado el escrutinio, el sistema permite a los observadores interesados, realizar una prueba para verificar la veracidad del resultado.

Es necesario comentar en qué consiste la auditoría del tally.

3.3.3. Protocolo criptográfico

Otra de las piedras angulares en las que se debe basar un sistema de votación por Internet es en su protocolo criptográfico y en las primitivas que utiliza, base para poder argumentar la fiabilidad de los procesos que se realizan.

Helios Voting basa su seguridad criptográfica en un protocolo de cifrado homomórfico (2.5.5).

El voto se encripta en el navegador del cliente utilizando una implementación del algoritmo de ElGamal Exponencial realizada en Javascript. Como se ha explicado en 2.5.5.1

3.4. Alcance del proyecto

Como se indica en el apartado 3.1...

Alcance del proyecto

3.5. Fases del proceso electoral

El Consejo Europeo, dentro de si definición de estándares, recomienda la aceptación para utilizar el *Election Markup Language* (EML). Desarrollado por la *Organization for the Advancement of Structured Information Standards* (OASIS), su objetivo es el de permitir el "intercambio de información entre hardware, software y proveedores de servicios implicados en cualquier aspecto relacionado con el desarrollo de elecciones o servicios a votantes tanto para organizaciones públicas como privadas." [12] Según el estándar EML, se distinguen cuatro actores implicados y tres fases en el proceso electoral.

Actores

- Autoridad
- Administrador
- Votante
- Auditor/observador

Fases

- Fase Pre-Voting

- Fase Voting
- Fase Post-Voting

(...)

Teniendo en cuenta el EML, identificamos las tres fases que dirigen el proceso electoral como fases preelectoral, electoral y postelectoral, adecuándolas al idioma español. Cada una de estas fases contiene una serie de procesos o tareas determinadas.

- 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.

3.5.1. Fase preelectoral

3.5.1.1. 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. (...)

3.5.1.2. 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 SUBDELEGADOS 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.

3.5.1.3. 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 única 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.

3.5.1.4. Presentación de las candidaturas

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

...

3.5.1.5. 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.

3.5.2. Fase electoral

3.5.2.1. 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 que 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, quizás no para el voto 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. Ciento es que podríamos hacer uso de la banda MRZ del documento escaneándola pero...
...

no estoy
seguro,
qué pa-
sa con
fotoco-
pias??,
yo me
fiaría de
los certi-
ficados

A partir de enero de 2015, el Ministerio del Interior de España, a través de la Dirección General de la Policía, ya está proporcionando a los ciudadanos una nueva versión del DNIE, la cual, entre varios avances, posee, junto al chip electrónico, otro chip de radiofrecuencia basado en tecnología NFC.

Sin entrar en los posibles problemas de seguridad que implica el uso de chips de radiofrecuencia, se observa interesante este avance en cuanto a una aplicación de voto por Internet. Hoy en día son muchos los dispositivos móviles (smartphones y tablets) que disponen de un lector de chips por NFC, con lo que el inconveniente de necesitar lectores externos para identificación del votante y firma digital del voto ya no existiría. El votante podría votar desde una app instalada en su smartphone sin necesidad de elementos externos, ya que este chip NFC contiene los mismos certificados que el chip por contacto que existía hasta ahora en la primera versión del DNIE.

Explicar un poco más el nuevo DNIE, ventajas e inconvenientes para el voto por Internet, así como un poco su funcionamiento con los cambios respecto al DNIE 1.0 —— aunque todo esto va en Estado de la cuestión

- 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 única entre el usuario-votante y su registro en el censo electoral.

hay que mirar bien esto del MobID, 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 DNle. 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.

3.5.2.2. 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

Lo que pasa es que me temo que estas tarjetas no tienen certificados, con lo que tampoco van a valer para la votación

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.

3.5.3. Fase postelectoral

3.6. 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 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 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.

3.7. ggggggggggggggggggggggggggg

Tras el estudio de cómo debe ser un sistema de voto por Internet, aparecen cuestiones importantes como puede ser el esquema criptográfico a utilizar, el flujo de procesos, actores intervenientes, fases, problemas asociados al voto electrónico, seguridad, confiabilidad, etc.

Teniendo en cuenta estos problemas, se ha valorado el uso de un sistema desarrollado desde cero, adecuado a las necesidades de la Elección de la Junta de Escuela que se quiere realizar. Frente a este escenario, otra opción es la de basarse en alguna herramienta existente y, si es necesario, realizar una adaptación de la misma para cuadrar con los requisitos de este proceso electoral.

El hecho de que este tipo de sistemas deban tener una base criptográfica muy importante es uno de los motivos principales para optar por la adaptación de alguna solución ya existente en lugar del desarrollo. En el estudio de soluciones en el mercado encontramos que, aunque no existen realmente muchas opciones libres que reutilizar, sí que existe un verdadero estudio teórico del problema del voto digital. Entre las opciones que han decidido desarrollar las propuestas teóricas hay algunos que merece tener en cuenta, como son Helios Voting, Agora Voting, Adder, el sistema electoral de Estonia, junto con otras opciones que no son E2E verificables o no tratan el voto remoto por completo, como pueden ser Votescript, Punch&Vote, ... ¡¡etc!!.

De entre todas estas opciones, las más atractivas para el tipo de elecciones que se quieren desarrollar en este proyecto resultan ser las propuestas por Ágora Voting previamente a la versión actual, aquella que comenzó a partir de un fork de Helios Voting, la otra opción que parece realmente interesante.

Helios Voting es un sistema de voto E2E verificable, basado en un esquema criptográfico homomórfico, utilizando pruebas de conocimiento nulo para verificar tanto el voto individual de cada votante como el correcto conteo de la elección. En el sistema hemos visto que no es necesario desencriptar los votos para realizar el escrutinio, sino que se realiza con los votos encriptados y, posteriormente, lo que se descifra es el cifrado del resultado del mismo. El desarrollador de Helios Voting se ha apoyado en gente bastante reputada en el campo de la seguridad informática, la criptografía y el voto digital por lo que el apartado criptográfico

Rellenar
este etc.

del sistema está suficientemente probado y documentado que cumple con los requisitos del voto electrónico.

Aunque el peso de la criptografía la estamos delegando en el sistema elegido, en este se observan una serie de elementos que no se ajustan a la primera idea sobre el sistema desde cero.

El esquema criptográfico utilizado por Helios es homomórfico. En una primera versión apostábamos por un esquema basado en mixnets, análogo al utilizado en el desarrollo del sistema estonio. El uso de una mixnet resultaba bastante interesante al pensar en la identificación del votante con un soporte que posee certificados digitales, como el DNIE, que permitiría identificar al votante y que este pudiese firmar su voto. Así, utilizando un protocolo de firma ciega, podría asegurarse la identificación unívoca del votante, su elegibilidad para votar y si ya ha ejercido su voto con anterioridad. A partir del momento en el que se cierra la votación y comienza el escrutinio, sería muy importante desacoplar el dato del votante del voto emitido, momento en el que entra en juego el esquema de mixnets, ideal para llevar a cabo este proceso de desacoplamiento votante-voto.

Aunque en la primera versión de Helios el esquema utilizado fue el de mixnets, a partir de la siguiente versión se cambió al homomorfismo. El futuro a partir de la versión 3 era implementar ambas soluciones en el sistema, pero al final se decidió no continuar con la integración de la mixnet.

El sistema de identificación actual de Helios es el de usuario/contraseña o el uso de protocolos OAuth contra entidades externas, como Google, Facebook, Yahoo! o Twitter. En el caso de las Elecciones a la Junta de Escuela, parece muy interesante la introducción de los certificados digitales, aprovechando el esfuerzo de la Administración al desarrollar una nueva versión del DNI electrónico, con chips sin contacto NFC, lo que puede suponer una oportunidad para el uso de certificados digitales desde dispositivos móviles. No obstante, eliminando el elemento innovador del nuevo chip del DNIE, observando casos de éxito del sistema Helios en elecciones reales, los organismos en los que se ha utilizado han desarrollado sus propios módulos de identificación de votantes. En concreto, en las elecciones de la Universidad de Louvain, se desarrolló el subsistema de identificación para que fuese compatible con las credenciales que los alumnos utilizaban para acceder a los servicios de la propia Universidad.

