16.

FECHA	miércoles, 2 de diciembre de 2020

Señores
UNIVERSIDAD DE CUNDINAMARCA
BIBLIOTECA
Ciudad

UNIDAD REGIONAL	Extensión Facatativá
TIPO DE DOCUMENTO	Trabajo De Grado
FACULTAD	Ingeniería
NIVEL ACADÉMICO DE FORMACIÓN O PROCESO	Pregrado
PROGRAMA ACADÉMICO	Ingeniería de Sistemas

El Autor (Es):

APELLIDOS COMPLETOS	NOMBRES COMPLETOS	No. DOCUMENTO DE IDENTIFICACIÓN
Pérez Bohórquez	Cristian Camilo	1070926072

Director (Es) y/o Asesor (Es) del documento:

APELLIDOS COMPLETOS	NOMBRES COMPLETOS
Valenzuela Sabogal	Gina Maribel

TÍTULO DEL DOCUMENTO
SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO AUTENTICACIÓN

SUBTÍTULO (Aplica solo para Tesis, Artículos Científicos, Disertaciones, Objetos Virtuales de Aprendizaje)

TRABAJO PARA OPTAR AL TÍTULO DE: Aplica para Tesis/Trabajo de Grado/Pasantía
Ingeniero de Sistemas

AÑO DE EDICION DEL DOCUMENTO	NÚMERO DE PÀGINAS
2020	194

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS (Usar 6 descriptores o palabras claves)	
ESPAÑOL	**INGLÉS**
1. Voto electrónico	Electronic voting
2. Autenticación	Authentication
3. Criptografía	Cryptography
4. Seguridad	Security
5. Clave Asimétrica	Asymmetric Key
6. Identidad Digital	Digital Identity

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS

(Máximo 250 palabras – 1530 caracteres, aplica para resumen en español):

Resumen

El presente proyecto establece el diseño, desarrollo e implementación de un módulo de autenticación multifactorial, que permita la validación de identidad y el control de acceso a la plataforma de voto por internet que se desarrolla actualmente en la universidad de Cundinamarca, representando un avance hacia la generación de un modelo de gobierno electrónico y la modernización de los procesos que se realizan dentro de la institución educativa, mediante la implementación de la criptografía de clave asimétrica, que se basa en la generación de un par de llaves relacionadas, una publica y una privada, a través de un algoritmo basado en las matemáticas de las curvas elípticas (ECC), que garantice la confidencialidad de la información así como un mayor nivel de seguridad y confianza en el proceso de autenticación. El desarrollo del módulo se basa fundamentalmente en el lenguaje de programación JAVA, mediante la implementación de la biblioteca Java Cryptography Architecture (JCA) y el proveedor de herramientas y algoritmos criptográficos Bouncy Castle. Esto, haciendo uso de algunos elementos de la metodología ágil SCRUM, debido a su amplia implementación en diversos desarrollos de software y hardware, llegando a destacar por la flexibilidad, adaptación, organización, incremento en la productividad y la calidad de los resultados finales. Además de la metodología de desarrollo en cascada, por lo que las actividades, se definen de acuerdo con las etapas inherentes a dicho modelo.

Abstract

This project establishes the design, development and implementation of a multifactorial authentication module, which allows identity validation and access control to the online voting platform currently being developed at the University of Cundinamarca, representing an advance towards generation of an electronic government model and the modernization of the processes carried out within the educational institution, through the implementation of asymmetric key cryptography, which is based on the generation of a pair of related keys, one public and one private , through an algorithm based on the mathematics of elliptic curves (ECC), which guarantees the confidentiality of the information as well as a higher level of security and confidence in the authentication process. The development of the module is fundamentally based on the JAVA programming language, through the implementation of the Java Cryptography Architecture (JCA) library and the provider of cryptographic tools and algorithms Bouncy Castle. This, making use of some elements of the SCRUM agile methodology, due to its wide implementation in various software and hardware developments, standing out for its flexibility, adaptation, organization, increased productivity and the quality of the final results. In addition to the cascade development methodology, so the activities are defined according to the stages inherent to said model.

AUTORIZACION DE PUBLICACIÒN

Por medio del presente escrito autorizo (Autorizamos) a la Universidad de Cundinamarca para que, en desarrollo de la presente licencia de uso parcial, pueda ejercer sobre mí (nuestra) obra las atribuciones que se indican a continuación, teniendo en cuenta que, en cualquier caso, la finalidad perseguida será facilitar, difundir y promover el aprendizaje, la enseñanza y la investigación.

En consecuencia, las atribuciones de usos temporales y parciales que por virtud de la presente licencia se autoriza a la Universidad de Cundinamarca, a los usuarios de la Biblioteca de la Universidad; así como a los usuarios de las redes, bases de datos y demás sitios web con los que la Universidad tenga perfeccionado una alianza, son:

Marque con una "X":

AUTORIZO (AUTORIZAMOS)	SI	NO
1. La reproducción por cualquier formato conocido o por conocer.	X	
2. La comunicación pública por cualquier procedimiento o medio físico o electrónico, así como su puesta a disposición en Internet.	X	
3. La inclusión en bases de datos y en sitios web sean éstos onerosos o gratuitos, existiendo con ellos previa alianza perfeccionada con la Universidad de Cundinamarca para efectos de satisfacer los fines previstos. En este evento, tales sitios y sus usuarios tendrán las mismas facultades que las aquí concedidas con las mismas limitaciones y condiciones.	X	
4. La inclusión en el Repositorio Institucional.	X	

De acuerdo con la naturaleza del uso concedido, la presente licencia parcial se otorga a título gratuito por el máximo tiempo legal colombiano, con el propósito de que en dicho lapso mi (nuestra) obra sea explotada en las condiciones aquí estipuladas y para los fines indicados, respetando siempre la titularidad de los derechos patrimoniales y morales correspondientes, de acuerdo con los usos honrados, de manera proporcional y justificada a la finalidad perseguida, sin ánimo de lucro ni de comercialización.

Para el caso de las Tesis, Trabajo de Grado o Pasantía, de manera complementaria, garantizo(garantizamos) en mi(nuestra) calidad de estudiante(s) y por ende autor(es) exclusivo(s), que la Tesis, Trabajo de Grado o Pasantía en cuestión, es producto de mi(nuestra) plena autoría, de mi(nuestro) esfuerzo personal intelectual, como

consecuencia de mi(nuestra) creación original particular y, por tanto, soy(somos) el(los) único(s) titular(es) de la misma. Además, aseguro (aseguramos) que no contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos de la Tesis o Trabajo de Grado es de mí (nuestra) competencia exclusiva, eximiendo de toda responsabilidad a la Universidad de Cundinamarca por tales aspectos.

Sin perjuicio de los usos y atribuciones otorgadas en virtud de este documento, continuaré (continuaremos) conservando los correspondientes derechos patrimoniales sin modificación o restricción alguna, puesto que, de acuerdo con la legislación colombiana aplicable, el presente es un acuerdo jurídico que en ningún caso conlleva la enajenación de los derechos patrimoniales derivados del régimen del Derecho de Autor.

De conformidad con lo establecido en el artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, *"Los derechos morales sobre el trabajo son propiedad de los autores"*, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables. En consecuencia, la Universidad de Cundinamarca está en la obligación de RESPETARLOS Y HACERLOS RESPETAR, para lo cual tomará las medidas correspondientes para garantizar su observancia.

NOTA: (Para Tesis, Trabajo de Grado o Pasantía):

Información Confidencial:

Esta Tesis, Trabajo de Grado o Pasantía, contiene información privilegiada, estratégica, secreta, confidencial y demás similar, o hace parte de la investigación que se adelanta y cuyos resultados finales no se han publicado. **SI** _X__ **NO** ___.
En caso afirmativo expresamente indicaré (indicaremos), en carta adjunta tal situación con el fin de que se mantenga la restricción de acceso.

LICENCIA DE PUBLICACIÒN

Como titular(es) del derecho de autor, confiero(erimos) a la Universidad de Cundinamarca una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, por un plazo de 5 años, que serán prorrogables indefinidamente por el tiempo que dure el derecho patrimonial del autor. El autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito. (Para el caso de los Recursos Educativos Digitales, la Licencia de Publicación será permanente).

b) Autoriza a la Universidad de Cundinamarca a publicar la obra en formato y/o soporte digital, conociendo que, dado que se publica en Internet, por este hecho circula con un alcance mundial.

c) Los titulares aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) El(Los) Autor(es), garantizo(amos) que el documento en cuestión, es producto de mi(nuestra) plena autoría, de mi(nuestro) esfuerzo personal intelectual, como consecuencia de mi (nuestra) creación original particular y, por tanto, soy(somos) el(los) único(s) titular(es) de la misma. Además, aseguro(aseguramos) que no contiene citas, ni transcripciones de otras obras protegidas, por fuera de los límites autorizados por la ley, según los usos honrados, y en proporción a los fines previstos; ni tampoco contempla declaraciones difamatorias contra terceros; respetando el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales. Adicionalmente, manifiesto (manifestamos) que no se incluyeron expresiones contrarias al orden público ni a las buenas costumbres. En consecuencia, la responsabilidad directa en la elaboración, presentación, investigación y, en general, contenidos es de mí (nuestro) competencia exclusiva, eximiendo de toda responsabilidad a la Universidad de Cundinamarca por tales aspectos.

e) En todo caso la Universidad de Cundinamarca se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

f) Los titulares autorizan a la Universidad para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

g) Los titulares aceptan que la Universidad de Cundinamarca pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

h) Los titulares autorizan que la obra sea puesta a disposición del público en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en el “Manual del Repositorio Institucional AAAM003”

i) Para el caso de los Recursos Educativos Digitales producidos por la Oficina de Educación Virtual, sus contenidos de publicación se rigen bajo la Licencia Creative Commons: Atribución- No comercial- Compartir Igual.

j) Para el caso de los Artículos Científicos y Revistas, sus contenidos se rigen bajo la Licencia Creative Commons Atribución- No comercial- Sin derivar.

Nota:
Si el documento se basa en un trabajo que ha sido patrocinado o apoyado por una entidad, con excepción de Universidad de Cundinamarca, los autores garantizan que se ha cumplido con los derechos y obligaciones requeridos por el respectivo contrato o acuerdo.

La obra que se integrará en el Repositorio Institucional está en el(los) siguiente(s) archivo(s).

Nombre completo del Archivo Incluida su Extensión (Ej. PerezJuan2017.pdf)	Tipo de documento (ej. Texto, imagen, video, etc.)
1. SISTEMA DE VOTO ELECTRONICO, MODULO AUTENTICACION.pdf	Texto
2.	
3.	
4.	

En constancia de lo anterior, Firmo (amos) el presente documento:

APELLIDOS Y NOMBRES COMPLETOS	FIRMA (autógrafa)
Pérez Bohórquez Cristian Camilo	Cristian Camilo Pérez.

21.1-51-20.

SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO AUTENTICACIÓN

CRISTIAN CAMILO PÉREZ BOHÓRQUEZ

UNIVERSIDAD DE CUNDINAMARCA

Facultad de Ingeniería

Programa de Ingeniería De Sistemas

Facatativá, 2020

SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO AUTENTICACIÓN

AUTOR:

Cristian Camilo Pérez Bohórquez

DIRECTORA DE PROYECTO:

Ing. Gina Maribel Valenzuela Sabogal

GRUPO DE INVESTIGACIÓN DE SISTEMAS Y TECNOLOGÍA DE FACATATIVÁ (GISTFA)

UNIVERSIDAD DE CUNDINAMARCA

Facultad de Ingeniería

Programa de Ingeniería de Sistemas

Facatativá, 2020

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____

Jurado

_____

Jurado

Facatativá, noviembre 2020

COMPROMISO DE AUTOR

Yo Cristian Camilo Pérez Bohórquez, con cedula de identidad No. 1.070.926.072 y con cód. 561216195 estudiante del programa de ingeniería de sistemas de la Universidad de Cundinamarca, declaro que:

El contenido del presente documento es un reflejo de mi trabajo personal y manifiesto que, ante cualquier notificación de plagio, copia o falta a la fuente original, soy responsable directo legal, económico y administrativo sin afectar al director del trabajo, a la Universidad y a cuantas instituciones hayan colaborado en dicho trabajo, asumiendo las consecuencias derivadas de tales prácticas.

Firma:

RESUMEN

El presente proyecto establece el diseño, desarrollo e implementación de un módulo de autenticación multifactorial, que permita la validación de identidad y el control de acceso a la plataforma de voto por internet que se desarrolla actualmente en la universidad de Cundinamarca, representando un avance hacia la generación de un modelo de gobierno electrónico y la modernización de los procesos que se realizan dentro de la institución educativa, tomando como referencia las pautas y los niveles de seguridad contenidos en el marco de garantía de autentificación de entidad, establecido por la unión internacional de telecomunicaciones (ITU), además de la incorporación de la criptografía de clave asimétrica, que se basa en la generación de un par de llaves relacionadas, una publica y una privada, a través de un algoritmo basado en las matemáticas de las curvas elípticas (ECC), que garantice la confidencialidad de la información así como un mayor nivel de seguridad y confianza en el proceso de autenticación. El desarrollo del módulo se basa fundamentalmente en el lenguaje de programación JAVA, mediante la implementación de la biblioteca Java Cryptography Architecture (JCA) y el proveedor de herramientas y algoritmos criptográficos Bouncy Castle. Esto, haciendo uso de algunos elementos de la metodología ágil SCRUM, debido a su amplia implementación en diversos desarrollos de software y hardware, llegando a destacar por la flexibilidad, adaptación, organización, incremento en la productividad y la calidad de los resultados finales. Además de la metodología de desarrollo en cascada, por lo que las actividades, se definen de acuerdo con las etapas inherentes a dicho modelo.

Palabras clave: Autenticación, Criptografía, Clave Asimétrica.

ABSTRACT

This project establishes the design, development and implementation of a multifactor authentication module, allows identity validation and access control to the online voting platform currently being developed at the University of Cundinamarca, representing an advance towards generation of a model of electronic government and the modernization of the processes that are carried out within the educational institution, taking as reference the guidelines and security levels contained in the framework of entity authentication guarantee, established by the international telecommunications union (ITU), in addition to the incorporation of asymmetric key cryptography, which is based on the generation of a pair of related keys, a publication and a private one, through an algorithm based on the mathematics of elliptic curves (ECC), that guarantees the confidentiality of the information as well as a higher level of security and conf Alliance in the authentication process. The module development is mainly based on the JAVA programming language, through the implementation of the Java Cryptography Architecture (JCA) library and the provider of cryptographic tools and algorithms Bouncy Castle. This, making use of some elements of the SCRUM agile methodology, due to its wide implementation in various software and hardware developments, standing out for its flexibility, adaptation, organization, increased productivity, and the quality of the results. In addition to the cascade development methodology, so the activities are defined according to the stages inherent to said model.

Keywords: Authentication, Cryptography, Asymmetric Key.

ÍNDICE GENERAL

LISTA DE TABLAS

LISTA DE GRAFICOS

LISTA DE ANEXOS

INTRODUCCIÓN

El proceso de autenticación constituye un factor fundamental de la seguridad dentro de las operaciones que se realizan a través de medios electrónicos e internet. Conforme a que se incrementa el desarrollo y el uso de recursos informáticos, también se hacen más frecuentes los riesgos y amenazas a la integridad, confidencialidad y disponibilidad de la información. Lo anteriormente mencionado supone un aumento en la necesidad de implementar metodologías de autenticación que permitan comprobar que un usuario sea quien dice ser de manera confiable. El creciente avance tecnológico y las investigaciones que se han realizado a través del tiempo en materia de seguridad informática, han permitido establecer diferentes métodos de autenticación de usuarios, divididos en tres grupos principales; aquellos basados en el conocimiento, las características biométricas inherentes al usuario y por último la posesión de una clave u objeto único. A la combinación de dos o más de estos métodos se le conoce como autenticación multifactor; principio en el cual está fundamentado el proyecto en curso, para su respectiva aplicación dentro de una plataforma institucional de votación por internet, en la cual es de vital importancia asegurar de manera fidedigna que la persona que accede para emitir un voto sea quien dice ser en realidad, por lo que se realiza la incorporación de la autenticación basada en el conocimiento a través de un usuario y contraseña, en conjunto con la generación de un par de claves relacionadas por una función matemática; una publica almacenada en la base de datos del sistema y una privada que se envía al dispositivo móvil de cada usuario, permitiendo así mediante la ejecución de un protocolo de desafío respuesta, basado en el cifrado de una cadena de caracteres, confirmar la identidad de la persona para posteriormente permitirle el acceso a los recursos de la plataforma web. Ésta se integra mediante una arquitectura basada en servicios web, ya que facilita el intercambio de información con cualquier otro desarrollo, sin importar el lenguaje en que este programado y su implementación en cualquier tipo de interfaz o dispositivo.

I. INFORME DE INVESTIGACION

1.1 Estado del arte

En la actualidad, tras el impacto generado por el uso masivo de sistemas informáticos y la implementación de nuevas tecnologías a nivel global, sumado al pleno auge del internet, se han generado avances significativos con respecto a la automatización de procesos y el tratamiento de la información, además de la evolución de los diferentes campos de las ciencias y la forma como se abordan los problemas del mundo contemporáneo, entre ellos, la identidad digital y la autenticación en la web.

> La identidad digital es la representación única de un sujeto involucrado en una transacción en línea. Una identidad digital siempre es única en el contexto de un servicio digital, pero no necesariamente necesita identificar de forma única al sujeto en todos los contextos. En otras palabras, acceder a un servicio digital puede no significar que se conoce la identidad de la vida real del sujeto(Grassi, Garcia, & Fenton, 2017).

Hasta el día de hoy se han adelantado múltiples estudios en esta área conforme al incremento en el uso de plataformas de e-learning y aplicaciones que vinculan las transacciones bancarias en línea, donde es una necesidad real la implementación de rigurosos sistemas de autenticación y validación de la identidad de los usuarios, con el fin de evitar accesos fraudulentos o malintencionados. Desde Métodos de autenticación simple como la implementación de usuario y contraseña, hasta validación de la identidad por medio de análisis biométrico en la dinámica de tecleo, siendo “la forma más transparente de aprovecharlo es recopilar información de tiempo sobre los datos que los usuarios escriben para iniciar sesión en el sistema, es decir, nombre de usuario y contraseña” (Peacock, Ke, & Wilkerson, 2004).