Por tanto, para las Elecciones de la EPS, sería una buena solución el desacoplar el módulo de identificación de votante y desarrollar uno nuevo que se comunique con la base de datos del censo de la Universidad. Para esto, se puede implementar, como en las elecciones de la Universidad de Louvain, un servicio

de usuario/password y continuar con el sistema Helios existente. También se podría desarrollar un servicio de autenticación OAuth siendo la propia Universidad la que proporciona los tokens. Pero, como se ha avanzado, se va a implementar un sistema de autenticación basado en las credenciales proporcionadas por el DNIe.

Un primer cambio importante que se propone para el sistema Helios es que la gestión del censo electoral pueda externalizarse. Actualmente, el sistema guarda en su propia base de datos la lista de votantes que pueden votar. De hecho, por el carácter general del sistema, esto es así para que el administrador de la elección pueda cargar el censo de votantes a través de ficheros csv, separados por comas. Para el cometido del proyecto, sería necesario modificar este sistema censal.

Modificaciones sobre Helios:

- Capar el sistema para que no permita el voto a cualquier votante, sino solamente a aquellos votantes que aparezcan en el censo.
- Externalizar el listado de votantes para que no lo gestione Helios, sino el organizador de la Elección.
- Cambiar los métodos de autenticación para que el permitido sea el DNIe.
- ~~Modificar la cabina de votación virtual para poder firmar el voto con el certificado digital del DNIe.~~
- ~~Adaptar el almacenamiento del voto mientras la elección está abierta a que éste esté firmado digitalmente por el votante.~~
- ~~Modificar el proceso de escrutinio. Una vez cerrada la votación y abierta la urna, los votos han de ser separados de la firma digital de sus votantes. Esta firma se utilizará para establecer la participación sobre el censo.~~
- ~~Adaptar el proceso de la votación y el escrutinio a la existencia de múltiples mesas electorales, imitando el concepto de mesas, colegios y circunscripciones de las elecciones a mayor escala. En las Elecciones a Junta de Escuela, teniendo en cuenta las características del votante, el censo es diferente y las papeletas también deben serlo, ya que se elige entre diferentes candidatos.~~
- Modificar la interfaz web del sistema para adecuarla a las Elecciones a la Junta de Escuela de la EPS.

Introducir la firma del voto con el DNIE no introduce ningún tipo de mejora en la seguridad respecto del que provee de por sí la propia herramienta Helios Voting. Así que no lo vamos a hacer. Hay que cambiar las modificaciones sobre la misma.

Tareas: 1. Implementación de un módulo de autenticación basado en el DNIE para Django. El nombre que tendrá será dnie.py.

3.7.1. Diagrama Entidad-Relación

A continuación se muestra el diagrama entidad-relación del sistema Helios Voting real.⁶

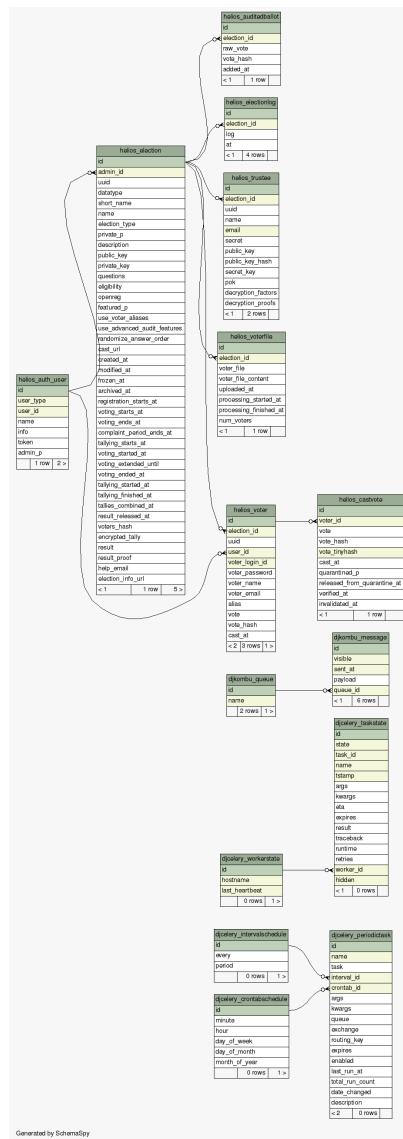


Figura 3.2: Diagrama ER del sistema Helios Voting

⁶Generado automáticamente con la herramienta, SchemaSpy (<http://schemaspy.sourceforge.net/>), que permite obtener el diagrama directamente de una base de datos PostgreSQL ya existente.

En el esquema se distinguen 3 clases de entidades:

- Las propias del core de Helios, cuyos nombres comienzan por *helios_*.
- Las entidades que utilizan la herramienta Celery (las que comienzan por *djcelery_*).
- Las entidades que utiliza la herramienta Kombu (las que comienzan por *djkombu_*).

Con respecto al primer grupo, las que forman la capa de negocio del sistema Helios, se observa un diseño bastante simple, aunque adecuado para las necesidades del sistema:

helios_election Es la tabla que almacena las diferentes elecciones que crean los administradores.

helios_auditedballot En esta tabla se almacenan los votos que los votantes deciden verificar y publicar en el tablón para que puedan ser posteriormente auditados.

helios_electionlog Esta entidad registra los eventos que suceden en torno a una elección, ya sea su creación, congelamiento de la papeleta, apertura de la urna, escrutinio, etc.

helios_trustee Es la entidad que recoge la información de los usuarios que actúan como trustees de la elección. Entre la información de estos que se registra se incluyen las claves públicas que se almacena automáticamente al dar de alta a un trustee. También la clave secreta, que el trustee habrá de subir al servidor una vez se requiera para poder realizar el escrutinio.

helios_voterfile Esta entidad almacena los ficheros de votantes que el administrador sube al servidor desde la interfaz web del sistema. Desde estos ficheros se carga el listado de votantes.

helios_user En esta tabla se almacenan los usuarios / votantes del sistema, relacionados cada uno con las elecciones a las que tienen derecho a voto.

helios_auth_user Para cada elección, esta tabla asocia usuarios del sistema (con derecho a voto o sin él) con las capacidades de administración.

3.7.2. Flujo oAuth DNle

Para utilizar el DNle como herramienta de identificación de votantes se ha implementado una variación del protocolo oAuth de 3 patas (3-legged oAuth).

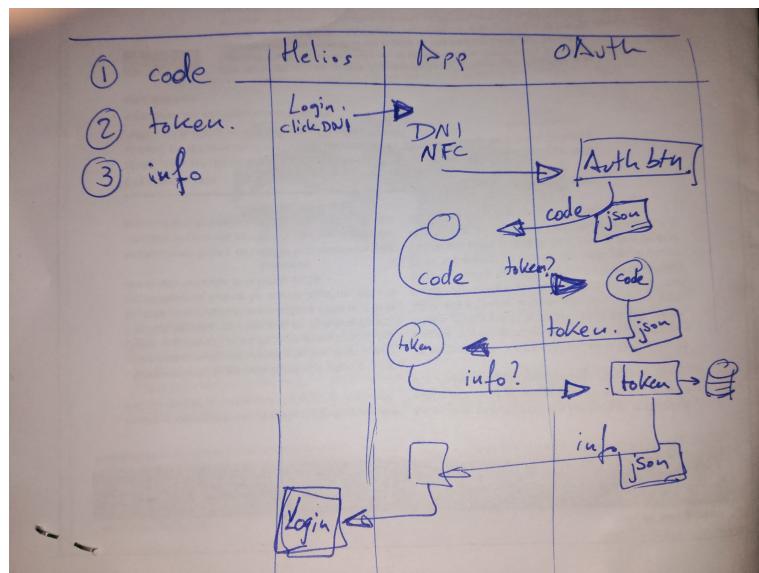


Figura 3.3: Flujo oAuth adaptado para permitir el uso del DNle

Hay que explicar el flujo que se ha implementado para el oAuth. Ver en el código.