En la Universidad de California en Berkeley Estados unidos, se ha ido un poco más allá realizando estudios acerca de la usabilidad y seguridad de autenticación mediante ondas cerebrales. “El tener un pensamiento pasajero en lugar de escribir una contraseña, puede constituir un método de autenticación que promete numerosas ventajas de seguridad, incluida la resistencia a los ataques de diccionario y la suplantación de identidad” (Chuang, Nguyen, Wang, & Johnson, 2013).

Por supuesto los procesos electorales no han sido la excepción en materia de modernización, esto debido a la incursión de medios informáticos que dan paso a la incorporación de métodos distintos en el marco de la administración electoral e impulsando el voto electrónico (e-vote) a través de medios tecnológicos con conexión a internet, como una alternativa a los sistemas de votación convencionales.

> La ventaja de esta modalidad es que un ciudadano puede emitir su voto aun cuando se encuentre distante de su lugar de residencia. Esta característica podría aumentar la participación de los ciudadanos en las elecciones, la que, como es sabido, tiende en la actualidad a disminuir drásticamente en casi todo el mundo (Pesado et al., 2008).

Una de las dificultades presentes en la implementación de dicho sistema, es la correcta identificación y autenticación de los votantes, asimilando que “La identidad digital de cada persona, es entendida como los elementos de hardware o software que permiten que una persona obtenga los permisos para acceder a determinados recursos de información o físicos”(Pareja, Pedak, Gómez, & Barros, 2017). Y Debido a que “el procedimiento individual de votación por Internet no puede ser supervisado por las autoridades u observado de la manera tradicional”(Madise & Martens, 2006). Se han desarrollado soluciones que van desde el uso de tarjetas electrónicas y contraseñas de un solo uso (OTP- one time password), hasta métodos que involucran la autenticación biométrica.

Estonia, un país reconocido mundialmente por ser pionero en materia de gobierno electrónico (e-Governement), debido a que fue el primer país en implementar el voto por internet a nivel nacional desde el 2005 y a los avances que ha presentado en este campo a través de los años.

> De hecho, estonia ha sido altamente clasificada en las comparaciones internacionales que miden los desarrollos de la sociedad de la información, no solo entre Europa central , también entre los estados miembros originales de la unión europea y otros países líderes en tecnología de la información y la comunicación (TIC) (Kalvet, 2012).

Uno de los factores que han influido en su éxito, es la implementación de la tarjeta nacional de identidad electrónica (ID card), que es un documento que incluye mecanismos electrónicos de autenticación y autorización.

> Las tarjetas de identificación nacionales de Estonia son tarjetas inteligentes con la capacidad de realizar funciones criptográficas. Por medio del uso de lectores de tarjetas y software de clientes, los estonios pueden autenticarse en sitios web (a través de la autenticación de clientes TLS) y realizar firmas legalmente vinculantes en los documentos. Las tarjetas se utilizan habitualmente para la banca en línea y para acceder a servicios de gobierno electrónico(Springall et al., 2014).

Todo esto mediante la implementación de “tecnología PKI (Public Key Infrastructure) e incorporando dos certificados: uno para autenticación y otro para firmas digitales. Para el uso de las claves privadas es necesario usar un código PIN”(Pareja et al., 2017). Permitiendo a las personas emitir su voto sin la necesidad de desplazarse a una mesa electoral, únicamente requiere de un lector de tarjetas y conexión a internet. Este documento es emitido por el estado y de carácter obligatorio. Además de este, existen otros mecanismos válidos para la autenticación de identidad como lo es Mobile-ID, se refiere a una tarjeta SIM de identidad Digital presente en los

teléfonos móviles, que permite realizar pagos, transacciones, proporcionar firmas digitales y participar en la votación electrónica. “La experiencia de Estonia demuestra que el uso de la biometría no es necesario para crear un ecosistema seguro en un país con alfabetización digital avanzada”(Pareja et al., 2017).

En España, la identidad digital ha estado presente dentro de las políticas públicas relacionadas con el desarrollo de nuevas estrategias para la administración de la información en un entorno informático y el desarrollo de sistemas seguros de gobierno electrónico.

> Entre las medidas tomadas se estableció el desarrollo del Documento Nacional de Identidad electrónico (DNI-e) y el establecimiento de un marco legal para la firma digital. Este chip, además de los datos biométricos e identificación, contenía dos certificados digitales. Desde su primera implementación en 2006 se ha ido sustituyendo a los antiguos DNI sin chip por los nuevos DNI-e, hasta cubrir hoy en día a prácticamente toda la población española, que está obligada a portarla(Pareja et al., 2017).

En España se encuentra una de las empresas líder en soluciones seguras de voto electrónico y modernización electoral (Scytl), consolidada en el mercado del software electoral. Países como Australia, Francia, Suiza y Brasil han recurrido a sus servicios.

A continuación, se presenta una tabla con las características más importantes de la implementación de sistemas de voto electrónico.

Tabla 1 Características voto electrónico en diferentes países.

País	Generalidades del voto electrónico
Estonia	*Voto por internet por medio de la Implementación de Tarjeta ID electrónica y Mobile ID.* *+1'000.000 tarjetas activas.* *+200.000 Mobile-Id activas.* *+1´000.000 transacciones por internet a diario.*
Australia	*Implementación tecnología Scytl que permite el voto por internet.* *Se realiza solicitud voto electrónico y se recibe Pin de 6 dígitos.* *+280.000 votos emitidos electrónicamente 2015.*
Suiza	*Voto por medio de plataforma nacional y por correo.* *Confirmación electrónica del voto.* *Actualmente suspendido por problemas de seguridad.* *De 2013 a 2014 aumento canales votación en línea.*
India	*Máquinas electrónicas de votación.* *Gujarat es pionero en la introducción del voto por internet.* *Sistema adhaar para la identificación digital.*
Francia	*Implementación de la huella dactilar integrada en una tarjeta (Smart card).*
Estados Unidos	*Máquina electrónica de registro automático (DRE).* *Voto remoto SERVE (2004).* *Tecnología Scytl (2012).* *Actualmente Estados Unidos lanzó un programa piloto basado en tecnología Blockchain.*

De la tabla anterior se puede concluir que el referente en materia de voto electrónico a gran escala, debido a su implementación en todo el país mediante la identificación digital, es Estonia.

A nivel Latinoamérica generalmente los sistemas informáticos de validación y autenticación de identidad digital, se basan mayormente en la firma electrónica y el registro de datos biométricos. Brasil es uno de los pocos países en el mundo que ha implementado un sistema electoral electrónico. El votante digita el número que identifica al candidato de su elección y después de que se muestra la foto de este, se procede a confirmar el voto.

> Varias tecnologías han sido desarrolladas en Brasil, entre ellas, se resalta el desarrollo de urnas biométricas que procesaban el voto a partir de la identificación biométrica del elector, con lo cual Brasil se posicionó como el país a la vanguardia tecnológica de los procesos electorales en todo el mundo(Fandiño Casas, 2012).

Perú ya incorpora la tarjeta de identificación electrónica para la realización de trámites y servicios estatales, acreditando de manera presencial y no presencial al titular de dicho documento. Hasta la fecha se han emitido más de seis millones de DNI electrónico en el país.

En Chile se adoptaron políticas para la digitalización de tramites por medio de la implementación de clave única, asociada al registro civil y una alianza con los integradores de la tecnología Open ID, un sistema de autenticación digital descentralizado con el que un usuario puede identificarse en la web.

Colombia cuenta con muchos avances en materia de automatización en los procesos de voto electrónico y autenticación digital. En el país aún utiliza los mecanismos presenciales de identificación y ejecución del derecho electoral por lo que cuenta con dos instituciones que intervienen en el desarrollo de los procesos electorales: el Consejo Nacional Electoral (CNE) y la Registraduría Nacional del Estado Civil, que tienen entre sus funciones ejercer la inspección y vigilancia de la organización electoral, velar por el cumplimiento de las normas sobre partidos políticos.

El estado actual de la automatización de todo el proceso electoral en Colombia ha establecido avances en materia del Censo electoral (ciudadanos que cumplen 18 años), en la inscripción automatizada de candidatos y en la designación de jurados, pero aún queda mucho por avanzar con respecto a la vinculación de las TIC (tecnologías de la Información y las Comunicación) en procesos electorales, autenticación e identificación digital a pesar de que se han realizado algunas investigaciones y pruebas piloto por parte de algunas entidades del estado e instituciones educativas. Por ejemplo, en Bogotá se realizó una prueba piloto de voto electrónico para la elección de representantes estudiantiles. Se implemento prototipo blockchain, sin embargo, en materia de autenticación no se profundizo, recurriendo únicamente a una validación del código de los estudiantes.

1.2 Línea de investigación

La línea de investigación en la cual se establece el proyecto se denomina *software, sistemas emergentes y nuevas tecnologías* debido a que está enmarcada dentro del área de la ingeniería, la innovación tecnológica y la materialización de ideas que den respuesta a las necesidades del mundo contemporáneo y generen un avance. De igual manera que contribuyan a la solución de problemas, optimización de las funciones o procesos en diferentes campos como la industria, la política, la medicina, el medio ambiente, etc. Mediante la implementación de herramientas computacionales y metodologías que permitan generar soluciones eficientes, con un menor gasto de recursos, representando un impacto en la sociedad actual.

1.3 Planteamiento del problema y pregunta de investigación

El creciente avance tecnológico y la influencia de los sistemas en el mundo actual, ha llevado a la automatización de diferentes procesos que se realizaban de forma manual, entre los que se encuentra la gestión electoral y por ende la ejecución del voto. La universidad de Cundinamarca, lleva a cabo este proceso de manera convencional, basada en la distribución de tarjetones, urnas físicas y la realización del escrutinio a cargo de un comité electoral que realiza el conteo de votos dentro de los cinco (5) días siguientes al día de la votación, como se describe en el acuerdo por medio del cual se reglamenta la elección de los representantes de los estudiantes ante el consejo superior, consejo académico y consejo de facultad, evidenciando la ausencia de un sistema de información que administre dicho proceso, además de procedimientos que requieren una mayor cantidad de recursos y tiempo, sin mencionar que los participantes de la jornada deben desplazarse al lugar establecido para ejercer su derecho al voto. Cabe destacar que otro de los procesos que se llevan a cabo en la institución es la elección de los representantes de los graduados que está a cargo únicamente del rector en supervisión del consejo superior de la universidad y no de manera democrática.

Lo anterior se suma a la desconfianza que generan los resultados de la implementación de un sistema de voto por internet (i-vote) y la seguridad en materia de autenticación e identificación de las personas habilitadas para participar en dicho proceso. Esto Debido a que el voto por internet se puede realizar desde cualquier parte con una conexión a internet, sin la supervisión de alguna autoridad, nos conduce a plantear la siguiente pregunta en la que se basa la investigación: ¿Cómo asegurar la identidad de una persona a través de un entorno web, en un medio de votación no controlado?

1.4 Objetivo general y objetivos específicos

OBJETIVO GENERAL:

Desarrollar un módulo de autenticación que administre y gestione el acceso a la plataforma de voto electrónico de la universidad de Cundinamarca.

OBJETIVOS ESPECÍFICOS:

- Realizar el levantamiento de requerimientos del módulo de autenticación.
- Diseñar la estructura del módulo (UML).
- Implementar la criptografía de clave asimétrica.
- Crear un repositorio de credenciales para el acceso a la plataforma de votación.
- Realizar pruebas de funcionamiento del módulo.
- Integrar el módulo de autenticación a la plataforma de i-vote.
- Analizar el impacto social del módulo.

1.5 Alcance e impacto del proyecto

La Universidad de Cundinamarca es una entidad pública comprometida con la preparación de profesionales altamente calificados, resaltando en ellos los principios éticos y humanos, en respuesta a las necesidades actuales del sector laboral, económico, político y social de Colombia, además de impulsar el conocimiento, la investigación y la interacción estudiantil, ratificando su apoyo a las ideas innovadoras que generen un beneficio a la comunidad. Actualmente carece de un sistema que permita gestionar de manera óptima los procesos electorales que

se realizan dentro la institución, por ejemplo, la elección de representantes estudiantiles, que se realiza de la manera convencional, basada en procesos manuales y que requieren de recursos y organización previa por parte de la administración de la universidad.

Por lo anterior es preciso afirmar que la elaboración del proyecto “Sistema de voto electrónico (Modulo autenticación)” es un paso hacia la modernización y agilización de los diferentes procesos electorales que se llevan a cabo en la institución, mediante el desarrollo e implementación de una solución basada en el uso de la tecnología y los sistemas de información, permitiendo ejecutar y administrar de manera más eficiente la jornada democrática, destacando la alternativa que se brinda a las personas de poder ejercer el voto desde cualquier lugar que tenga una conexión a internet e Incentivando la participación de la comunidad educativa en los temas relevantes en el marco de la gestión y el plan de desarrollo de la universidad, planteando las bases para lo que se denomina “gobierno electrónico” institucional, sin mencionar los beneficios en materia de seguridad, procesamiento de datos y confiabilidad de los resultados. A esto se suma el diseño y construcción de un módulo de autenticación independiente que pueda ser aprovechado en diferentes proyectos a futuro. Además del aporte que se hace al cumplimiento de uno de los objetivos de desarrollo (ODS), que nos habla de promover sociedades, justas, pacificas e inclusivas, más específicamente como una herramienta que aporte a la reducción de la corrupción y soborno en todas sus formas.

1.6 Metodología (De investigación y De Desarrollo)

La metodología de investigación propuesta para el proyecto es la mixta, debido a que “esta implica la combinación de los enfoques cuantitativos y cualitativos” (Hernández Sampieri, Fernández-Collado Baptista Lucio McGraw-Hill México, & Edición, 2006). Mediante el método cuantitativo basado en la información detallada y los principios teóricos, además del análisis de resultados experimentales, implicando el uso de herramientas informáticas para ello, indispensables en el desarrollo del sistema y el método cualitativo más enfocado en el estudio de fenómenos que permitan fortalecer el planteamiento de una teoría mediante la evaluación e interpretación de información, se contribuye a la recolección y análisis de información de diferentes fuentes y autores con diferentes enfoques, que hayan incursionado en los temas relacionados con la temática del proyecto permitiendo establecer las bases teóricas de la investigación, una mejor comprensión del problema y la generación de ideas innovadoras.

Para el diseño y desarrollo del módulo de autenticación se establece el uso de elementos de la metodología ágil basada en SCRUM, debido a que este “es un marco dentro del cual puede emplear diversos procesos y técnicas” (Schwaber & Sutherland, 2011). Además de que ha sido ampliamente implementado en desarrollos de software y hardware debido a los beneficios que este ofrece, entre los que se destacan la flexibilidad, adaptación, organización, reducción de riesgos, incremento en la productividad y la calidad de los resultados. La forma en que se adapta esta metodología al desarrollo del módulo, se basa en el establecimiento de objetivos claros y alcanzables en un tiempo determinado por el equipo de trabajo, que permitan evidenciar avances en el desarrollo del proyecto además de generar un plan estratégico basado en dicho progreso, con una respuesta al cambio y a los problemas que se puedan presentar, además de la retroalimentación en cada uno de los procesos presentes en la ejecución e incremento del software, analizando la

forma de trabajo, el progreso y las falencias que se presentaron, con el objetivo de ampliar de manera continua la productividad.

La organización y jerarquización de las tareas se realizará basándonos en el modelo en cascada para el proceso de desarrollo, por lo que inicialmente se realiza una definición de requerimientos, seguido del diseño y desarrollo del módulo, para luego proceder a la implementación e integración del módulo.

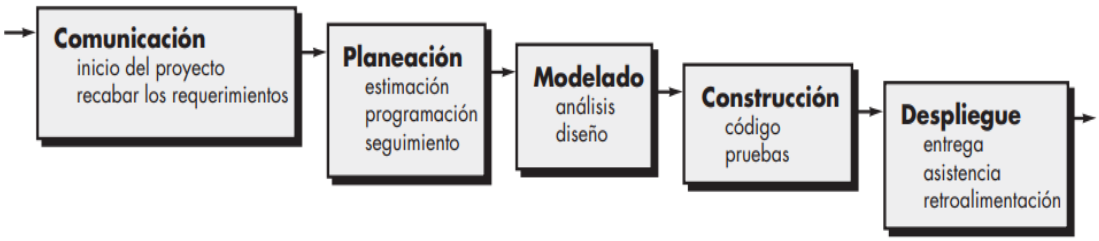


Figura 1 Modelo en cascada

Tomado de Ingeniería del software un enfoque práctico (Fandiño Casas, 2012).

De igual manera la adaptación del marco de garantía de autenticación de entidad, Recomendación UIT-T X.1254 del 2013 establecido por la Unión Internacional de Telecomunicaciones. Este documento especifica un marco para la gestión de los niveles de garantía, proporciona directrices sobre las tecnologías de control que se deben utilizar para mitigar las amenazas a la autentificación, sobre la base de la evaluación de riesgos, orienta sobre la correspondencia entre los cuatro niveles de garantía y otros planes de garantía de autentificación, además de facilitar orientación para el intercambio de resultados de autentificación basados en los cuatro niveles de garantía.

1.7 Marcos de Referencia

1.7.1 Marco teórico

1.7.1.1 Seguridad

La seguridad de la información se define como "proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados"(Legal Information Institute, 2014). Por lo que es una necesidad la implementación de normas, métodos y técnicas de confianza que permitan salvaguardar los datos almacenados en un sistema informático de quienes tratarían de usarlos de manera indebida, además con el objetivo de preservar:

- Integridad: Garantía de que los datos no han sido alterados en su contenido o destruidos, en pocas palabras la autenticidad y precisión de la información
- Confidencialidad: La información está únicamente al alcance de las personas, entidades o mecanismos autorizados
- Disponibilidad: La información debe estar disponible en el momento oportuno, para los usuarios autorizados cuando la necesiten (Dussan, 2006).