Capítulo 4

Riesgos

4.1. 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-)

4.1.1. 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.
- **Coerción 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 of Service - Denegación de Servicio*)

vicio). 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.

- **ddd******* 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.
- **Fecha límite** Un problema de este proyecto es el tiempo. No se trata de un desarrollo evolutivo en el cual se pueden ir desarrollando versiones que, una vez puestas en producción, pueden ser actualizadas para corregir errores o añadir funcionalidades. En este caso, el sistema tiene un barrera temporal claramente definida y que, en ningún caso, puede ser traspasada. El proceso electoral tiene unos tiempos establecidos a base de hitos predefinidos. A pesar de la existencia de hitos en la fase preelectoral, la importancia del sistema radica en que el día (o durante el período definido) de la Jornada Electoral debe estar en producción, totalmente funcional y lo más depurado posible para evitar prácticamente todos los fallos que puedan ser estimados. Por tanto, la variable temporal de este proyecto conlleva un riesgo extremadamente importante, ya que no tenerlo en cuenta y no cumplir los plazos establecidos conduce a la inutilidad del sistema y, por tanto, al fracaso del proyecto.
hay que encontrar una mejor palabra
- **Errores en software** Puede parecer una obviedad, pero los errores de software para este sistema pueden resultar catastróficos. Dependiendo del tipo de aplicación, un error software puede ser más o menos grave, más o menos subsanable. En muchos casos puede suponer una pérdida económica y en otros, incluso, poner en peligro vidas humanas. En el caso de este proyecto, lo que puede suponer es un conteo incorrecto o la imposibilidad de realizar un escrutinio. Por ejemplo, en los sistemas que se utilizan para realizar el escrutinio provisional de las elecciones legislativas territoriales en España, estos se basan en un conteo manual de las papeletas sufragadas, una comunicación digital de los datos contados en cada mesa y, a continuación, el escrutinio de estos datos. En caso de caerse el sistema y ser imposible realizar el escrutinio provisional, aún siendo un fracaso del proyecto, puede recuperarse la información, que está en las actas físicas

de cada mesa, para realizar el escrutinio definitivo de forma manual, por lo que la caída del sistema no afecta a la elección como para que no pueda ser llevada a cabo. Dependiendo del sistema que se quiera desarrollar para el proyecto del voto en la EPS, si no se usa ningún tipo de urna, pues el voto sería completamente digital, puede ocurrir que, en caso de caída del sistema o de fallo general, sin posibilidad de recuperación de la contingencia, sea imposible realizar un escrutinio manual alternativo. Aquí es donde se puede valorar el uso de otros sistemas y la conveniencia de realizar un voto por Internet *puro*, ya que el riesgo que conlleva en cuanto a la falla grave del sistema es bastante importante y puede llevar al fracaso de la elección o a que tenga que ser repetida.

Este párrafo está improvisado, habría que darle una vuelta.

- **Caída del sistema** .-.....

Capítulo 5

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.

5.1. Especificación de requisitos

5.1.1. 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** : *****

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

5.1.2. 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 únicamente en el sistema, sin suplantaciones. (***** DNle? 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 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 la 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.

5.1.3. Restricciones generales

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

Restricciones

5.1.4. 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.
(Analizando este requisito, la mejor forma es habilitar 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.

(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.

Esto de
sin po-
sibilidad
de error
ni me
gusta ni
queda
correcto

5.1.5. 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 2.1.3, 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 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 coerción** : 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 coerción al votante por medio de éste.

NO ESTOY DE ACUERDO CON ESTO. ALGUNOS AUTORES INDICAN LO CONTRARIO, QUE ES PRIMORDIAL QUE EL VOTANTE SE QUEDA 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 COERCIÓN, ¿O SÍ?

- **Possibilidad 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.

5.1.6. Requisitos del proceso electoral

- **Ejemplo** : Aquí va un requisito.

5.1.7. 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 un 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.

5.1.8. 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.

ESTE
NO
CREO
QUE
DEBA
IR, YA
QUE
ES UN
RESU-
MEN DE
LOS SI-
GUIEN-
TES

- **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.

(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 COERCIÓN 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 [23], 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 [28] y en este post al respecto [21], 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 ren-

dimiento, 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.

- 5.1.9. Restricciones de diseño**
- 5.1.10. Requisitos funcionales**
- 5.1.11. Requisitos de la interfaz**
- 5.1.12. Requisitos de calidad**
- 5.1.13. Requisitos de evolución**
- 5.1.14. Requisitos del proyecto**
- 5.1.15. 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

5.2. 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 únicamente 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.

- Auditar el correcto escrutinio de la elección.

- **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.
- Designar los trustees de la elección.

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**

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.

CAMBIAR
EL
NOM-
BRE de
miembro
de la
Junta
Electoral

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.

Teniendo en cuenta la organización de Helios, los miembros de la Junta Electoral que tenemos aquí son los trustees del sistema original de Adida.

- **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). Al hacer uso del DNle para la identificación y firma del votante, en estas fases, es la Dirección General de la Policía, dependiente del Ministerio del Interior, la que actúa como Autoridad de Certificación, combinando dos pares de claves con un ciudadano concreto a través de la emisión de sendos Certificados de conformidad con los términos de la Declaración de Prácticas y Políticas de Certificación (DPC) [16] [17] que rige el funcionamiento y operaciones de la Infraestructura de Clave Pública de los Certificados de identidad pública y firma electrónica del Documento Nacional de Identidad (DNle).

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 personas 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 e 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.

PLANTILLA PARA PROYECTO DE FIN DE GRADO (Universidad de Cádiz) Propuesta de REDiris

5.3. 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.

5.4. 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.

5.4.1. 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).

5.5. 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.

5.6. 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.

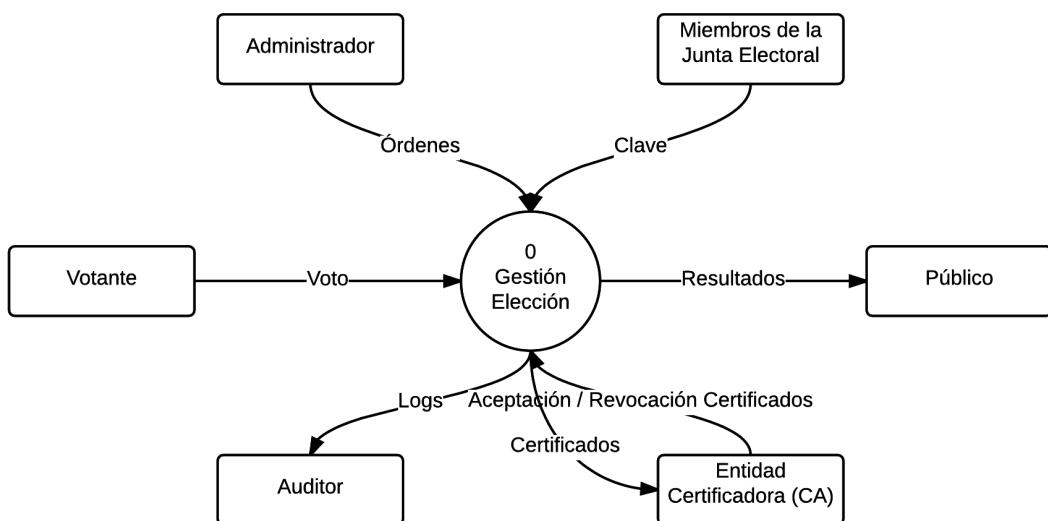


Figura 5.1: DFD Contexto

5.7. Esquema de Voto Electrónico

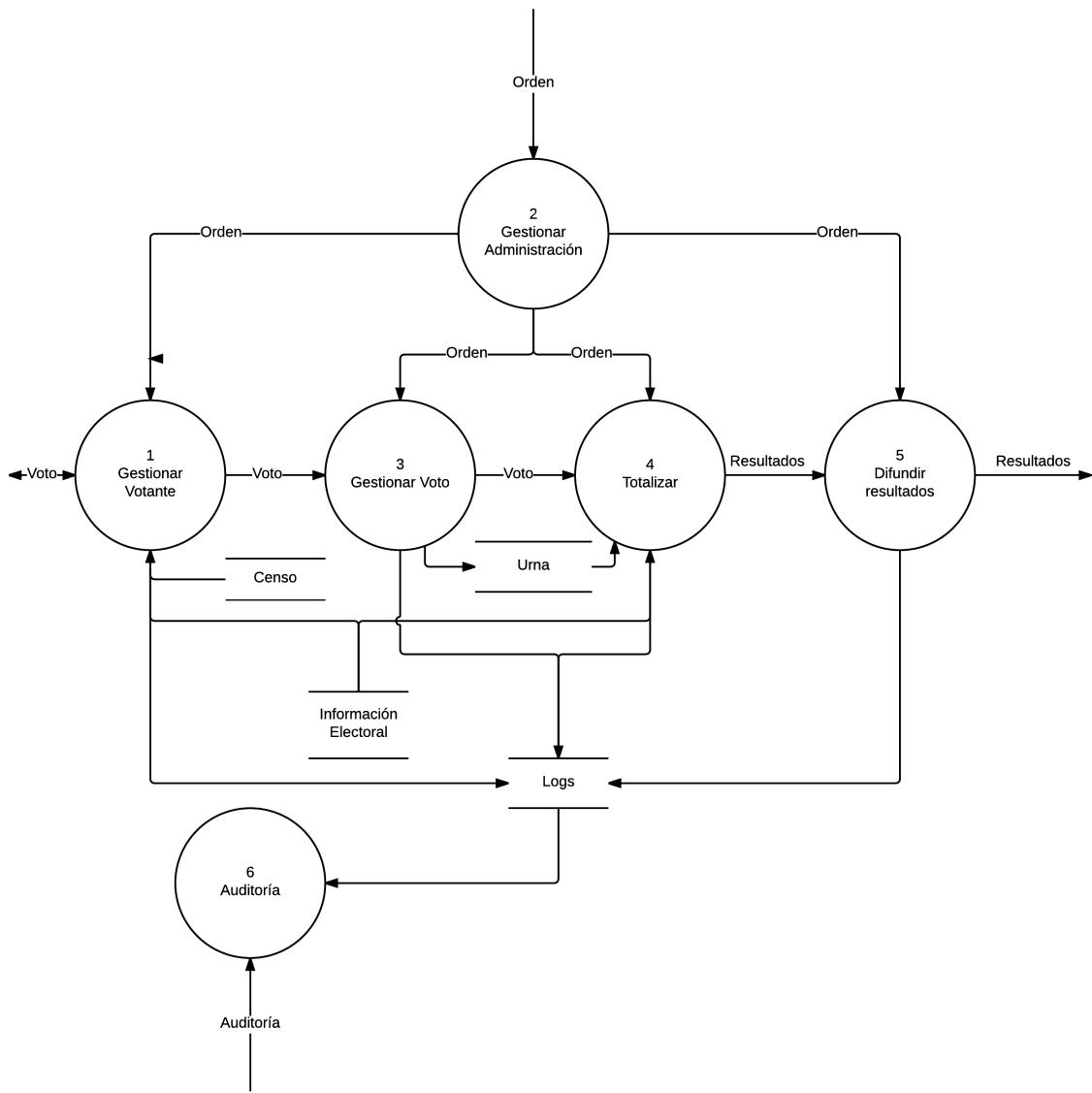


Figura 5.2: DFD 0

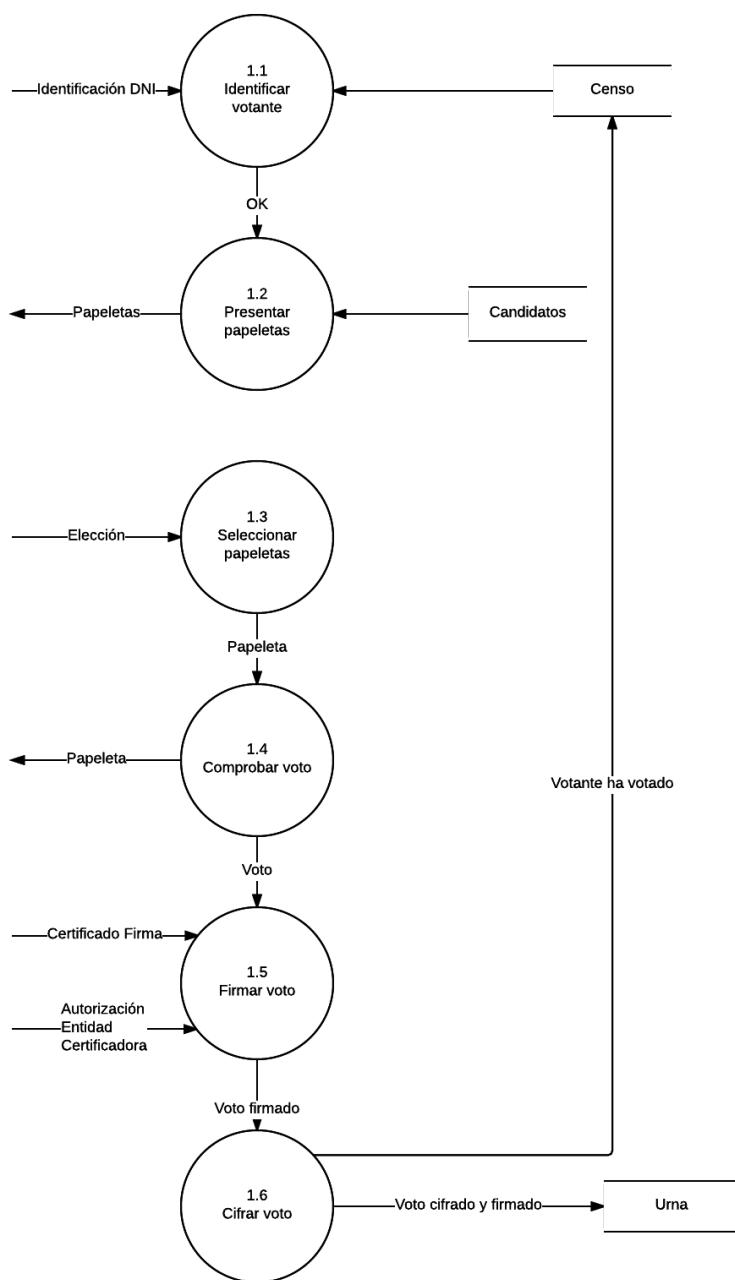


Figura 5.3: DFD 1. Gestión de votante

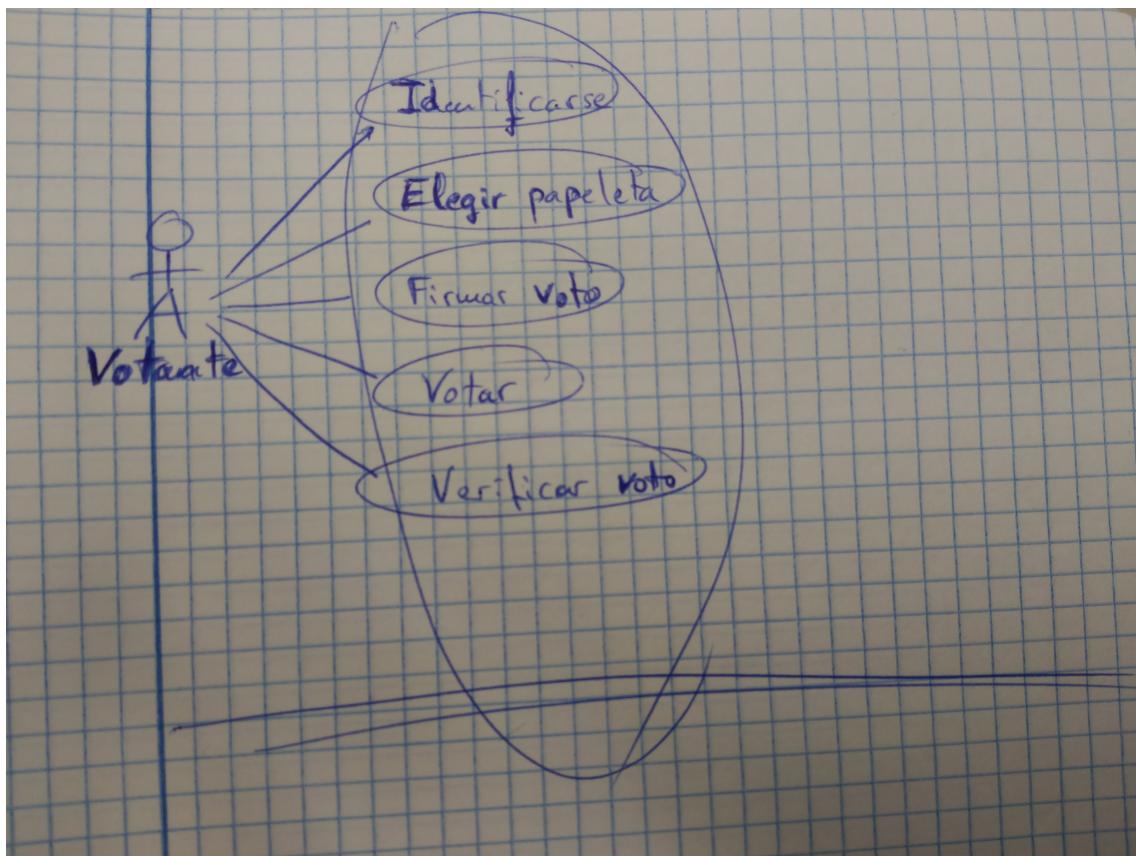


Figura 5.4: Caso de uso 1. Votante

Capítulo 6

Solución

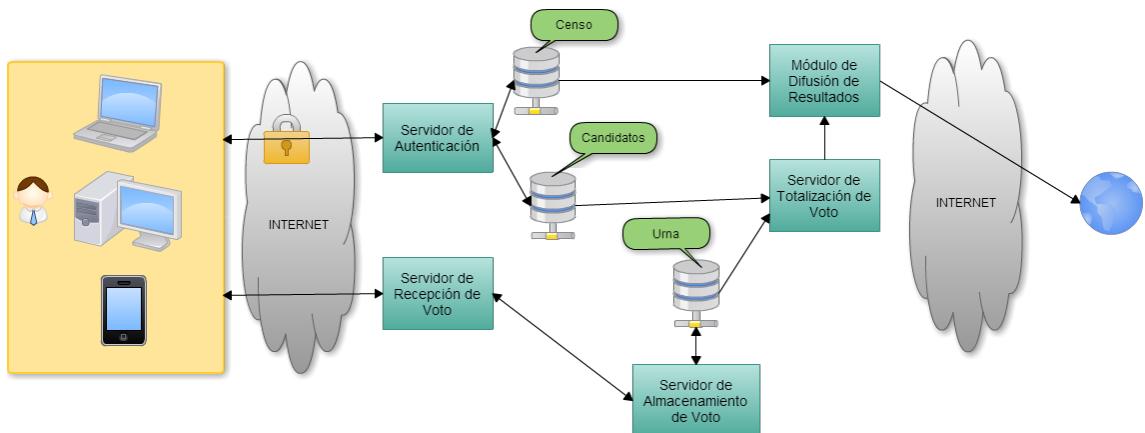


Figura 6.1: Diagrama de flujo del Sistema

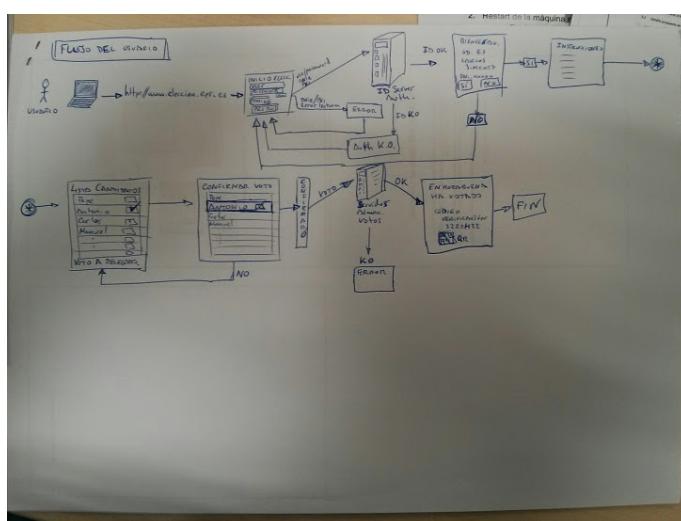


Figura 6.2: Esquema del flujo que sigue el votante

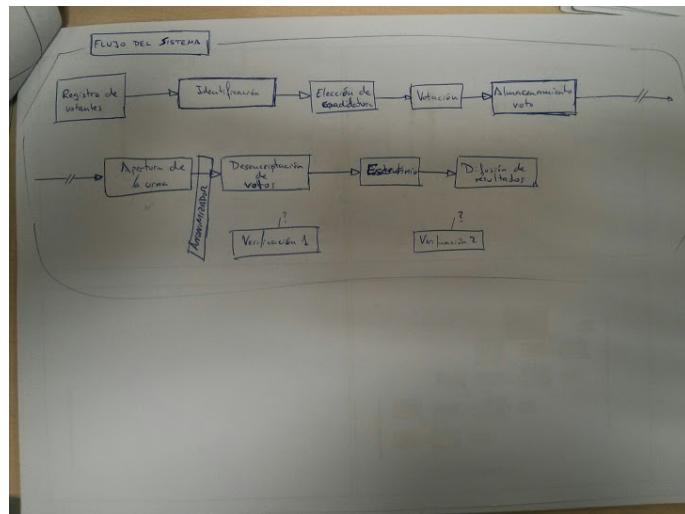


Figura 6.3: Esquema del flujo del Sistema

6.1. Diseño

6.1.1. Diseño del esquema de votación

6.1.1.1. Registro

La fase de registro de votantes en el sistema no será interactivo en cuanto a que no es el propio votante el que debe inscribirse para poder votar en las elecciones, sino que es la Autoridad Electoral la que lo registra en el censo. En esta fase, pues, se trata de establecer el censo de votantes que tienen autoridad para votar en el proceso electoral.

Como se advierte en el análisis se ha tomado en consideración que sean los administradores del sistema quienes tengan responsabilidad sobre el tratamiento del censo, por lo que se ha de cargar en el sistema y éste es el que lo va a tratar.

El censo ha de cargarse en dos servicios del sistema, tanto en el servidor de autenticación como en el sistema de votación.

El censo del subsistema de autenticación se utilizará para llevar el control de los votantes que tienen derecho de acceso al sistema, por lo que a los votantes se les puede añadir otros usuarios necesarios para llevar a término la votación, como pueden ser administradores o auditores, aunque estos no tengan derecho de voto. Así se conformaría la base de usuarios activos del sistema.

En el subsistema de voto también se vuelca el censo para cada uno de los diferentes procesos de voto que conformen la elección.

El procedimiento a seguir consistirá en que la Autoridad Organizadora del Proceso Electoral, la Universidad, proveerá una lista del censo a los administra-

dores del sistema. El administrador utilizará la función de carga de votantes con la lista proporcionada para realizar la carga inicial de votantes para cada una de las subelecciones que se configuren.

La lista proporcionada por la Universidad debe contener la siguiente información de cada uno de los votantes:

- Nombre y apellidos
- DNI
- Clase / grupo de votantes
- E-mail

La carga de los votantes a través de su aplicación se realiza subiendo un fichero csv con la información requerida. Este fichero se pone a disposición de la cola de procesos, la cual, llegado el momento volcará cada uno de los registros en la base de datos del sistema de votación.