La autenticación se puede considerar como parte de un método de control de acceso, la mayoría de las ocasiones esto se complementa con otras partes de un sistema(Romero Castro et al., 2018). Los sistemas de información se pueden ver amenazados por factores de diferente índole (personas, maquinas o sucesos), se clasifican en los siguientes grupos: a) Interrupción: corte en la prestación de un servicio, b) Interceptación: copia de la información transmitida, c) Modificación o Falsificación: accede y modifica información transmitida, d) Generación: fabricación de mensaje engañando al receptor (Purificacion, 2010).

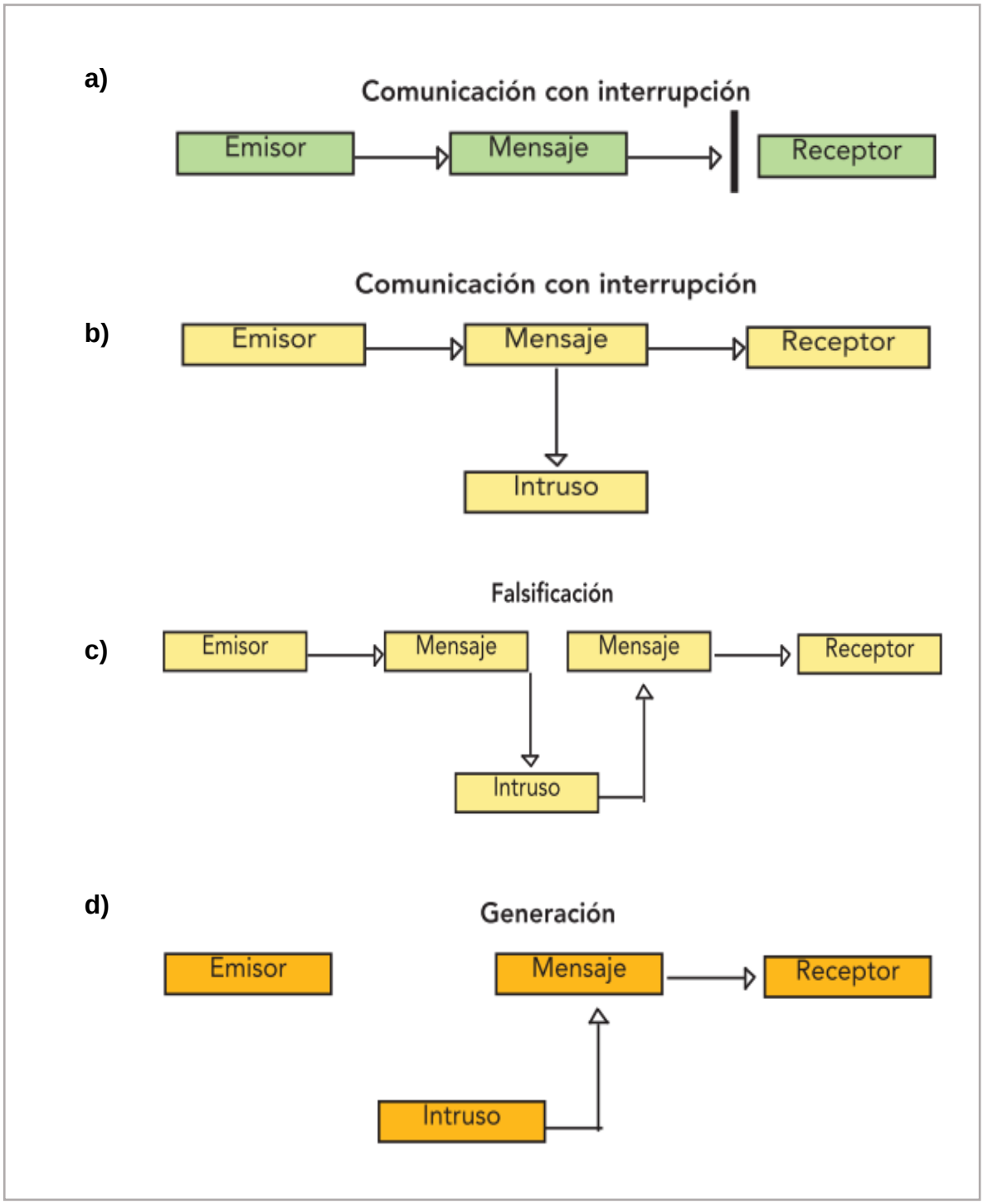


Figura 2 Amenazas en la comunicación de datos

Fuente: Interrupción, interceptación, falsificación y generación (Paredes, 2006).

1.7.1.2 Identificación

La identificación, es simplemente una afirmación de quiénes somos, como persona o a través de un sistema informático.(Andress & Winterfeld, 2014). Por lo tanto, es el usuario se da a conocer al sistema, además de distinguir un individuo de otro.

Tabla 2 Verificación y validación de identidad

Verificación de identidad	Validación de identidad
• Existe registro de esa persona. • Coinciden los datos con el registro de una persona.	• Verifica si la información representa datos reales. • Es una capa adicional de mitigación de riesgos.

Fuente: *(Branddocs, 2018)*

1.7.1.3 Autenticación

El proceso de autenticación constituye uno de los principios fundamentales de la seguridad en un sistema de información, debido a que este permite determinar si un usuario que requiere el acceso a un sistema es quien dice ser. En un sentido de seguridad de la información, el conjunto de métodos que utilizamos para establecer un reclamo de identidad como verdadero (Andress & Winterfeld, 2014).

La autenticación electrónica es el proceso para establecer la confianza en las identidades de los usuarios presentadas electrónicamente a un sistema de información, esta presenta un desafío técnico cuando este proceso involucra la autenticación remota de personas individuales a través de una red abierta, con el propósito del gobierno electrónico y el comercio (Burr et al., 2013).

El paradigma clásico para los sistemas de autenticación identifica tres factores como la piedra angular de la autenticación: a) algo que se sabe, b) Algo que se tiene, c) Algo que se es (aquello inherente a la entidad) (Burr et al., 2013).

a) **Autenticación basada en conocimiento** también como conocido KBA (Knowledge-Based Authentication), es un factor muy común y el más débil porque si la información de la que depende el factor está expuesta, puede anular la singularidad de nuestro método de autenticación. Este método incluye contraseñas, PIN, frases de contraseña o casi cualquier elemento de información que una persona pueda recordar (Andress & Winterfeld, 2014).

b) **Autenticación basada en la posesión** depende de algo que esté en poder de los usuarios del sistema, por lo general algo físico, un elemento o dispositivo, aunque este factor también puede extenderse a algunos conceptos lógicos. Podemos ver dichos factores en uso general en forma de tarjetas de cajero automático, tarjetas de identidad emitidas por el estado o por el gobierno federal. o tokens de seguridad basados en software (Andress & Winterfeld, 2014).

c) **Autenticación biométrica** es un factor basado en los atributos físicos relativamente únicos de un individuo, a menudo referidos como biométricos. Este factor puede basarse en atributos simples, como la altura, el peso, el color del cabello o el color de los ojos, pero estos no pretenden ser lo suficientemente únicos como para hacer identificadores muy seguros, lo que lo hace un factor más seguro y confiable, ya que falsificar o robar una copia del identificador físico es una tarea algo más difícil, aunque no imposible (Andress & Winterfeld, 2014).

Las buenas prácticas señalan que, para operaciones de alto riesgo, se debe utilizar una combinación de al menos dos de estos elementos lo que se denomina autenticación multifactor, proporcionando un método más confiable para verificar la verdadera identidad, ya que confiar en una única fuente de datos puede generar brechas de seguridad (Pareja et al., 2017).

Elementos de autenticación

Para autentificarse, un usuario proporciona en general al menos 2 elementos:

- Su identificador que permite su definición.
- Uno o más elementos que permiten garantizar la propia autenticación.

Tabla 3 Siete elementos de autenticación

Tipo	Descripción
El identificador y la contraseña	Simple, robusto, incluso rústico, su más grande defecto es que el nivel de seguridad depende directamente de la complejidad de la contraseña.
El identificador y la contraseña OTP (One-Time Password)	El OTP permite asegurar el uso de la contraseña en la red. En efecto, con un sistema OTP el usuario posee un calculador especializado que le proporciona bajo petición una contraseña. Esta contraseña es válida solo durante una duración limitada, y para una única utilización.
Los certificados PKI sobre tarjeta inteligente o token USB	El identificador es un certificado público que es firmado y en consecuencia garantizado por una autoridad de certificación reconocida. El usuario debe proporcionar un secreto para poder utilizar los distintos elementos criptográficos: “el código PIN de su tarjeta o su tecla USB”. Esta
Tecla “Confidencial Defensa”	Se trata de una declinación particular del ejemplo anterior. Es en general una llave multifunciones: almacenamiento de certificado X.509, almacenamiento de datos, recurso criptográfico etc.
El identificador y la contraseña sobre una tarjeta inteligente	El almacenamiento del identificador y la contraseña sobre una tarjeta inteligente permite suplementar la protección del proceso de autenticación. La contraseña puede así ser muy compleja y cambiada regularmente de manera automática y aleatoria. Sin la tarjeta, y sin su código PIN, no se puede acceder a la contraseña.
Biométrica	La autenticación por biométrica se basa en la verificación de un elemento del cuerpo del usuario (generalmente la huella dactilar). Puede basarse en un distribuidor central, en el puesto de trabajo o en una tarjeta inteligente para almacenar los datos biométricos del usuario.
La definición sin contacto	El RFID es una tecnología que hoy se despliega en los proyectos de Identificación/Autenticación. Un chip RFID es insertada en una tarjeta y lleva un número de identificación. Este número se asocia a continuación a un usuario en un sistema informático. El RFID pasivo o HID, que supone que la tarjeta no posee alimentación propia. El RFID activo se basa en los protocolos de comunicación RFID, pero asocia a la carta una alimentación propia.

Fuente: (Evidian, 2015).

Autenticación multifactor (MFA)

La autenticación multifactor (MFA) es un sistema de seguridad que requiere más de una forma de autenticación para verificar la legitimidad de una transacción (searchdatacente, 2014).

El objetivo de la MFA es crear una defensa por capas y hacer que sea más difícil para una persona no autorizada acceder a un objetivo, como una ubicación física, un dispositivo de cómputo, una red o una base de datos. Si uno de los factores se ve comprometido o se rompe, el atacante todavía tiene al menos una barrera más que romper antes de ingresar con éxito en el objetivo (searchdatacente, 2014).

Tabla 4 Autenticación multi factores

Ejemplos de sistema de autenticación a 1 factor:	• *Identificador + contraseña (elemento que se sabe),* • *Definición sin contacto (elemento que se posee),* • *Biométrica o identificador + biométrica (elemento que es).*
Ejemplos de sistema de autenticación a 2 factores:	• *Tarjeta inteligente + código PIN (elementos que se posee Y que se sabe),* • *Tarjeta inteligente + biométrica (elemento que se posee Y que es),* • *Biométrica + contraseña (elemento que es Y que se sabe).*
Ejemplo de sistema de autenticación a 3 factores:	• *Tarjeta inteligente + cifra PIN + biométrica (elementos que se posee Y que se sabe Y que es).*

Fuente: (Evidian, 2015).

La multiplicación del número de factores de autenticación aumenta el nivel de seguridad general, pero supone algunos retos como la administración del ciclo de vida de cada factor, la usabilidad del sistema, los costes de elementos electrónicos como tarjetas, lectores o sensores biométricos y la carga del servicio de ayuda al usuario (Evidian, 2015).

1.7.1.4 Criptografía

La criptografía es la disciplina que se encarga del estudio de códigos secretos o llamados también códigos cifrados (en griego kriptos significa secreto y gráhos, escritura) (Fernández, 2004). La encriptación o también conocido como cifrado, es un procedimiento en el que se busca que la información sea ilegible, ya aplicado este procedimiento la información es inservible para cualquier persona que no sea la autorizada, aunque el mensaje sea interceptado (Romero Castro et al., 2018).

En su clasificación dentro de las ciencias, la criptografía proviene de una rama de las matemáticas, que fue iniciada por el matemático Claude Elwood Shannon en 1948, denominada: Teoría de la Información (Paredes, 2006).

Para garantizar la confidencialidad, podría asegurarse el medio de transmisión o bien la información; la Criptografía utiliza este último enfoque, encripta la información de manera que, aun cuando se encuentre disponible para cualquiera, no pueda utilizarla, a menos que alguien autorizado la descifre (Marrero Travieso, 2003).

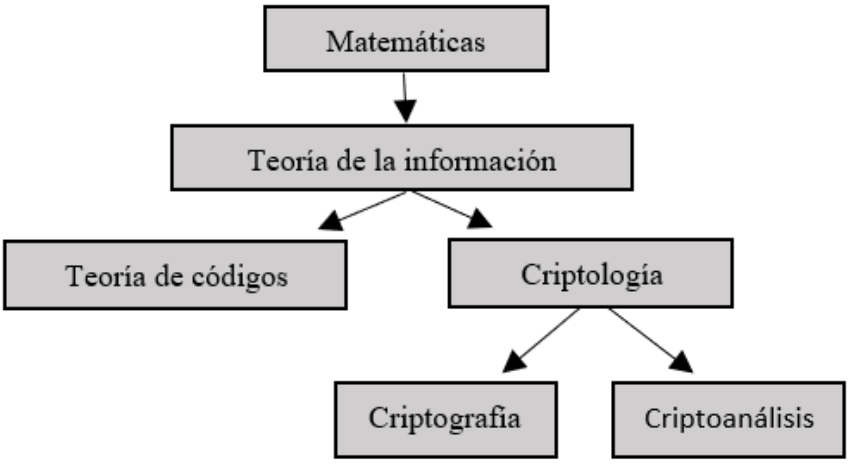


Figura 3 Origen de la Criptografía

Fuente: (Paredes, 2006).

La criptografía se puede clasificar históricamente en dos: La criptografía clásica y la criptografía moderna. La criptografía clásica es aquella que se utilizó desde antes de la época actual hasta la mitad del siglo XX. También puede entenderse como la criptografía no computarizada o mejor dicho no digitalizada (Paredes, 2006).

Se puede decir que la criptografía moderna se inició después de tres hechos: el primero fue la publicación de la "Teoría de la Información" por Shannon; el segundo, la aparición del estándar del sistema de cifrado DES (Data Encryption Standard) en 1974 y finalmente con la aparición del estudio realizado por Whitfield Diffie y Martin Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifrado, denominado cifrado de llave pública en 1976 (Paredes, 2006).

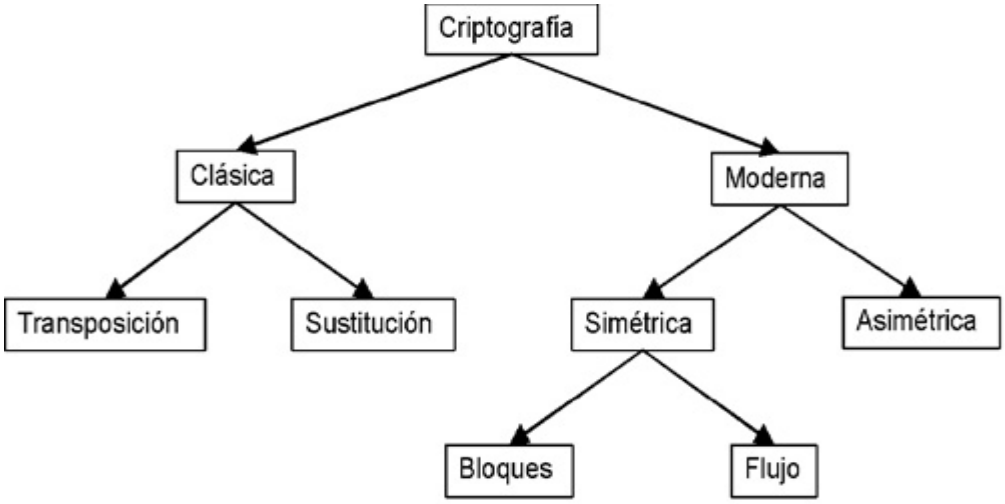


Figura 4 Clasificación de la criptografía

Fuente: (Paredes, 2006).

Los objetivos principales de la encriptación y cifrado de datos son: La confidencialidad que consiste en que la información sólo puede ser accedida por su legítimo dueño o destinatario, la autentificación quiere decir que el emisor y el receptor son los que pueden confirmar la identidad, finalmente la integridad de la información significa que no debe ser posible que sea alterada en caso de que sea interceptada la información.

La criptografía se divide en dos grandes ramas, la Criptografía de clave privada o simétrica y la Criptografía de clave pública o asimétrica.

Criptografía simétrica

El cifrado simétrico (o criptografía de clave privada) es un método de ofuscación que permite el transporte seguro de datos a través de canales de comunicación inseguros. Por ejemplo, para comunicarse de forma segura, Alice y Bob primero acuerdan el algoritmo de cifrado y una clave secreta. Más tarde, cuando Alice quiere enviar algunos datos a Bob, usa la clave secreta para cifrar los datos. Bob usa la misma clave para descifrarlo (Ristić, 2015).

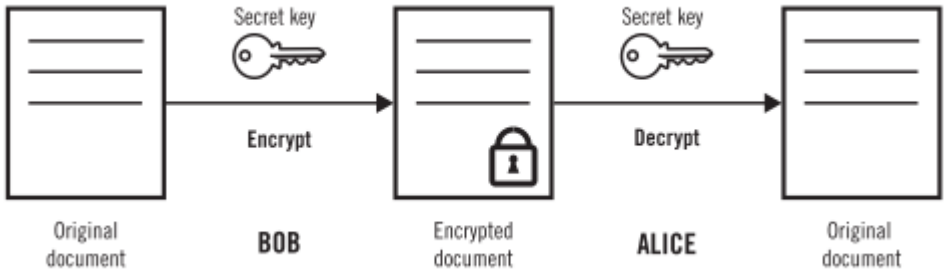


Figura 5 Cifrado Simétrico

Fuente: (Ristić, 2015).