Falta definir el proceso de carga de votantes para el servicio de autenticación.

6.1.1.2. Identificación

El servicio de identificación es un subsistema clave en el proceso electoral. En él recae parte de la responsabilidad de la robustez del sistema, en cuanto a que debe asegurar varios de los requisitos básicos que definen el voto electrónico en concreto:

Esto es así según los requisitos de Fujio-ka, si se utilizan los de la UNEX, se puede modificar.

Solidez: Debe asegurar que un votante deshonesto no tenga capacidad de acceder al sistema e interrumpir la votación. Es decir, que sólo debe dar acceso a los votantes que realmente deben ingresar al sistema de votación.

Elegibilidad: Este requisito implica que el sistema debe controlar que ningún votante que no tenga permitido el voto pueda votar. Aunque es el proceso de votación el que debe controlar esta circunstancia cuando un usuario trata de emitir un voto, el sistema de votación, de forma análoga al requisito anterior, también debe proteger el sistema evitando el acceso a aquellos que, directamente, no tengan permisos para votar.

Sin duplicados: El sistema debe evitar que un votante duplique o reemplace el voto de otro. Igualmente, aunque es el sistema de votación el que debe tener mecanismos que controlen esta situación, la primera barrera debe ser la servicio de autenticación del votante.

6.1.1.3. Elección de candidatura**6.1.1.4. Votación****6.1.1.5. Escrutinio****6.1.1.6. Difusión de resultados****6.1.2. Diseño de la arquitectura****6.1.3. Diseño de la capa de datos****6.1.4. Diseño de la red****6.1.5. Diseño de la interfaz de usuario****6.1.5.1. Estructura de la página web****6.1.5.2. Estructura de la aplicación móvil****6.1.5.3. Colores****6.1.5.4. Logo de la elección****6.1.5.5. 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 2.2.8 y SEVI 2.2.9 o los españoles de Víctor Moreno [28] o Votescript ??????? 2.2.6 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 votantes auditar que su voto ha sido correctamente incluido y contado en el proceso. Esta fase postelectoral también tiene más operativas ...

continuar con fase postelectoral

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

continuar...

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

6.1.6. 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 (2.2.6) 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,

Continuar protocolos

6.1.6.1. 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 escrita y bien puesto

6.2. ESTO ES EL PFC

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 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 de 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

Circunscripción???
No hay una forma mejor de expresarlo???

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 repartir 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)

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

continuar...

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 disagregaciones 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

continuar

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 únicamente 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, aunque utilizando DNIE con lector de chip sin contac-

InfoTUI

to, no haría falta si se hace uso de un dispositivo con sensor de radiofrecuencia, con capacidad para leer información a través de NFC.

A través de la app Android (o la app web), el votante accede al servicio de votación por Internet. El primer paso es la identificación del votante. Es la primera vez que hará uso de los certificados del DNIE. En este caso, la app leerá (con NFC o chip con contacto) el certificado de Autenticación del DNIE, por el cual se asegura la identidad del votante. Con la identidad del votante verificada (por la DGP), se contrasta con el censo, para comprobar:

- Si el votante existe en el censo.
- Si el votante ha votado previamente.
- Los datos censales del votante, para comprobar circunscripción, mesa electoral y, por ende, ser capaz de obtener los candidatos entre los que puede escoger.

Una vez verificado el votante y comprobados sus datos censales, se procede a construir la boleta con los candidatos que entre los que le corresponde elegir basándose en su circunscripción electoral. El sistema ha de presentar la boleta al votante y permitir que éste marque la o las opciones que permita el sistema electoral para constituir el voto a emitir.

Una vez constituido el voto (papeleta), hay que proceder a la votación digital. Para ello nos basamos en cifrado y firma ciega. Así, el primer paso es que la app utiliza la clave pública de la Entidad Electoral para cifrar el voto. Con el voto cifrado, el votante ha de firmarlo. La firma se realiza con el certificado de Firma que posee el DNIE. Así, el votante firma un conjunto de [voto cifrado + votante], que es el paquete que se pasará al subsistema de gestión del voto.

Una vez el votante ha emitido el voto, el sistema le devuelve un resguardo (código QR como en Estonia, un código alfanumérico, no sé todavía) con el cual puede verificar que el voto ha sido correctamente incluído en el sistema. Además, podrá verificar que el voto ha sido correctamente incluído en el escrutinio.

(No sé si con este resguardo debe poder llegar a la opción de voto elegida, todo depende de cómo tomemos el requisito de coerción y qué es lo que menos le afecta)

El votante puede votar tantas veces como desee cambiar su voto. Para ello, hay un protocolo por el cual cuando un votante emite su voto, todos los anteriores son anulados.

Hay que definir el protocolo para la anulación de votos por 'revoto'

Así disminuimos el riesgo de coerción

El sistema de gestión del voto es el encargado de los votos sufragados durante la jornada electoral. El sistema almacena los votos firmados (voto cifrado

+ votante) en una *urna* digital durante el tiempo que dura la jornada electoral. En caso de recibir un voto de un votante que ya previamente había emitido su voto, debe ser capaz de anular los votos anteriores que éste hubiese sufragado. Una vez que el Administrador del Proceso Electoral da por terminada la Jornada Electoral, los Miembros de la Junta Electoral utilizan sus claves para formar la clave maestra que permite dar por terminada la fase de votación y comenzar con el Escrutinio. La primera fase del Escrutinio es que los votos firmados deben ser *anonimizados*. Esto lo vamos a realizar en dos pasos. Primero, comprobamos la validez de la firma del voto firmado. Si la firma se corresponde con u voto a descartar, se elimina. Si la firma es válida, se extrae (abrimos el sobre donde va la info del votante y el sobre con su voto secreto) del contenido del voto firmado tanto el voto cifrado como la información asociada del votante. Por un lado, la información del votante se almacena para sacar un listado de votantes (que podrá compararse con el resultado de votantes del censo). Por otra parte, los votos cifrados pasan a otro almacén ya sin asociación con su votante. Para terminar de separar los votos de sus votantes, pasamos por un proceso anonimizador que ...

Como
digo an-
tes, hay
que defi-
nir cómo
se hace
esto de
anular
votos
emitidos

Aquí entra en juego ElGamal y sus amigos o las mixnets

. Una vez tenemos los votos separados de sus votantes, procedemos a la siguiente fase del escrutinio, que es la de (abrir el sobre del voto secreto) descifrar el voto. El sistema necesita la clave privada de la Entidad Electoral para descifrar los votos que, recordemos, están cifrados con la clave pública. Con esta clave privada, extraemos el contenido del voto cifrado y obtenemos cada uno de los votos en plano de las urnas digitales. Una vez obtenidos el conjunto de los votos en plano de cada urna digital, podemos proceder a la consolidación de los votos. Se realiza el conteo de cada urna y, con los resultados obtenidos, se puede realizar la totalización para llegar al resultado final de la Elección.

El último paso del sistema será el de la Difusión de los Resultados. El sistema de Escrutinio (o Totalización) informa de los resultados al módulo de Difusión, el cual les aplicará el formato necesario para cumplir con las necesidades de publicación de los mismos. En el caso del Proceso Electoral asociado a este proyecto, una web y diversos listados PDFs para poder ser cotejados.

Sería muy interesante que, como en Estonia, los votantes tuvieran una herramienta para poder verificar que su voto ha sido correctamente incluido y escrutado en el Proceso.

Paralelamente a todo el proceso, cada subsistema ha de generar una serie de registros, ficheros logs, que puedan ser visualizados por un conjunto de audi-

tores, observadores u otro grupo de profesionales que tengan que dar cuenta del correcto funcionamiento del Proceso y de la transparencia del mismo, así como del éxito técnico del Sistema.