Se puede indicar varios ejemplos de cifrado simétrico:

- **DES:** (Data Encryption Standard): fue el primer estándar de cifrado que será publicado por el NIST (instituto nacional de Estándares y Tecnología),
- **AES:** (advanced Encryption Standard): también conocido como el algoritmo Rijndael (pronunciado como lluvia muñeca),
- **3DES:** Triple DES simplemente extiende el tamaño de clave de DES mediante la aplicación del algoritmo de tres veces en sucesión con tres llaves diferentes (Medina & Miranda, 2015).

Longitud de clave: Un espacio de claves grande es una condición necesaria, pero no suficiente, para un cifrador simétrico seguro. Este debe ser además resistente ante ataques de fuerza bruta y de tipo analítico (Franchi, 2012).

Tabla 5 Estimación de Seguridad Clave Simétrica

Largo de clave	Estimación de seguridad
56-64 bits	Corto plazo: horas o días.
112-128 bits	Largo plazo: décadas en ausencia de computadoras cuánticas.
256 bits	Largo plazo: décadas aun con computadoras cuánticas.[1]

Fuente: (Franchi, 2012)

Criptografía asimétrica

La criptografía de clave asimétrica, también conocida como criptografía de clave pública, utiliza dos claves: una clave pública y una clave privada. La clave pública se utiliza para cifrar los datos enviados desde el remitente al receptor, las clave privada se utilizan para descifrar los datos que llegan al extremo receptor (Andress & Winterfeld, 2014).

Existe una relación matemática especial entre estas llaves que permite algunas funciones útiles. Si encripta datos utilizando la clave pública de alguien, solo su clave privada correspondiente puede descifrarla (Ristić, 2015).

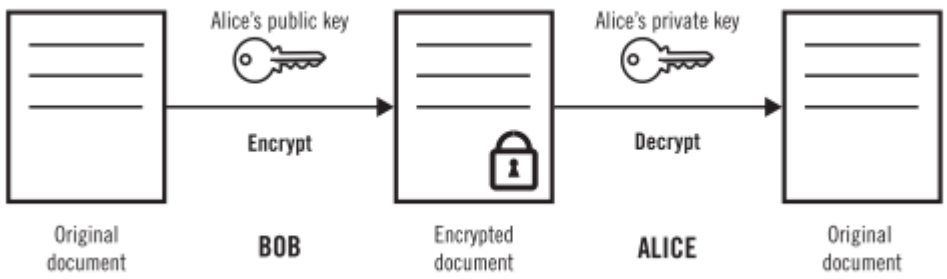


Figura 6 Cifrado Asimétrico

Fuente: (Ristić, 2015).

Parte del funcionamiento de la criptografía de clave pública se basa en que, todo aquel que quiera comunicarse con alguien, debe poseer su clave pública (Casado Santos, 2017).

Algoritmos de clave asimétrica

Algunos ejemplos de criptografía asimétrica más representativos son RSA y Curvas Elípticas:

- **RSA:** El algoritmo RSA, llamado así por sus creadores Ron Rivest, Adi Shamir y Leonard Adleman, es un algoritmo asimétrico utilizado en todo el mundo, incluso en el protocolo Secure Sockets Layer (SSL), que se utiliza para asegurar muchas transacciones comunes como Web y e- tráfico de correo RSA se creó en 1977 y sigue siendo uno de los algoritmos más utilizados en el mundo hasta el día de hoy (Andress & Winterfeld, 2014). Se basan en la dificultad de factorizar números enteros de gran tamaño (Franchi, 2012) .

- **ECC:** La criptografía de curva elíptica (ECC) es una clase de algoritmos criptográficos, aunque a veces se la denomina como un algoritmo en sí mismo. ECC lleva el nombre del tipo de problema matemático en el que se basan sus funciones criptográficas. Tiene varias ventajas sobre otros tipos de algoritmos entre los que se destaca una mayor fuerza criptográfica con claves más cortas que muchos otros tipos de algoritmos, lo que significa que podemos usar claves más cortas con ECC mientras mantenemos una forma de cifrado muy segura. También es un tipo de algoritmo muy rápido y eficiente, que nos permite implementarlo en hardware con un conjunto de recursos más restringido, como un teléfono celular o dispositivo portátil, más fácilmente (Andress & Winterfeld, 2014).

Los algoritmos de clave pública requieren operandos y claves de gran tamaño. Cuanto más grande son estos más seguros se vuelven los algoritmos. Un parámetro de comparación entre los distintos algoritmos es el nivel de seguridad. Se dice que un algoritmo tiene un nivel de seguridad de n bits si el ataque requiere 2^n pasos. Para los algoritmos de clave simétrica esta relación es natural, dado que con n bits tenemos un espacio de claves de 2^n (Franchi, 2012).

Tabla 6 Largo de Claves y Nivel de Seguridad

Algoritmo	Criptosistema	Nivel de Seguridad (bits)			
		80	128	192	256
Factorización de enteros	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Logaritmo discreto	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Curvas Elípticas	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Clave simétrica	AES, 3DES	80 bit	128 bit	192 bit	256 bit

Fuente: (Franchi, 2012)

Estándares ECC

Los hallazgos teóricos relacionados con RSA o ECC no se pueden usar directamente, ya que es necesario definir estructuras y procedimientos de datos para administrar la información (Gayoso, Hernandez, & Sanchez, 2010). Actualmente hay tres aplicaciones inmediatas para ECC en criptografía:

1. ECDH (Elliptic Curve Diffie-Hellman).
2. ECDSA (Elliptic Curve Digital Signature Algorithm).
3. ECIES (Elliptic Curve Integrated Encryption Scheme).

ECIES es el esquema de cifrado más conocido en el ámbito de ECC, que es una de las tendencias criptográficas actuales más interesantes.

- Acuerdo clave (KA): función utilizada para la generación de un secreto compartido por dos partes,
- Función de derivación de clave (KDF): mecanismo que produce un conjunto de claves a partir de material de claves y algunos parámetros opcionales,

- Cifrado (ENC): algoritmo de cifrado simétrico,
- Código de autenticación de mensajes (MAC): datos utilizados para autenticar mensajes,
- Hash (HASH): función de resumen, utilizada dentro de las funciones KDF y MAC (Gayoso et al., 2010).

1.7.2 Marco legal

El proyecto se desarrolla en el marco de la legalidad vigente en la constitución nacional de Colombia. En él se establecen puntos importantes con respecto a la privacidad de la información, al tratamiento y protección de datos, el derecho de autor y la propiedad intelectual dentro del ecosistema de las TIC, el software y los sistemas computacionales, en el marco jurídico y constitucional de la investigación y la ejecución del proyecto:

La ley Estatutaria 1581 (2012). La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma (Ley 1581, 2012).

Ley 527 DE 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones (Ley 527, 1999).

Ley 1341 de 30 de julio de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (Ley 1341, 2009).

Ley 1273 de 5 de enero de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Ley 1273, 2009).

La ley 23 (1982). Regula los derechos morales y patrimoniales que la ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística o científica, esté publicada o inédita. (Ley 23, 1982).

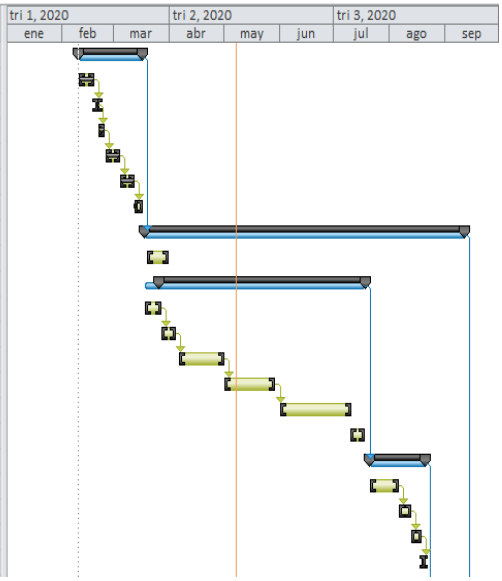
La ley Estatutaria 1266 (2008). por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones (Ley 1266, 2008).

II. DOCUMENTACIÓN DEL SOFTWARE

2.1 Plan de proyecto

A continuación, se muestra el plan de desarrollo del proyecto, diseñado en Project. Allí se establece el plan de trabajo estimado en cada una de las actividades del proyecto.

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Fase de planeacion y modelado**	**26 días**	**lun 10/02/20**	**lun 16/03/20**	
2	Analisis de requerimientos	7 días	lun 10/02/20	mar 18/02/20	
3	Casos de uso	1 día	jue 20/02/20	jue 20/02/20	2
4	Modelo entidad relacion	1,5 días	vie 21/02/20	lun 24/02/20	3
5	Diagramas de secuencia	6 días	mar 25/02/20	mar 3/03/20	4
6	Diagramas de actividades	6 días	mié 4/03/20	mié 11/03/20	5
7	Diagrama de clases	3 días	jue 12/03/20	lun 16/03/20	6
8	**Fase de Desarrollo**	**128 días**	**mié 18/03/20**	**vie 11/09/20**	**1**
9	Creacion base de datos postgres	8 días	jue 19/03/20	lun 30/03/20	
10	**Aplicación movil**	**82 días**	**jue 26/03/20**	**dom 19/07/20**	
11	Generacion de llaves	7 días	mié 18/03/20	jue 26/03/20	
12	Cifrado y Descifrado	6 días	vie 27/03/20	vie 3/04/20	11
13	Registro de usuarios	19 días	lun 6/04/20	jue 30/04/20	12
14	Correo de verificacion	20 días	vie 1/05/20	jue 28/05/20	13
15	Incorporacion FCM	30 días	lun 1/06/20	vie 10/07/20	14
16	Validaciones	6 días	vie 10/07/20	vie 17/07/20	
17	**Servicios web**	**23 días**	**mar 21/07/20**	**jue 20/08/20**	**10**
18	Incorporacion FCM web	12 días	mar 21/07/20	mié 5/08/20	
19	Inicio de sesion	5 días	jue 6/08/20	mié 12/08/20	18
20	Validacion de correo	4 días	jue 13/08/20	mar 18/08/20	19
21	Validaciones	2 días	mié 19/08/20	jue 20/08/20	20
22	**Fase de pruebas**	**16 días**	**vie 21/08/20**	**vie 11/09/20**	**17**
23	Caja blanca	6 días	vie 21/08/20	vie 28/08/20	
24	Caja negra	5 días	lun 31/08/20	vie 4/09/20	
25	Correción de errores	5 días	dom 6/09/20	jue 10/09/20	
26	**Fase de Despliegue**	**30 días**	**lun 14/09/20**	**vie 23/10/20**	**8**
27	Integración a la plataforma web	10 días	lun 14/09/20	vie 25/09/20	
28	Manuales de usuario	6,5 días	lun 28/09/20	mar 6/10/20	27
29	Capacitacion	3,5 días	mar 6/10/20	vie 9/10/20	28
30	Evaluación de impacto	10 días	lun 12/10/20	vie 23/10/20	29



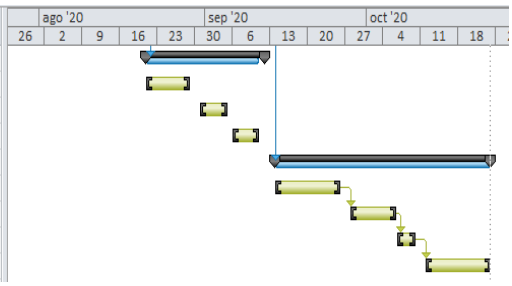


Figura 7 Plan del proyecto

2.2 Determinación de requerimientos

2.2.1 Introducción

En este documento se especifican los requerimientos del software; Sistema de Voto Electrónico para los Cuerpos Colegiados de la Universidad de Cundinamarca, desarrollado por el grupo de investigación GISTFA de la Universidad de Cundinamarca extensión Facatativá.

2.2.1.1 Propósito

El proyecto tiene como propósito el desarrollo del módulo de autenticación multifactor para el sistema de voto electrónico para los cuerpos colegiados de la Universidad de Cundinamarca, una herramienta para la automatización del proceso de identificación, ejecución, conteo y publicación de resultados de las jornadas electorales de la institución. El documento va dirigido al comité de proyectos de grado del programa de ingeniería de sistemas de la Universidad de Cundinamarca.

2.2.1.2 Ámbito del sistema

El módulo de autenticación del sistema de voto electrónico será el encargado de administrar el acceso a la plataforma electoral, por medio de la generación de un par de llaves para cada usuario y un protocolo de desafío-respuesta dispuesto para el proceso de autenticación y verificación de identidad de las personas habilitadas para participar en la jornada de votaciones.

2.2.1.3 Definiciones, Acrónimos y abreviaturas

Tabla 7 Acrónimos, abreviaturas y definiciones

Nombre	**Definición**
JAVA	Lenguaje de programación orientado a objetos.
JCA	Java Cryptography Architecture (JCA) es una especificación del lenguaje que sirven de base para las implementaciones concretas de algoritmos criptográficos y es parte del API de seguridad del lenguaje

JCE	Java Cryptography Extension (JCE) que más exactamente proporciona implementaciones para cifrado, algoritmos de encriptación, generación y concordancia de claves
Entidad	Usuario, puede ser un dispositivo, persona o servidor.
OTP	One Time Password, contraseña de un solo uso.
TLS	Abreviatura de Transport Layer, protocolo criptográfico que proporciona comunicación segura por una red.
ECC	Abreviatura de Elliptic curve cryptography, criptografía de curva elíptica.
BC	Proveedor para gestionar eficientemente los algoritmos criptográficos y soporte para la generación de llaves.

2.2.1.4 Referencias

La Especificación de requerimientos del Software se ha diseñado basándose en normas dadas por el estándar IEEE 830, 1998.

2.2.1.5 Visión General del Documento

El documento está dividido principalmente en tres partes. Inicialmente una introducción en la que se hace referencia a los conceptos generales del proyecto, el propósito de su desarrollo y la definición de algunos términos y abreviaturas presentes en el documento.

La segunda parte consta de la descripción del software, en donde se describen las características, funciones y restricciones, además de la caracterización de los usuarios que interactúan con el sistema.

Para finalizar, una tercera parte donde se establecen los requisitos funcionales y no funcionales con los que debe cumplir el módulo de autenticación que se pretende desarrollar.

2.2.2 Descripción general

El módulo de autenticación para la plataforma de voto electrónico administra el proceso de autenticación y verificación de identidad, mediante la implementación de métodos para la encriptación de datos, complementado con el uso de protocolos para el envío seguro de datos y la generación de llaves asimétricas.

2.2.2.1 Perspectiva del Producto

El sistema de voto electrónico para los cuerpos colegiados de la Universidad de Cundinamarca consta de un módulo de autenticación, el cual se pretende que sea totalmente independiente y adaptable, con el objetivo generar una herramienta de acceso y autenticación para futuros desarrollos de software. Se proyecta que el módulo sea el encargado de la generación, administración y verificación de llaves públicas y cifrado asimétrico para la ejecución de un proceso de identificación confiable de los usuarios que estén habilitados para ingresar en la plataforma y ejercer su derecho al voto.

2.2.2.2 Funciones del producto

Las funciones o procesos que desempeña el módulo de autenticación son los siguientes:

- **Gestión de registro de votantes:** se encargará de gestionar el registro de las personas habilitadas para votar.
- **Generación y administración de claves asimétricas:** Generación de par de claves relacionadas para cada entidad, una publica para la identificación y el cifrado de datos, una privada para desencriptación.
- **Almacenamiento de datos personales:** Almacenamiento de los datos personales de las personas registradas en el sistema.
- **Gestión del acceso a la plataforma de votación:** Validación de identidad y proceso de autenticación.

2.2.2.3 Características de los usuarios

Usuario: El usuario es aquella persona que desea ingresar a la plataforma de votación y participar de la jornada electoral, por lo que inicialmente debe haber un registro de datos para la generación de un par de claves, para la comunicación segura con el servidor de aplicaciones. Posteriormente realizara el proceso de autenticación e ingreso al sistema de votación, de la siguiente manera:

- Realiza el inicio de sesión en la plataforma, mediante usuario y contraseña.
- El sistema verifica los datos y envía una OTP al celular del usuario, en el que la aplicación móvil realiza las operaciones criptográficas y completar el proceso de autenticación mediante un protocolo de desafío respuesta.

2.2.2.4 Restricciones

El módulo de autenticación para el sistema de voto electrónico estará diseñado para realizar el envío de datos y la conexión mediante la infraestructura de servicios web, que permita la comunicación e integración con casi cualquier desarrollo. La app móvil estará disponible únicamente para dispositivos con sistema operativo Android.

- La arquitectura implementada para el módulo es la siguiente:
- Servidor Ubuntu Linux
- Servidor de aplicaciones Glassfish
- Base de Datos PostgreSQL
- Java JDK
- Java JCA – JCE
- Android SDK – Retrofit
- Firebase Cloud Messaging

2.2.2.5 Suposiciones y dependencias

El algoritmo seleccionado para la generación de claves asimétricas es el ECC, criptografía de curvas elípticas.

2.2.2.6 Requisitos futuros

El módulo debe adaptarse a futuros cambios y a su implementación en diferentes proyectos de desarrollo de software web, en los que se requiera la autenticación y verificación de identidad.

2.2.3 Requisitos específicos

En esta sección, se presentan los requisitos específicos con los que debe cumplir el módulo a desarrollar.

2.2.3.1 Interfaces Externas

No Aplica.

2.2.3.2 Funciones

Tabla 8 Funciones modulo autenticación

RF01 – Registrar votante	
Actores	Usuario
Descripción	El Usuario podrá registrarse a través de una aplicación móvil, para generar y almacenar unas credenciales de acceso a la plataforma de voto electrónico.
Entradas	Nombre, Apellido, Tipo documento, Numero documento, Correo institucional, Tipo persona, Sede, Programa, Número telefónico, Código y contraseña.
RF02 – Iniciar sesión	
Actores	Usuario
Descripción	El usuario accede a través de la plataforma web. Esta consume el servicio web para la autenticación, envía los datos de inicio de sesión y el módulo se encarga del procesamiento y validación de la información. Si el usuario es válido envía clave OTP al móvil del usuario.
Entradas	Usuario, Contraseña.