Capítulo 7

Plan de pruebas

Capítulo 8

Líneas futuras

Uso de Enigma http://enigma.media.mit.edu/enigma_full.pdf(8.9, página 13) para el voto por Internet. Otro: <http://www.pabloyglesias.com/cifrado-homomorfico-bl>

Capítulo 9

Conclusiones

Bibliografía

- [1] ADIDA, B. Advances in Cryptographic Voting Systems. Master's thesis, MIT - Massachusetts Institute of Technology - Department of Electrical Engineering and Computer Science, Agosto 2006. <http://assets.adida.net/research/phd-thesis.pdf>.
- [2] ADIDA, B. Helios: Web-based open-audit voting. In *Proceedings of the Seventeenth Usenix Security Symposium (USENIX Security 2008)* (July 2008), pp. 335–348.
- [3] BENALOH, J. Simple verifiable elections. In *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop* (Berkeley, CA, USA, 2006), EVT'06, USENIX Association, pp. 5–5.
- [4] ØBERG, M. W. Improving the Norwegian Internet Voting Protocol. Master's thesis, Department of Mathematical Sciences, NTNU - Norwegian University of Science and Technology, Junio 2011. <https://daim.idi.ntnu.no/masteroppgaver/005/5823/masteroppgave.pdf>.
- [5] BURNAND, F. E-voting to advance slowly in 2011. <http://www.swissinfo.ch/eng/e-voting-to-advance-slowly-in-2011/29138944>, 2011.
- [6] 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 Congreso de Ecuaciones Diferenciales y Aplicaciones. X Congreso de Matemática Aplicada* (Septiembre 2007).
- [7] 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.
- [8] CARTER CENTER. Internet Voting Pilot: Norway's 2013 Parliamentary Elections, Mar. 2014.
- [9] Certificados Digitales - FNMT. <https://www.cert.fnmt.es/curso-de-criptografia/certificados-digitales>.
- [10] CHAUM, D. L. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Commun. ACM* 24, 2 (Feb. 1981), 84–90.
- [11] 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.
- [12] CODINA LLIGOÑA, J. Bases teóricas y herramientas para el análisis y comparación de sistemas de votación de código abierto. Master's thesis, Universitat Oberta de Catalunya - Institut Municipal d'Informàtica de Barcelona, Enero 2014. <http://openaccess.uoc.edu/webapps/o2/handle/10609/28282>.
- [13] CORTÉS POLO, DAVID MIGUEL, HORNERO ÍNCERA, ALEXEI, MARTÍNEZ BRAVO, LORENZO, AND GONZÁLEZ-SÁNCHEZ, JOSÉ LUIS. Estudio de infraestructura para sistemas de voto electrónico. *Departamento de Informática, Escuela Politécnica. Universidad de Extremadura (-)*. <http://gitaca.unex.es/agila/voto/voto.pdf>.
- [14] 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.
- [15] DHILLON, KYLE. Challenges for LargeScale Internet Voting Implementations. Tech. rep., Princeton University Department of Computer Science, Enero 2015. https://www.cs.princeton.edu/sites/default/files/uploads/kyle_dhillon.pdf.
- [16] DIRECCIÓN GENERAL DE LA POLICÍA - MINISTERIO DEL INTERIOR - ESPAÑA. Infraestructura de Clave Pública - DNI Electrónico - Proyecto de Declaración de Prácticas y Políticas de Certificación. http://www.dnielectronico.es/PDFs/politicas_de_certificacion.pdf, Marzo 2006.

- [17] DIRECCIÓN GENERAL DE LA POLICÍA - MINISTERIO DEL INTERIOR - ESPAÑA. Infraestructura de Clave Pública de la Dirección General de la Policía - Declaración de Prácticas y Políticas de Certificación. <http://www.policia.es/DPC/dpc.pdf>, Enero 2014.
- [18] Internet Voting - Voting methods in Estonia - Estonian National Electoral Committee. <http://www.vvk.ee/voting-methods-in-estonia/engindex/>.
- [19] 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), ASIACRYPT '92, Springer-Verlag, pp. 244–251.
- [20] 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>.
- [21] 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.
- [22] 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.
- [23] IEEE. IEEE Recommended Practice for Software Requirements Specifications. *IEEE Std 830-1998* (1998).
- [24] KIAYIAS, A., KORMAN, M., AND WALLUCK, D. An internet voting system supporting user privacy. In ACSAC (2006), IEEE Computer Society, pp. 165–174.
- [25] 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.

- [26] 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>.
- [27] 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>.
- [28] MORENO PEÑA, ADRIÁN. Portal web para la gestión 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>.
- [29] 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>.
- [30] 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.
- [31] 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>.
- [32] PANIZO ALONSO, L. Desarrollo de una metodología para el análisis y la clasificación de los sistemas de voto electrónico. Master's thesis, Universidad de León - Departamento de Ingeniería Eléctrica y de Sistemas y Automática, Diciembre 2014. https://buleria.unileon.es/bitstream/handle/10612/4237/tesis_b4cfc6.PDF.
- [33] PÉREZ BELLEBONI, E. Aplicación de documentos de identificación electrónica a un esquema de voto telemático a escala paneuropea, seguro,

- auditabile 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.
- [34] PÉREZ BELLEBONI, EMILIA, AND CARRACEDO GALLARDO, JUSTO. Uso del DNle 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.
- [35] Indra. Procesos Electorales. <http://www.indracompany.com/sector/procesos-electorales>.
- [36] 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.
- [37] Scytel. <http://www.scytl.com/>.
- [38] SMYTH, B., FRINK, S., AND CLARKSON, M. R. Election Verifiability: Cryptographic Definitions and an Analysis of Helios and JCJ. *Cryptology ePrint Archive*, Report 2015/233, 2015. <https://eprint.iacr.org/2015/233.pdf>.
- [39] U.S. ELECTION ASSISTANT COMMISSION. A Survey of Internet Voting. <http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf>, Septiembre 2011.
- [40] 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>.
- [41] Voting Machines Pros and Cons. <http://votingmachines.procon.org/view.timeline.php?timelineID=000021>.

Notas (para borrador)

■	IMAGEN DOS CONJUNTOS, UNO (E-VOTING) CONTIENE AL OTRO (I-VOTING)	14
■	COMENTADO POR AHORA	16
■	Breve Historia del voto electrónico	16
■	If there is any invention on Earth that we don't want down here, that is it.	16
■	UN POQUITO MÁS DE HISTORIA ***** HABLAR DE DRE Y TARJETAS PERFORADAS	18
■	Aquí referencia a los requisitos del voto electrónico	20
■	Hay que arreglar este párrafo.	26
■	Voting systems are hard to make trustworthy because they have strong, conflicting security requirements: - Integrity of election results must be assured so that all voters are convinced that votes are counted correctly. Any attempt to corrupt the integrity of an election must be detected and correctly attributed. - Confidentiality of votes must be assured to protect voters' privacy, to prevent selling of votes, and to defend voters from coercion. Integrity is easy to obtain through a public show of hands, but this destroys confidentiality. Confidentiality can be obtained by secret ballots, but this fails to assure integrity. Because of the civic importance of elections, violations of these requirements can have dramatic consequences. https://www.cs.cornell.edu/projects/civitas/papers/clarkson_civitas_tr.pdf	26
■	Hay que citar el documento que hay en https://www.jbisa.nl/download?id=17700076&download=1	31
■	Hay que marcar que la fuente de estos datos provienen del Tribunal Electoral de Estonia (o como se diga), concretamente de la web http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics	32

■ ***** EXPLICAR UN POCO EL FUNCIONAMIENTO Y ANALIZARLO	
***** SEGÚN BELLEBONI, EN SUS CONCLUSIONES: - Interesante por ser una elección a nivel 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 (¿?) *****	34
■ INTERESANTE – http://elecciones.smartmatic.com/estonia-y-el-voto-por-internet/	35
■ ¿Hay que hablar de Noruega?	35
■ Destacar que estas tablas vienen de una ponencia de Justo Carracedo, presentación en Posibilidades del voto telemático en la democracia digital http://www.criptored.upm.es/descarga/ConferenciaJustoCarracedoTASSI2014.pdf	35
■ seguir?...	36
■ Indra	37
■ (Scytel)	37
■ Nombre de la Universidad!!	38
■ ME HE QUEDADO POR AQUÍ	38
■ SELES	38
■ Quitar el pie que viene implícito en la imagen!!!	38
■ http://www.cs.cornell.edu/projects/civitas/	39
■ Civitas is a new, secure voting system. Civitas is the first voting system implementation that allows voters to vote securely from the remote client of their choice, while provably providing universal verifiability, voter verifiability, anonymity, and coercion resistance. Civitas scales up to a large number of voters, with a low marginal computational cost per voter.	39