RF03 – Autenticar votante	
Actores	Usuario
Descripción	El usuario mediante una aplicación que debe instalar en su dispositivo móvil procede a realizar el proceso de autenticación mediante un protocolo de desafío-respuesta, a partir de la clave OTP que ha recibido.
Entradas	Contraseña del Usuario.
RF04 – Validar Correo	
Actores	Usuario
Descripción	Mediante la aplicación móvil, el usuario ingresa el código de validación que fue enviado a su correo electrónico durante el proceso de registro.
Entradas	Código de verificación.
RF05 – Renovación de Llaves	
Actores	Usuario
Descripción	En caso de que el usuario no pueda realizar el proceso de autenticación debido a la perdida de la llave privada almacenada en su teléfono móvil, el sistema ofrece la opción de generar un nuevo par de llaves y asociarlos a un usuario que ha sido registrado con anterioridad.
Entradas	Usuario, Contraseña, fecha de registro.

2.2.3.3 Requisitos de rendimiento

El módulo debe ser capaz de responder a solicitudes simultaneas de registro y autenticación de los usuarios que van a acceder a la plataforma de votación.

El método de encriptación y los protocolos de transporte de datos deben brindar seguridad y agilidad, en el desempeño de las funciones del módulo.

Una interfaz gráfica ágil e intuitiva para el acceso a la plataforma de voto electrónico.

2.2.3.4 Restricciones de diseño

Para el diseño y desarrollo del módulo de autenticación se establece el uso de elementos de la metodología ágil basada en SCRUM, debido a que este es un

marco dentro del cual puede emplear diversos procesos y técnicas, además de que ha sido ampliamente implementado en desarrollos de software.

La organización y jerarquización de las tareas se realizará basándonos en el modelo en cascada para el proceso de desarrollo, por lo que inicialmente se realiza una definición de requerimientos, seguido de la fase diseño y desarrollo, para luego proceder a la implementación e integración del módulo con la plataforma web. El modelado del sistema se realiza mediante diagramas basados en algunos elementos de UML.

De igual manera la adaptación del marco de garantía de autenticación de entidad, Estándar internacional ISO/IEC DIS 29115, que hace referencia a los niveles de garantía de autenticación y las pautas establecidas en el documento directriz de autenticación electrónica NIST SP 800-63.

2.2.3.5 Atributos del sistema

A continuación, se detallan los atributos de calidad del módulo de autenticación.

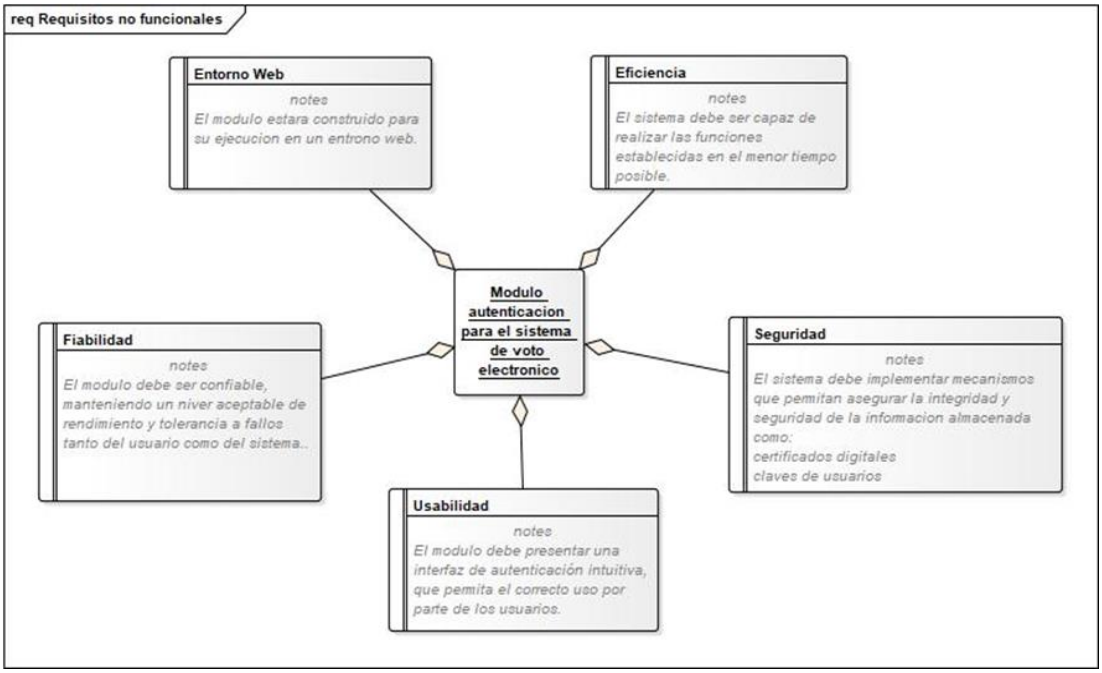


Figura 8 Requisitos no funcionales

2.3 Especificación del diseño

2.3.1 Modelo entidad relación (MER)

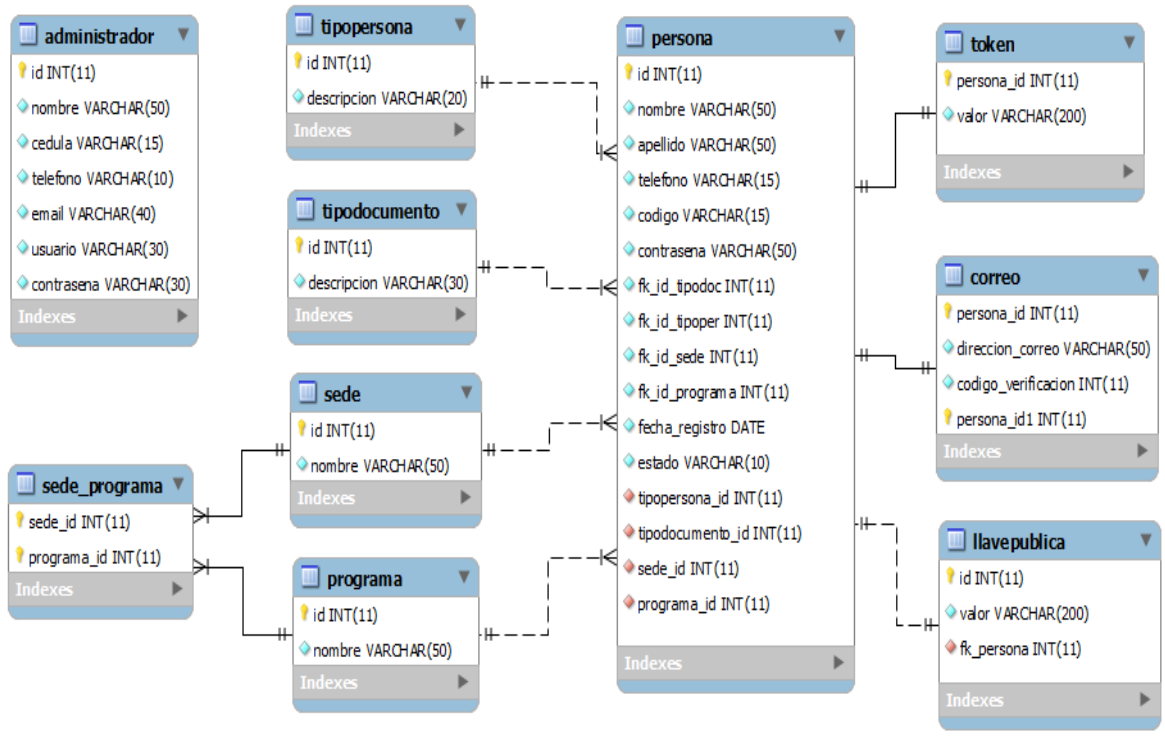


Figura 9 Modelo Entidad Relación

Descripción de tablas:

- **Tipo documento:** Esta tabla contiene los tipos de documento de identificación validos en Colombia.
- **Tipo persona:** Esta tabla contiene los roles de los usuarios que se registran en el sistema (Estudiante, Docente, Directivo, Egresado).
- **Programa:** Esta tabla contiene los diferentes programas que ofrece la Institución educativa.
- **Sede:** Esta tabla contiene las diferentes sedes de la institución educativa.
- **Sede_Programa:** Esta tabla guarda la relación entre sedes y programas.

- **Llave publica:** En esta tabla se almacenan las llaves publicas correspondientes a cada persona registrada en el módulo, con la cual se realizará el proceso de cifrado.
- **Personas:** En esta tabla se almacena la información correspondiente a cada persona registrada en el módulo, en ella se puede encontrar los datos personales. Es la tabla principal del módulo de autenticación.
- **Token:** Almacena el token del dispositivo móvil del usuario para él envió de la notificación con la OTP.
- **Correo:** Almacena la información relacionada con el email de la persona.
- **Administrador:** Esta tabla almacena la información de las personas que administran las opciones del módulo.

2.3.2 Diagrama de Roles

El módulo de autenticación tiene dos roles: 1) El administrador del módulo, que puede parametrizar las opciones para el registro de usuarios. 2) El usuario de la aplicación móvil con la cual se realiza el proceso de autenticación para el acceso al a la plataforma de votación por internet.

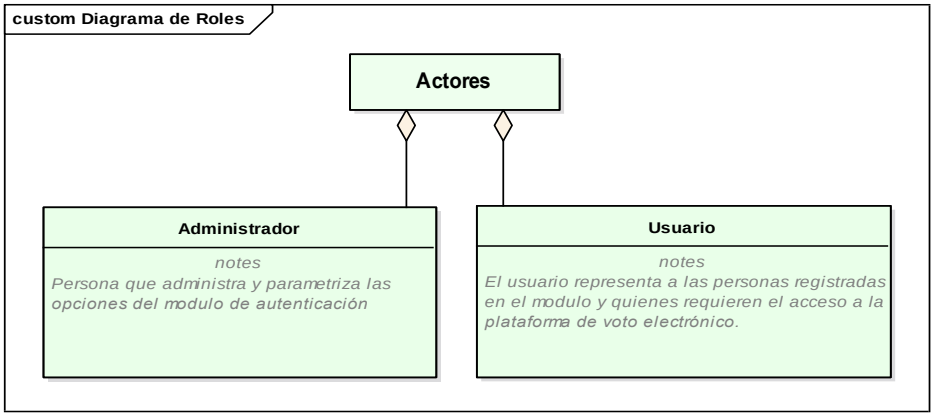


Figura 10 Diagrama de Roles

2.3.3 Diagramas de casos de uso

El siguiente diagrama muestra los casos de uso establecidos para el módulo de autenticación, teniendo en cuenta los dos roles presentes en el sistema y los requisitos funcionales de este.

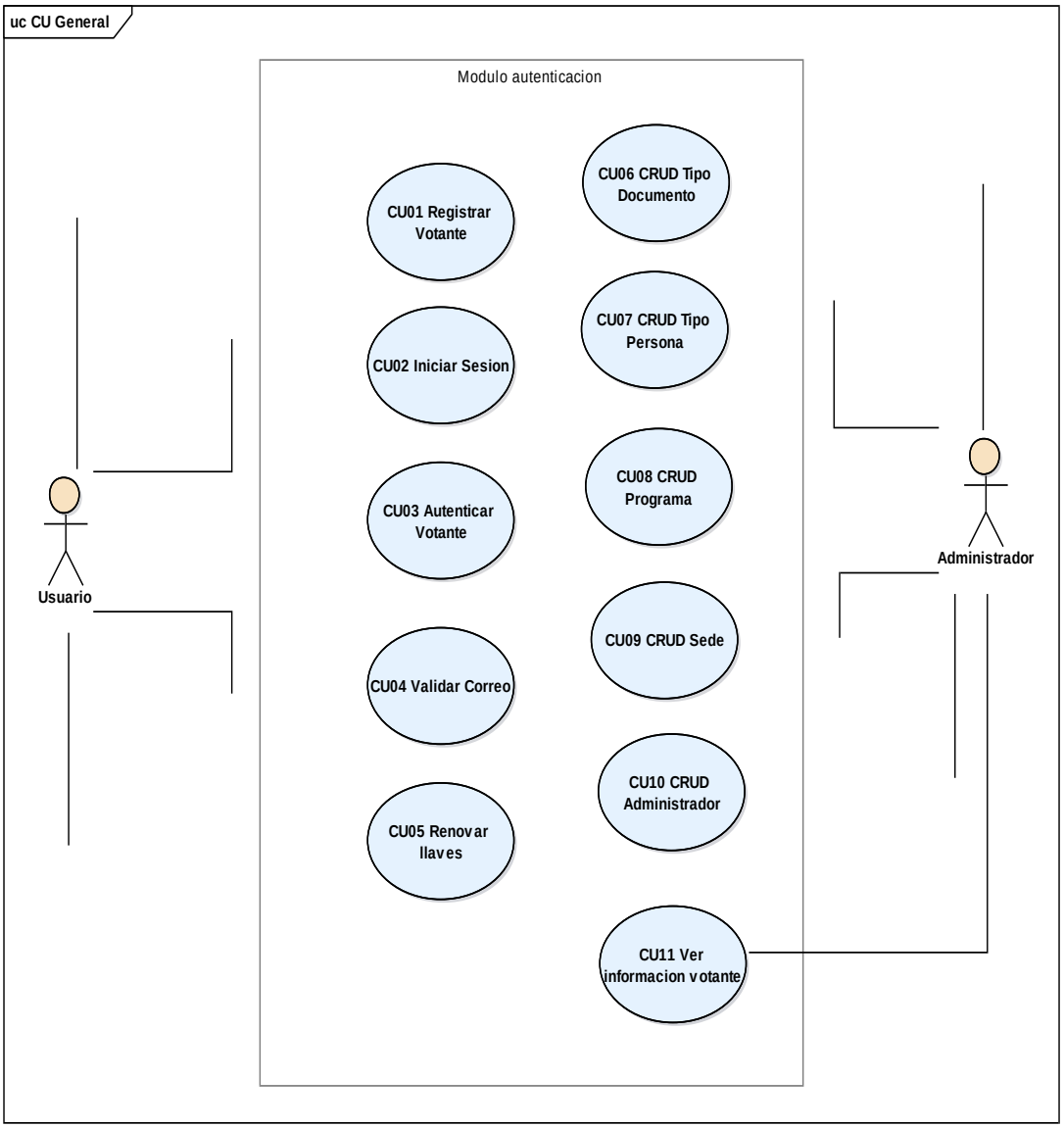


Figura 11 Diagrama General Casos de Uso

Caso de uso registrar votantes CU01

Tabla 9 CU01 Registrar Votantes

Nombre:	**CU01 Registrar Votantes**
Autor:	Cristian Camilo Pérez
Descripción:	Permite el ingreso y registro de los datos personales de cada usuario que requiera acceso a la plataforma de voto por internet, además de la generación de un par de llaves relacionadas de las cuales el usuario es acreedor y por medio de las cuales se realizara el proceso de autenticación.
Actor:	Usuario
Precondiciones:	1. El usuario debe tener su dispositivo móvil a la mano y haber instalado la aplicación de autenticación. 2. El usuario tiene que disponer de un correo institucional valido de la Universidad de Cundinamarca.
Flujo normal:	1. El usuario ingresa sus datos personales. 2. El sistema valida la información 3. Generación de llaves pública y privada. 4. Envió de correo de validación. 5. Almacenamiento de registro en base de datos. 6. El sistema informa que el registro se ha realizado.
Postcondición:	El usuario esta correctamente registrado en la base de datos del sistema, se hace responsable de la llave privada almacenada en su teléfono y debe realizar la validación de correo para quedar activo.

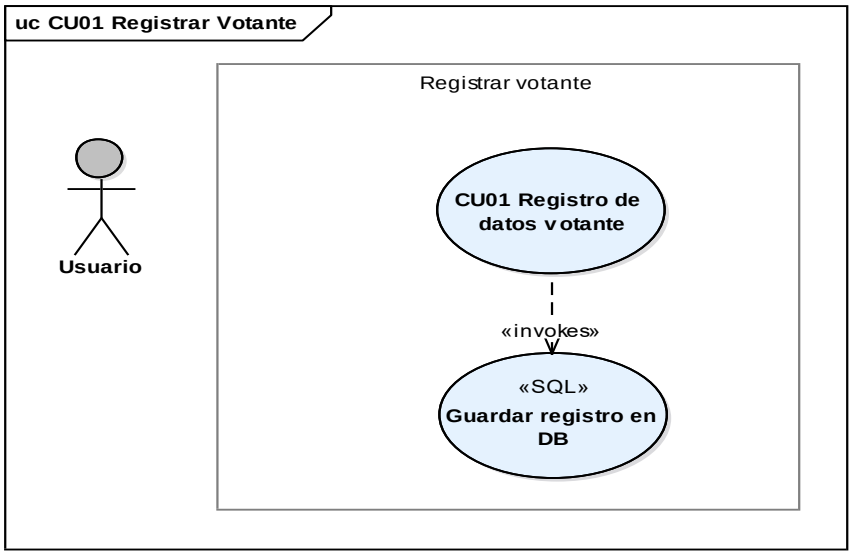


Figura 12 CU01 Registrar Votantes

Caso de uso iniciar sesión CU02

Tabla 10 CU02 Iniciar Sesión

Nombre:	**CU02 Iniciar sesión**
Autor:	Cristian Camilo Pérez
Descripción:	Este caso de uso permite el ingreso a la plataforma de voto por internet por medio de un proceso de autenticación multifactor.
Actor:	Plataforma web
Precondiciones:	1. El usuario (Votante) debe haberse registrado previamente CU01. 2. Debe disponer de su dispositivo móvil para completar el proceso de autenticación. 3. Debe haber completado la validación de su correo electrónico exitosamente.
Flujo normal:	1. El usuario ingresa su usuario y contraseña 2. El sistema valida la información. 3. Se genera OTP. 4. Se encripta OTP con clave pública del usuario. 5. El sistema realiza el envío de OTP cifrada al móvil del usuario. 6. Retorna OTP. 7. Se realiza el proceso de autenticación CU03.
Postcondición:	El usuario se ha ingresado correctamente a la plataforma de voto por internet.

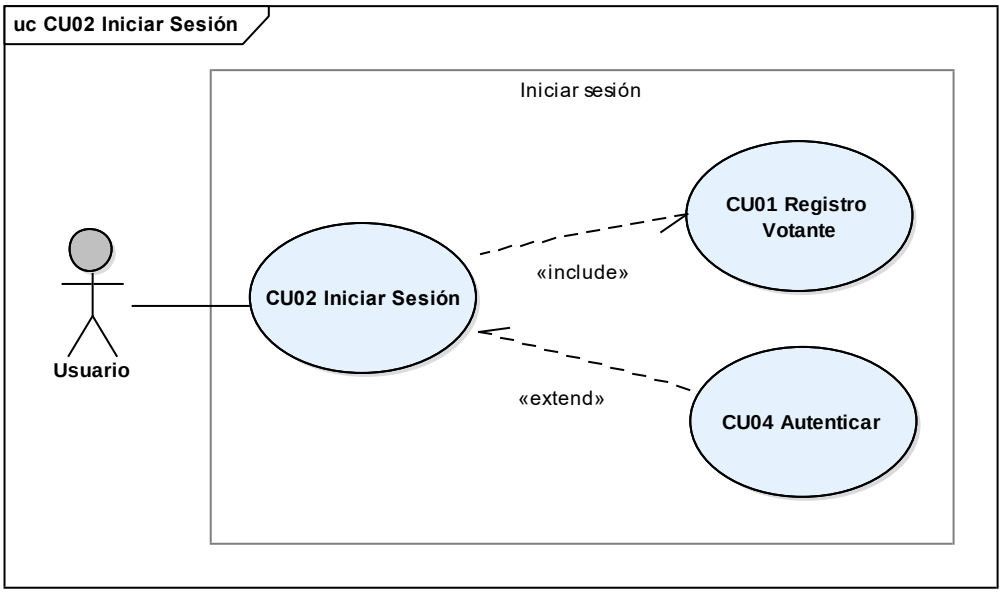


Figura 13 CU02 Iniciar Sesión

Caso de uso autenticar votante CU03

Tabla 11 CU03 Autenticar Votante

Nombre:	**CU03 Autenticar votante**
Autor:	Cristian Camilo Pérez
Descripción:	Permite realizar el proceso de autenticación a través de un protocolo de desafío respuesta
Actor:	Usuario
Precondiciones:	1. El usuario debe tener a la mano el móvil con conexión a internet. 2. El usuario debe haber iniciado sesión.
Flujo normal:	1. El usuario realiza el proceso de inicio de sesión CU02. 2. Recepción de OTP cifrada en el móvil. 3. La app descifra La OTP recibida. 4. Se muestra valor real de OTP al usuario. 5. El usuario debe ingresar el valor de esa OTP en la plataforma web.
Postcondición:	El usuario se ha autenticado correctamente y puede acceder a los recursos de la plataforma de voto por internet.

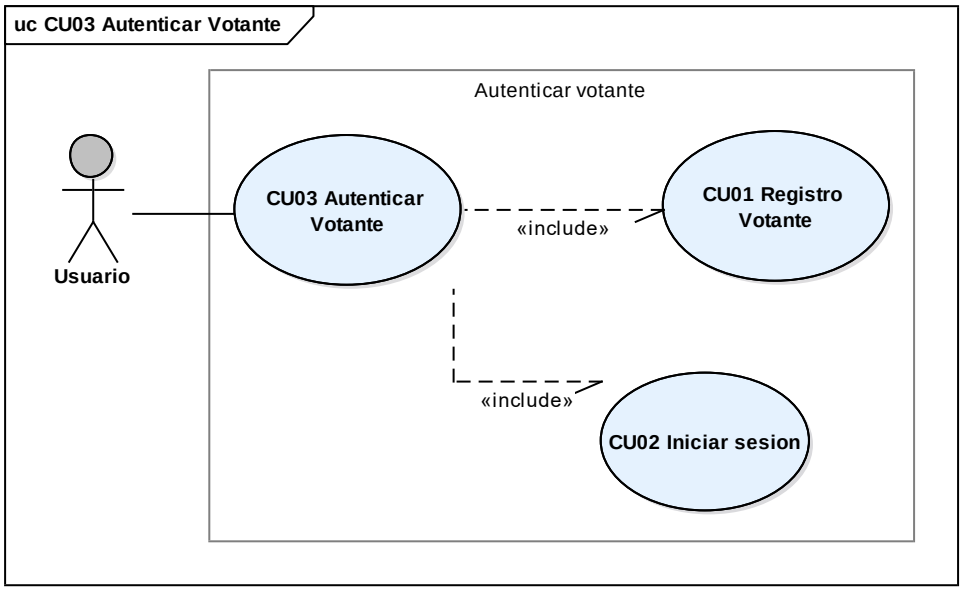


Figura 14 CU03 Autenticar Votante

Caso de uso validar correo CU04

Tabla 12 CU04 Validar Correo

Nombre:	**CU04 Validar correo**
Autor:	Cristian Camilo Pérez
Descripción:	Permite validar que la dirección de correo electrónico proporcionada sea válida y corresponda a una persona de la institución.
Actor:	Plataforma web
Precondiciones:	1. El usuario debe tener acceso al correo institucional de la Universidad de Cundinamarca. 2. El usuario debe haber realizado el proceso de registró previamente.
Flujo normal:	1. El usuario realiza el proceso de registro, el sistema envía un código de validación al correo proporcionado por el usuario. 2. El usuario entra en la app móvil al apartado de validación de correo, allí ingresa el código que fue enviado a su correo electrónico. 3. El sistema valida los datos y actualiza el estado del usuario (ACTIVO).
Postcondición:	El usuario ha validado correctamente su dirección de correo electrónico, confirmando que es una persona perteneciente a la institución.

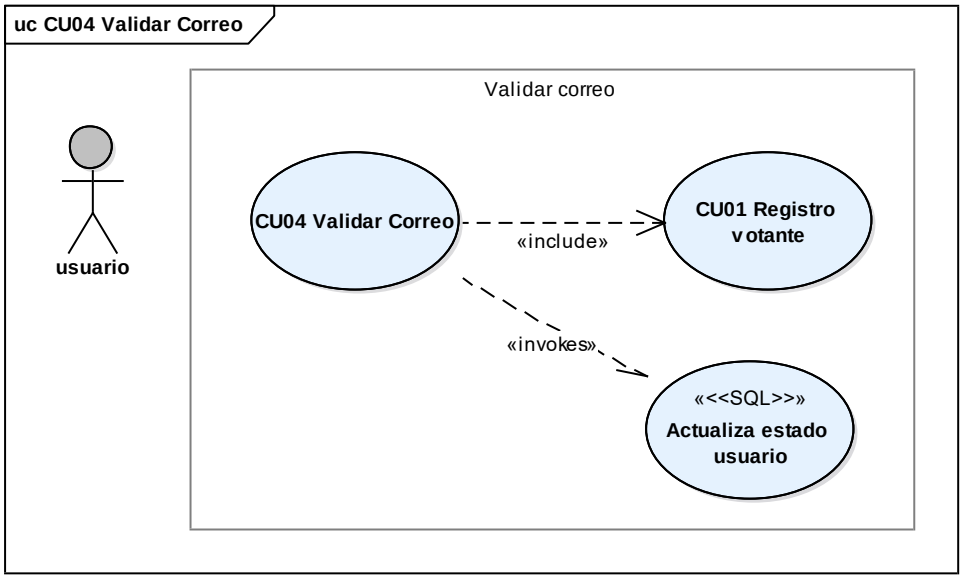


Figura 15 CU04 Validar Correo

Caso de uso renovar llaves CU05

Tabla 13 CU05 Renovar Llaves

Nombre:	**CU05 Renovar Llaves**
Autor:	Cristian Camilo Pérez
Descripción:	Permite la renovación de las llaves pública y privada, esto en caso de que el titular de las credenciales, por alguna razón se vea forzado a cambiar de teléfono móvil y por lo tanto pierda el acceso a la plataforma de votación, debido a que sin este no es posible el proceso de autenticación.
Actor:	Usuario
Precondiciones:	1. El usuario debe haber estado registrado previamente. 2. El usuario debe volver a instalar la aplicación en su nuevo dispositivo móvil.
Flujo normal:	1. El usuario realiza la solicitud de renovación de llaves, ingresando los datos requeridos. 2. El sistema valida los datos, verificando que coincidan con un registro en la base de datos. 3. El sistema genera un nuevo par de claves. 4. Actualiza la información del usuario. 5. Almacena nueva clave privada en el móvil del usuario. 6. muestra mensaje, credenciales recuperados correctamente.
Postcondición:	El usuario ha recuperado en el móvil, sus credenciales de acceso a la plataforma web.

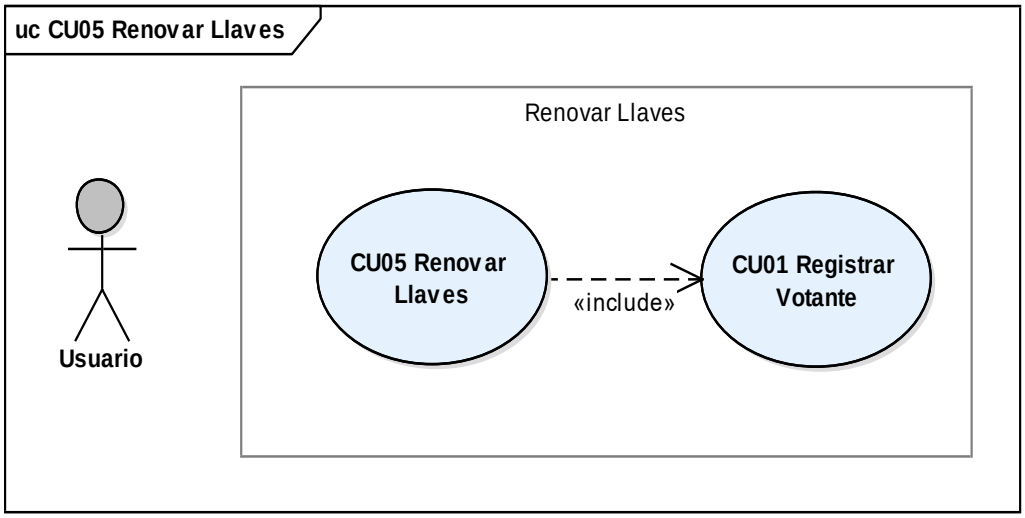


Figura 16 CU05 Renovar Llaves

Caso de uso CRUD tipo documento CU06

Tabla 14 CU06 CRUD Tipo Documento

Nombre:	**CU06 CRUD Tipo Documento**
Autor:	Cristian Camilo Pérez
Descripción:	Permite la administración de los tipos de documentos válidos para realizar el registro en el módulo de autenticación.
Actor:	Administrador
Precondiciones:	1. El administrador debe ingresar a la plataforma de administración del módulo con su usuario y contraseña.
Flujo normal:	**Registrar** 1. El administrador ingresa nombre del nuevo tipo de documento. 2. El sistema almacena registro en base de datos. 3. El sistema actualiza tabla de tipos de documento.
	Listar 1. El administrador va a la pestaña de documentos. 2. El sistema muestra la tabla con los tipos de documento.
	Actualizar 1. El administrador presiona la opción para editar un registro. 2. Edita el registro y acepta. 3. El sistema guarda y refleja los cambios en la tabla.
	Borrar 1. El administrador selecciona el o los registros que desea eliminar, y presiona el botón borrar. 2. Confirma que quiere borrar los registros. 3. El sistema borra los registros y actualiza la tabla.
Postcondición:	El administrador ha parametrizado los tipos de documentos con los cuales un usuario se puede registrar en el módulo de autenticación.

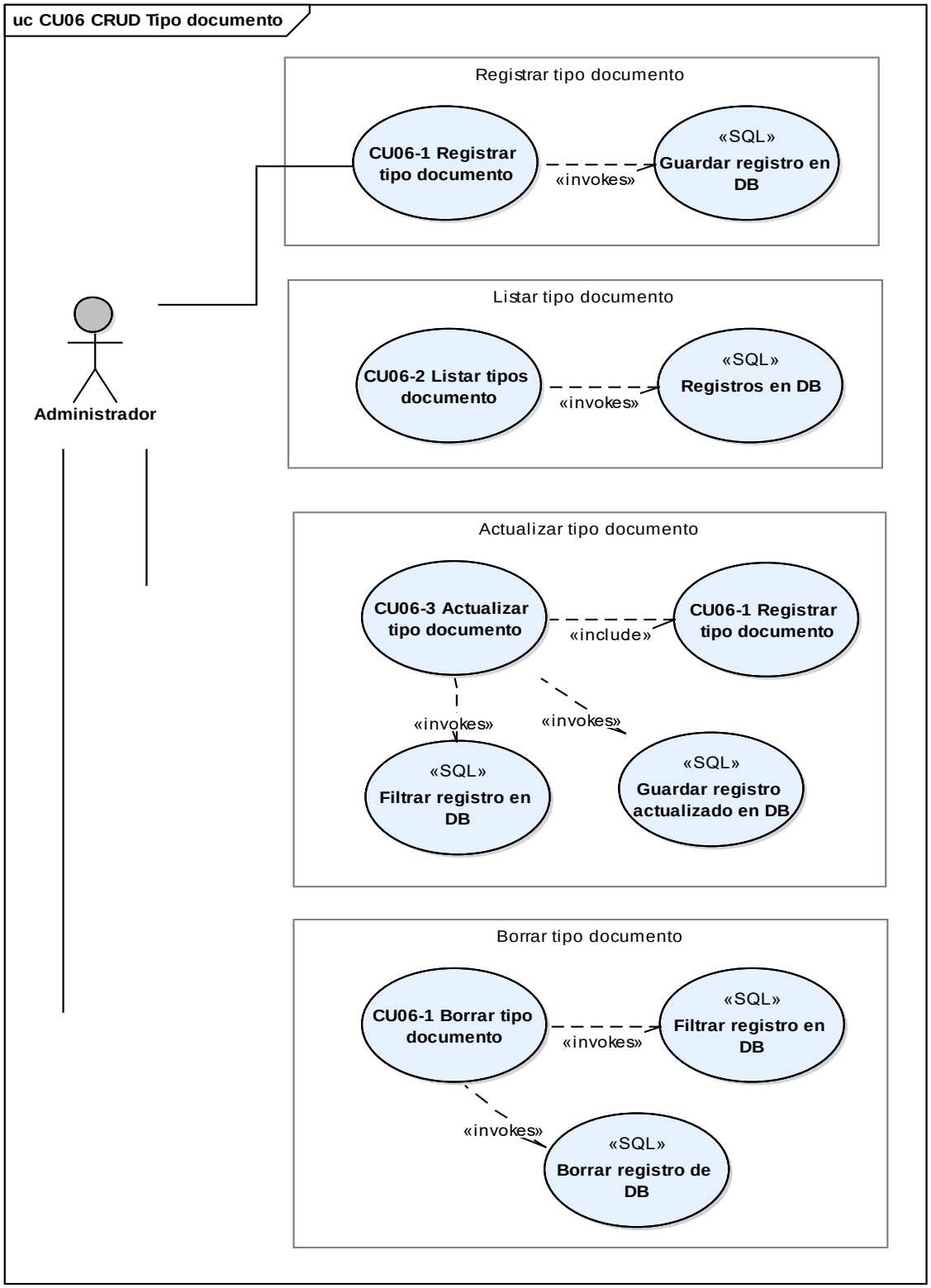


Figura 17 CU06 CRUD Tipo Documento

Tabla 15 CU07 CRUD Tipo Persona

Nombre:	**CU07 CRUD Tipo Persona**
Autor:	Cristian Camilo Pérez
Descripción:	Permite la administración de los tipos de persona válidos para realizar el registro en el módulo de autenticación.
Actor:	Administrador
Precondiciones:	1. El administrador debe ingresar a la plataforma de administración del módulo con su usuario y contraseña.
Flujo normal:	**Registrar** 1. El administrador ingresa nombre del nuevo tipo de persona. 2. El sistema almacena registro en base de datos. 3. El sistema actualiza tabla de tipos de persona.
	Listar 1. El administrador va a la pestaña de roles. 2. El sistema muestra la tabla con los tipos de persona.
	Actualizar 1. El administrador presiona la opción para editar un registro. 2. Edita el registro y acepta. 3. El sistema guarda y refleja los cambios en la tabla.
	Borrar 1. El administrador selecciona el o los registros que desea eliminar, y presiona el botón borrar. 2. Confirma que quiere borrar los registros. 3. El sistema borra los registros y actualiza la tabla.
Postcondición:	El administrador ha parametrizado los tipos de persona con los cuales un usuario se puede registrar en el módulo de autenticación.