■ On-line Voting System is a web based system that facilitates the running of elections and surveys online. This system has been developed to simplify the process of organizing elections and make it convenient for voters to vote remotely from their home computers while taking into consideration security, anonymity and providing auditing capabilities. Users are individuals who interact with the system. All user interaction is performed remotely through the user's web browser. Users are categorized into three classes: Administrator, returning Officers and Voters. A running version of the system will have only one Administrator but it typically has multiple returning officers and voters. The administrator is responsible for managing user accounts, polls, system resources and logs and for the health and safekeeping of the system. Returning officers have the responsibility of managing a poll as assigned by the administrator, whereas voters only have the ability to submit ballots on polls in which they are admitted.	40
■ quitar esto, que no va a ir aquí	40
■ Falta decir el porqué!! Porqué se olvidan los votantes de la amenaza? pues porque el E2E consigue que se demuestre la invariabilidad del voto emitido frente al contado...E2E	41
■ Aquí va la imagen de la arquitectura de ADDER.	43
■ esto no está muy bien explicado	44
■ Ver una descripción de Helios v4 en [38]	45
■ la siguiente info para analizar está sacada de https://eprint.iacr.org/2015/942.pdf	45
■ PRIMITIVAS CRIPTOGRÁFICAS O ESQUEMAS DE VOTO ELECTRÓNICO ???	47
■ EL TEMA ES QUE EXISTEN ESTAS PRIMITIVAS BÁSICAS Y LUEGO LOS ESQUEMAS SE BASAN EN ELLAS PARA SER DISEÑADOS	47
■ Hablamos del cifrado homomórfico	50
■ Ahondar un poco en la criptografía, pero sólo la parte que entiendo.	50
■ LITERAL	52
■ LITERAL	52
■ Explicación del proceso (Chaum??)	52
■ ***** VER BELLEBONI *****	53
■ ***** Según [27] *****	53
■ Estoy diciendo cosas contradictorias. Arreglar.	53
■ MÁS MÁS MÁS MÁSSSSSS	55

■ Buena fuente de información en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_RFID.pdf	55
■ DNle - Añadir DNle 3.0	56
■ ?¿?¿?¿, además de un coste ajustado,	58
■ SEGUIR CON LOS OBJETIVOS	59
■ AQUÍ HACE FALTA ENCONTRAR UN TEXTO LEGAL EXPLICANDO EL PROCEDIMIENTO DE LAS ELECCIONES	60
■ No me gusta nada cómo está redactado esto ni me parece que esté en el sitio correcto. Cambiar.	62
■ Poner aquí qué significa esta información	65
■ Explicar en qué consiste la verificación	65
■ Es necesario comentar en qué consiste la auditoría del tally.	65
■ Alcance del proyecto	66
■ 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	67
■ ***** CREO QUE ESTÁ MAL. REALMENTE, LOS ALUMNOS SON UNA ÚNICA CIRCUNSCRIPCIÓN: SU CENSO LO FORMAN LOS DELEGADOS Y SUBDELEGADOS DE CADA UNO DE LOS GRUPOS, QUE COMPONEN TAMBIÉN LOS CANDIDATOS. CANDIDATOS = CENSO EN ESTA "CIRCUNSCRIPCIÓN"	69
■	70
■ LOPD ?? ? ? ?	71
■ ***** no estoy seguro, qué pasa con fotocopias??, yo me fiaría de los certificados	74
■	74
■ Explicar un poco más el nuevo DNle, ventajas e inconvenientes para el voto por Internet, así como un poco su funcionamiento con los cambios respecto al DNle 1.0 —— aunque todo esto va en Estado de la cuestión	74
■ hay que mirar bien esto del MobID, pues no sé si habrá algo desarrollado, de todos modos, en España esto ni se contempla	75

■ Lo que pasa es que me temo que estas tarjetas no tienen certificados, con lo que tampoco van a valer para la votación	75
■ 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	76
■ Rellenar este etc.	78
■ Introducir la firma del voto con el DNle no introduce ningún tipo de mejora en la seguridad respecto del que provee de por sí la propia herramienta Helios Voting. Así que no lo vamos a hacer. Hay que cambiar las modificaciones sobre la misma.	81
■ Hay que explicar el flujo que se ha implementado para el OAuth. Ver en el código.	83
■ hay que encontrar una mejor palabra	86
■ Este párrafo está improvisado, habría que darle una vuelta.	87
■ 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	88
■ Restricciones	91
■ (Analizando este requisito, la mejor forma es habilitar 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)	91
■ (24/7, un día, varios días... depende de cómo se defina el proceso)	91
■ Esto de sin posibilidad de error ni me gusta ni queda correcto	92
■ 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	92
■ NO ESTOY DE ACUERDO CON ESTO. ALGUNOS AUTORES INDICAN LO CONTRARIO, QUE ES PRIMORDIAL QUE EL VOTANTE SE QUEDA 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 COERCIÓN, ¿O SÍ?	93
■ ESTE NO CREO QUE DEBA IR, YA QUE ES UN RESUMEN DE LOS SIGUIENTES	94

■ (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)	95
■ 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	95
■ ¿QUEREMOS ESTO? TOTAL, EL RIESGO DE COERCIÓN ES MUY BAJO EN ESTAS ELECCIONES... PERO SI QUEREMOS ACERCARNOS A UNAS GENERALES, QUIZÁS SEA IMPEPINABLE, SIGUIENDO EL MODELO ESTONIO *****)	96
■ 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	96
■ OTRA FORMA EN LA QUE PODEMOS ORDENAR LA ESPECIFICACIÓN DE REQUISITOS HAY QUE RE-REDACTARLO	96
■ Todas las restricciones	97
■ CAMBIAR EL NOMBRE de miembro de la Junta Electoral	99
■ Teniendo en cuenta la organización de Helios, los miembros de la Junta Electoral que tenemos aquí son los trustees del sistema original de Adida.	99
■ PLANTILLA PARA PROYECTO DE FIN DE GRADO (Universidad de Cádiz) Propuesta de REDiris	100
■ 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.	100
■ 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.	101

■ 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)	101
■ 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.	101
■ 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.	101
■ Falta definir el proceso de carga de votantes para el servicio de autenticación.	107
■ Esto es así según los requisitos de Fujioka, si se utilizan los de la UNEX, se puede modificar.	107
■ ???????	108
■ ???????	108
■ continuar con fase postelectoral	109
■ continuar...	109
■ Antes de este punto hay que hacer un resumen de los diferentes esquemas de votación, teniendo estos como Firma ciega, mixnets, etc...	109
■ Continuar protocolos	111
■ 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	111
■ Cir-cuns-crip-ción??? No hay una forma mejor de expresarlo??	111
■ *****	112
■ (Aquí encontramos un primer punto de auditoría importante).	113
■ (En algunos países, en vez de elaborarse un censo oficial, son los propios votantes los que han de registrarse)	113
■ continuar...	113
■ 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	113

■ Pasamos a la siguiente fase: Identificación	113
■ En el caso de las elecciones de la EPS, los documentos válidos son	114
■ continuar	114
■ ***InfoTUI***	114
■ (No sé si con este resguardo debe poder llegar a la opción de voto elegida, todo depende de cómo tomemos el requisito de coerción y qué es lo que menos le afecta)	115
■ Así disminuimos el riesgo de coerción	115
■ Hay que definir el protocolo para la anulación de votos por 'revoto'	115
■ Como digo antes, hay que definir cómo se hace esto de anular votos emitidos	116
■ Aquí entra en juego ElGamal y sus amigos o las mixnets	116