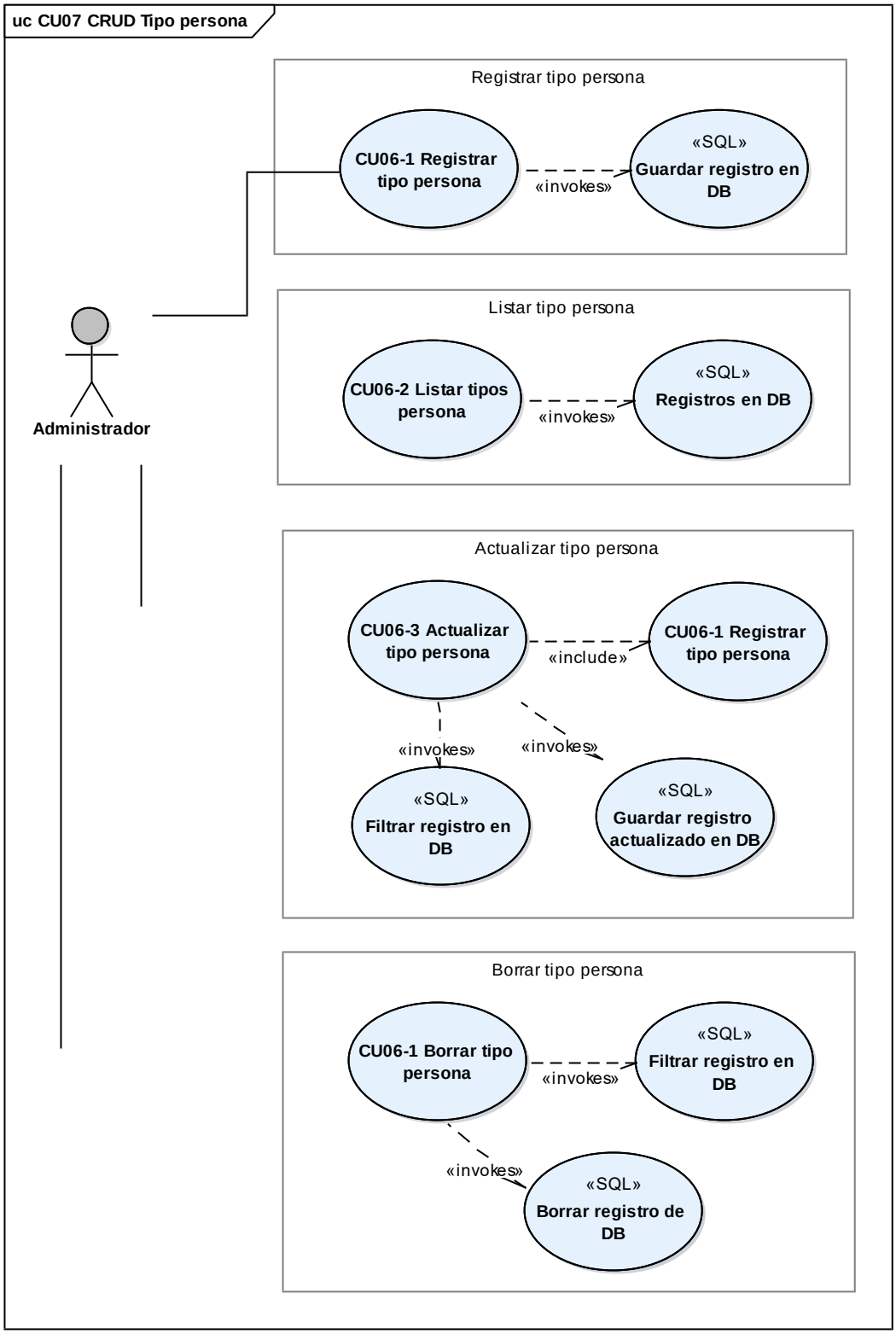


Figura 18 CU07 CRUD Tipo Persona

Tabla 16 CU08 CRUD Programa

Nombre:	**CU08 CRUD Programa**
Autor:	Cristian Camilo Pérez
Descripción:	Permite la administración de los programas académicos que ofrece la institución educativa.
Actor:	Administrador
Precondiciones:	1. El administrador debe ingresar a la plataforma de administración del módulo con su usuario y contraseña.
Flujo normal:	**Registrar** 1. El administrador ingresa nombre del nuevo programa académico. 2. El sistema almacena registro en base de datos. 3. El sistema actualiza tabla de programas académicos.
	Listar 1. El administrador va a la pestaña de programas. 2. El sistema muestra la tabla con los programas registrados.
	Actualizar 1. El administrador presiona la opción para editar un registro. 2. Edita el registro y acepta. 3. El sistema guarda y refleja los cambios en la tabla.
	Borrar 1. El administrador selecciona el o los registros que desea eliminar, y presiona el botón borrar. 2. Confirma que quiere borrar los registros. 3. El sistema borra los registros y actualiza la tabla.
Postcondición:	El administrador administra los programas educativos que ofrece la institución educativa.

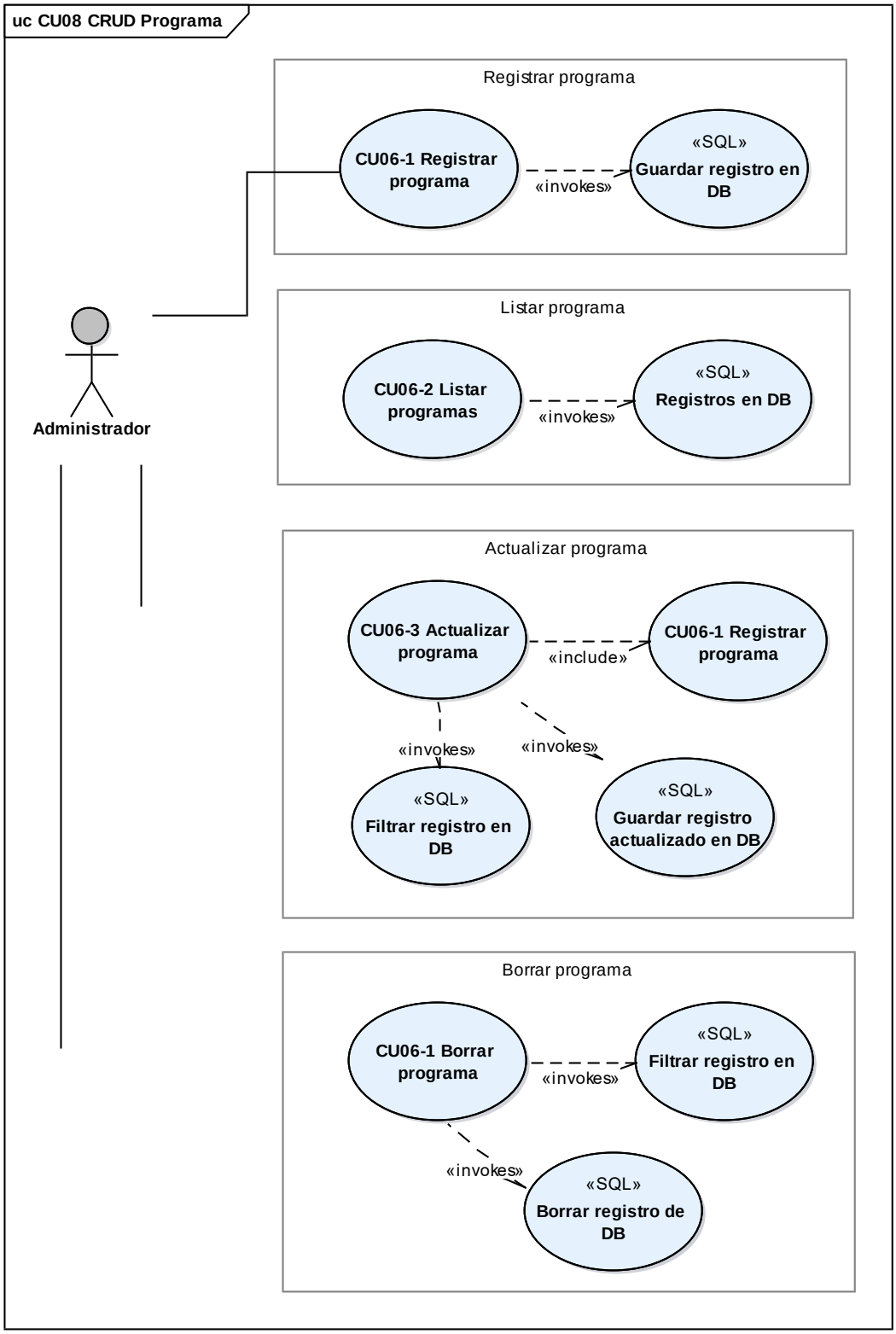


Figura 19 CU08 CRUD Programas

Tabla 17 CU09 CRUD Sede

Nombre:	**CU09 CRUD Sede**
Autor:	Cristian Camilo Pérez
Descripción:	Permite la administración de las sedes que tiene la institución educativa.
Actor:	Administrador
Precondiciones:	1. El administrador debe ingresar a la plataforma de administración del módulo con su usuario y contraseña. 2. Registrar programas para asociarlos a las sedes CU08.
Flujo normal:	**Registrar** 1. El administrador ingresa nombre de la nueva sede. 2. El sistema almacena registro en base de datos. 3. El sistema actualiza tabla de sedes. 4. El administrador puede asociar programas a cada sede según corresponda.
	Listar 1. El administrador va a la pestaña de sedes. 2. El sistema muestra la tabla con las sedes registradas.
	Actualizar 1. El administrador presiona la opción para editar un registro. 2. Edita el registro y acepta. 3. El sistema guarda y refleja los cambios en la tabla.
	Borrar 1. El administrador selecciona el o los registros que desea eliminar, y presiona el botón borrar. 2. Confirma que quiere borrar los registros. 3. El sistema borra los registros y actualiza la tabla.
Postcondición:	El administrador administra las sedes de la institución educativa.

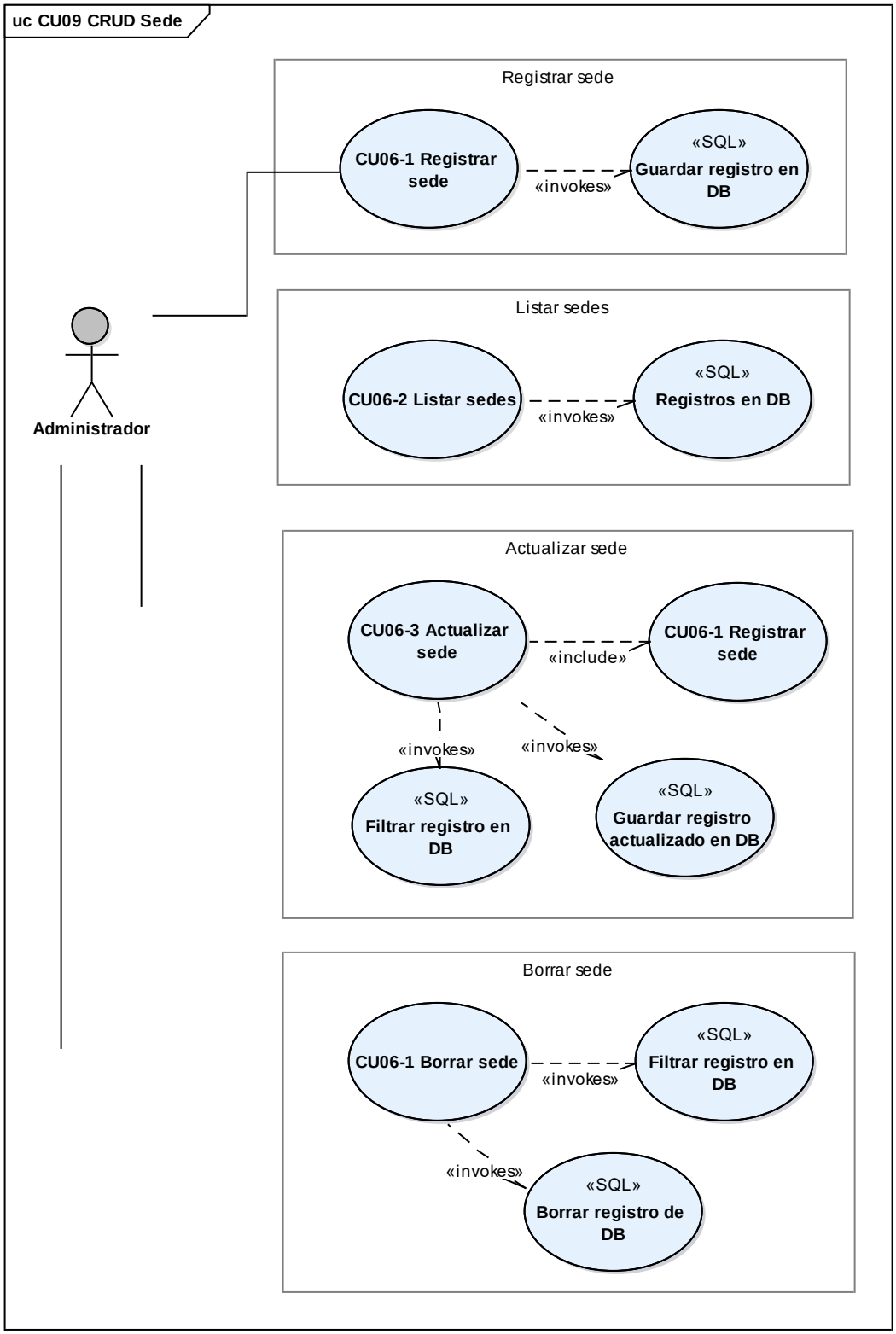


Figura 20 CU09 CRUD Sedes

Tabla 18 CU10 CRUD Administrador

Nombre:	**CU10 CRUD Administrador**
Autor:	Cristian Camilo Pérez
Descripción:	Permite la asignación de los administradores del módulo de autenticación.
Actor:	Administrador
Precondiciones:	1. Uno de los administradores del sistema debe ingresar a la plataforma del módulo con su usuario y contraseña.
Flujo normal:	**Registrar** 1. El administrador completa y envía el formulario para asignar un nuevo administrador. 2. El sistema almacena registro en base de datos. 3. El sistema actualiza tabla de administradores.
	Listar 1. El administrador va a la pestaña admin. 2. El sistema muestra la tabla con las personas registradas como administradores del módulo.
	Actualizar 1. El administrador presiona sobre la opción actualizar datos, que abre un formulario con sus datos personales. 2. Edita el registro y acepta. 3. El sistema guarda los cambios realizados. Se reflejan en la sección donde se ve la información del usuario que está en la plataforma.
	Borrar 1. El administrador selecciona el o los registros que desea eliminar, y presiona el botón borrar. 2. Confirma que quiere borrar los registros. 3. El sistema borra los registros y actualiza la tabla. Como Mínimo siempre hay dos administradores.
Postcondición:	Los administradores a cargo pueden administrar quienes pueden acceder a la plataforma de control de las opciones del módulo.

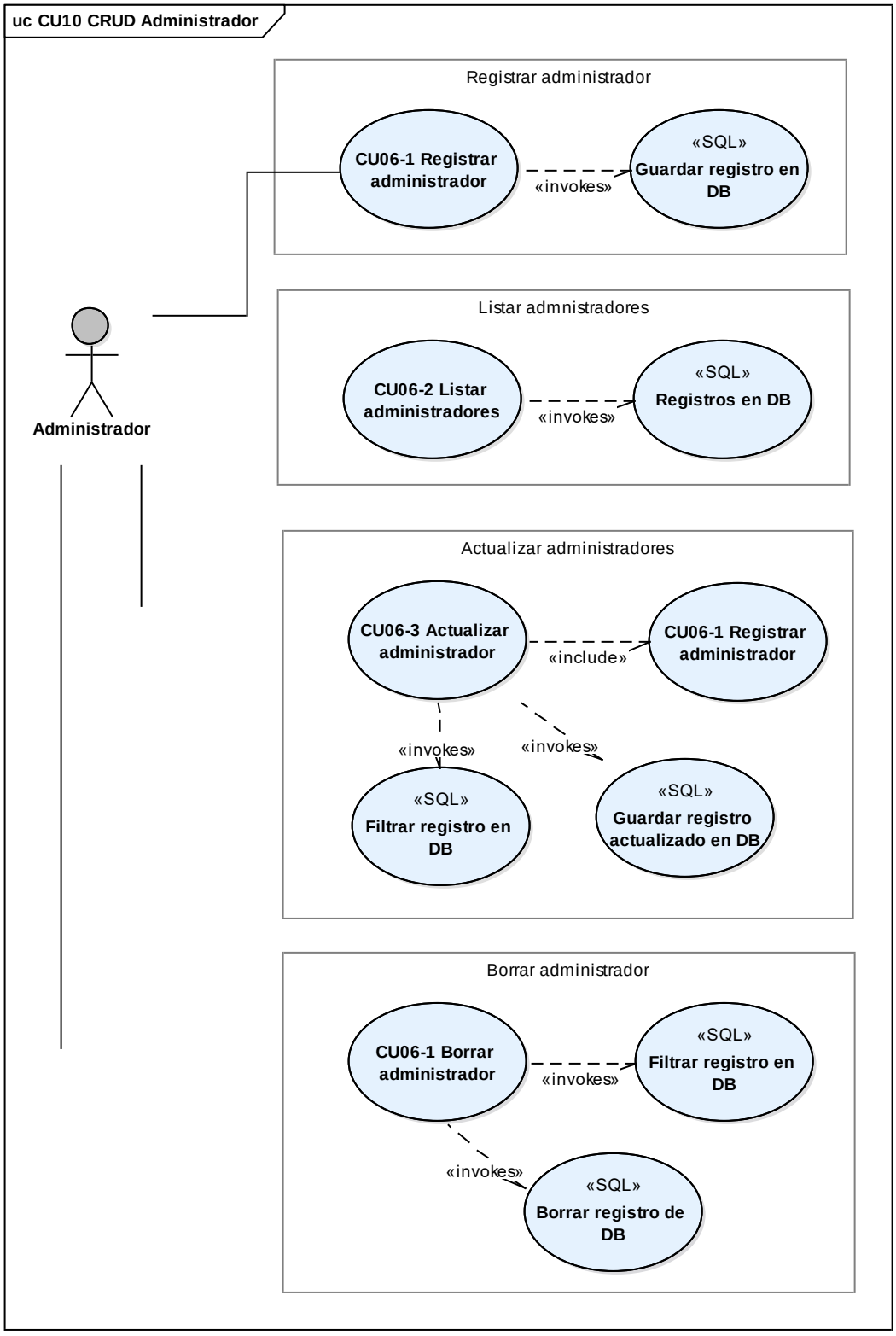


Figura 21 CU10 CRUD Administrador

Tabla 19 CU11 Ver Información Votante

Nombre:	**CU11 Ver Información Votante**
Autor:	Cristian Camilo Pérez
Descripción:	Permite buscar y ver la información de los votantes que se encuentren registrados en el módulo de autenticación.
Actor:	Administrador
Precondiciones:	1. El administrador debe ingresar a la plataforma de administración del módulo con su usuario y contraseña.
Flujo normal:	1. El administrador va a la pestaña Votantes. 2. Ingresa el id del votante que desea consultar. 3. El sistema muestra la información del usuario según corresponda.
Postcondición:	El administrador puede consultar la información de cualquiera de los usuarios registrados en el módulo autenticación.

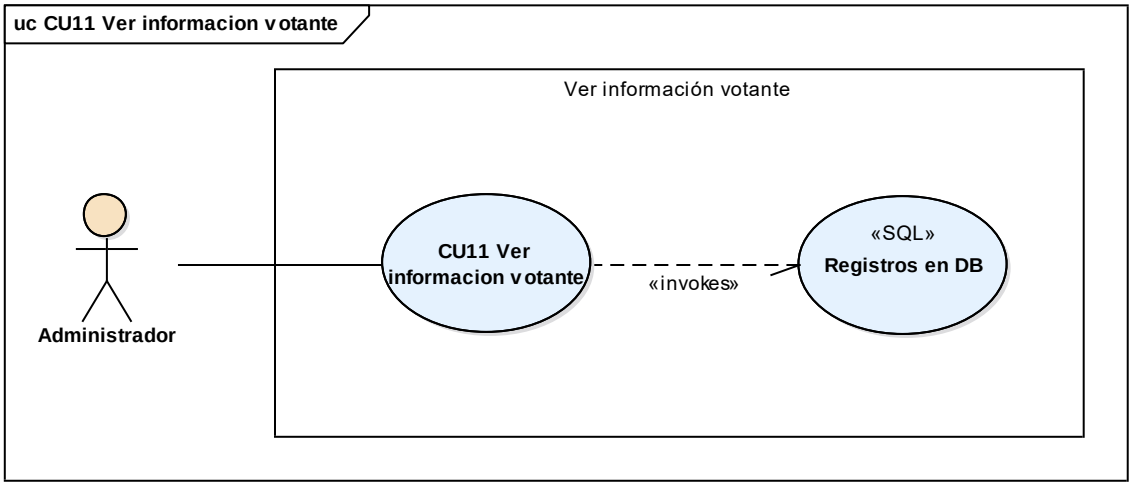


Figura 22 CU11 Ver Información Votante

2.3.4 Diagramas de secuencias

El siguiente diagrama de secuencia representa el proceso de registro de los votantes, que se realiza mediante la aplicación móvil que hace parte del módulo de autenticación, allí cada usuario ingresa sus datos personales para obtener las sus credenciales de acceso.

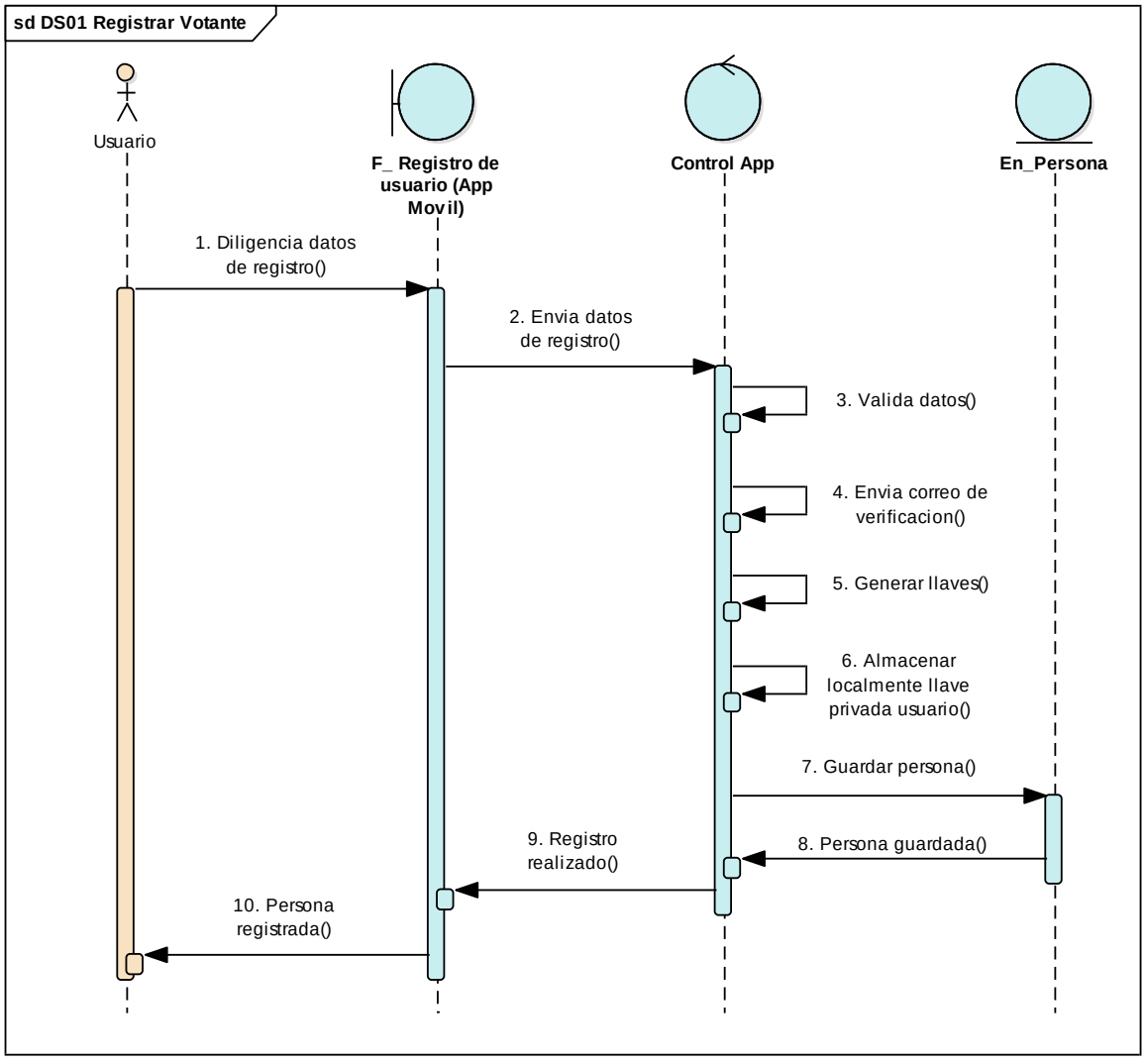


Figura 23 DS01 Registrar Votante

El siguiente diagrama de secuencia representa el proceso de inicio de sesión de los usuarios desde la plataforma que consume el servicio web del módulo de autenticación, el cual verifica la información recibida y realiza el envió de la OTP al móvil del usuario.

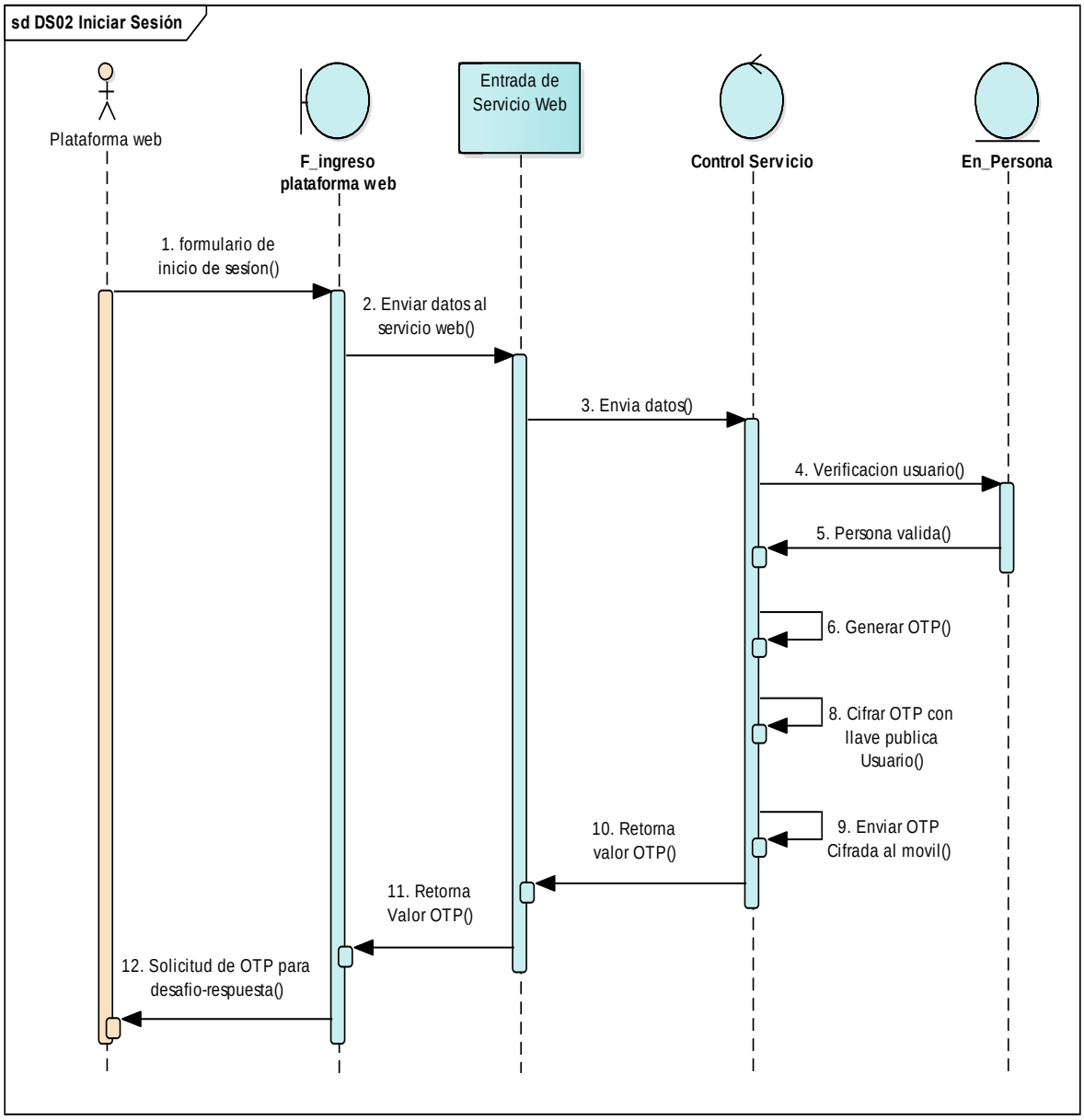


Figura 24 DS02 Iniciar Sesión

El siguiente diagrama de secuencia representa el proceso de autenticación a partir de la recepción de una OTP cifrada en el móvil de cada usuario, esto para posteriormente cumplir con el protocolo de desafío-respuesta.

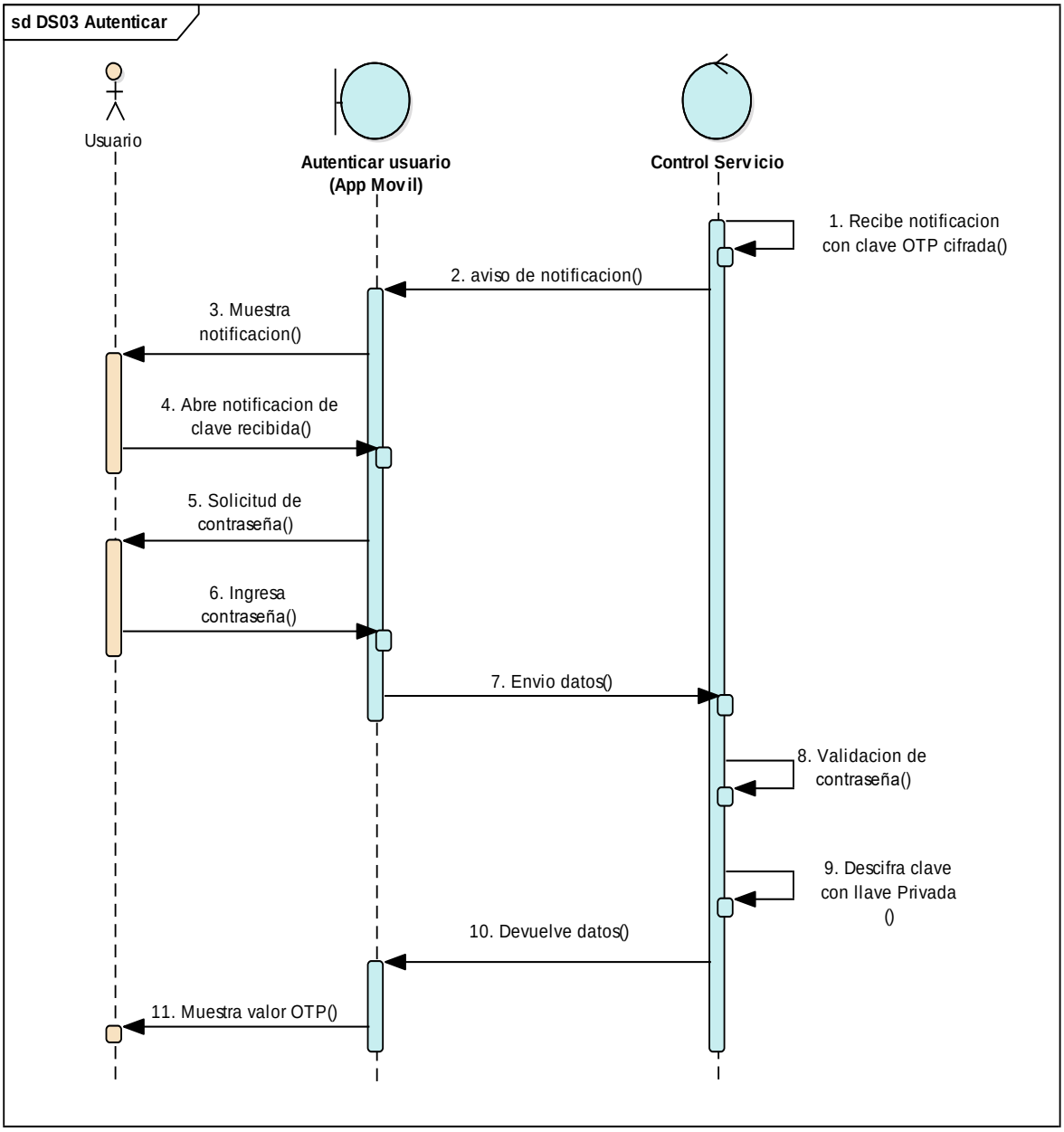


Figura 25 DS03 Autenticar Votante

El diagrama de secuencia que sigue a continuación representa el proceso de validación de correo electrónico. Un paso necesario para verificar la veracidad de la información además de restringir el acceso a la plataforma de voto, única y exclusivamente a personas de la Universidad de Cundinamarca.

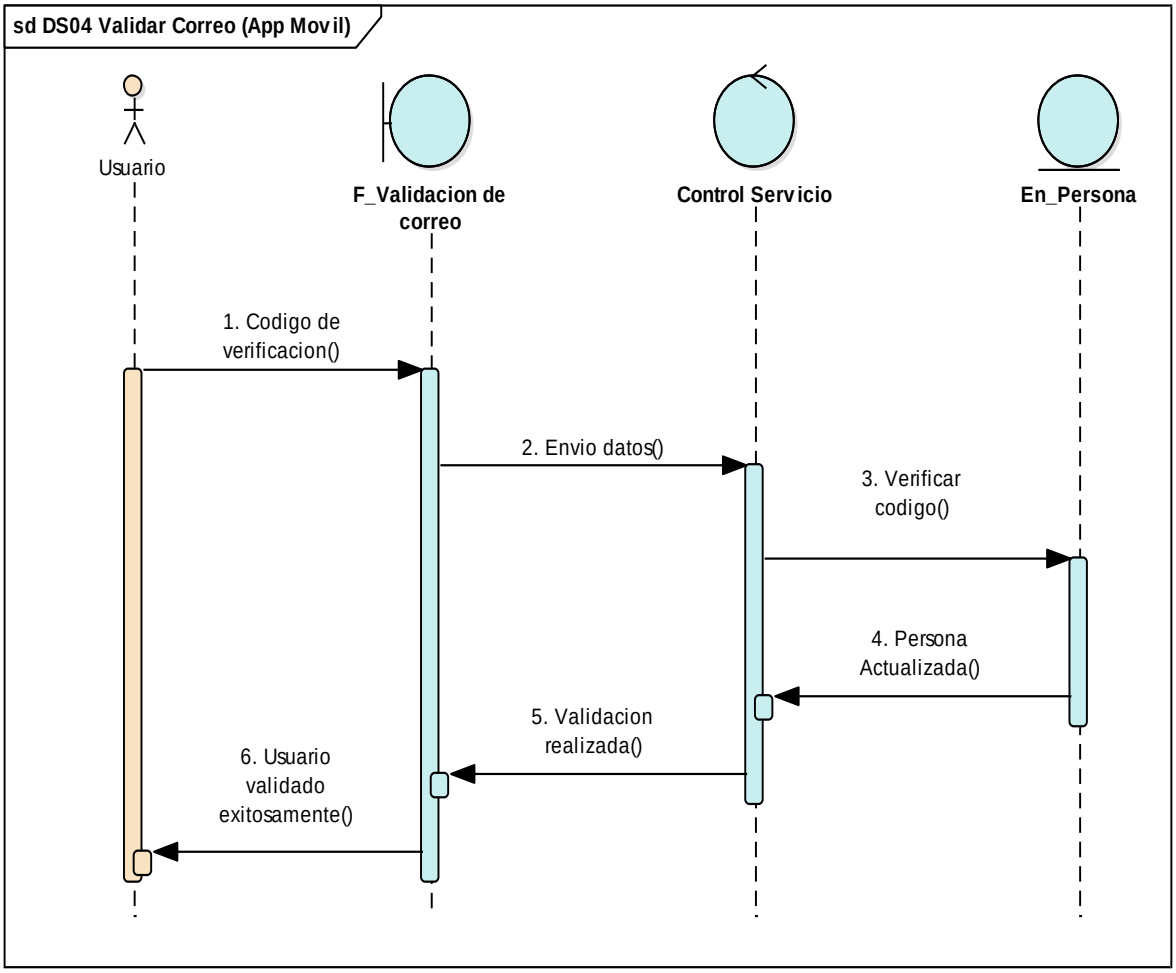


Figura 26 DS04 Validar Correo

El diagrama de secuencia que representa el proceso de la renovación de llaves (pública y privada), esto en caso de pérdida de la llave privada inicialmente generada con el registro, debido a diferentes causas como lo puede ser la pérdida del teléfono móvil donde esta se almacenaba, cambio de número telefónico y demás razones que lleven al usuario a realizar esta solicitud.

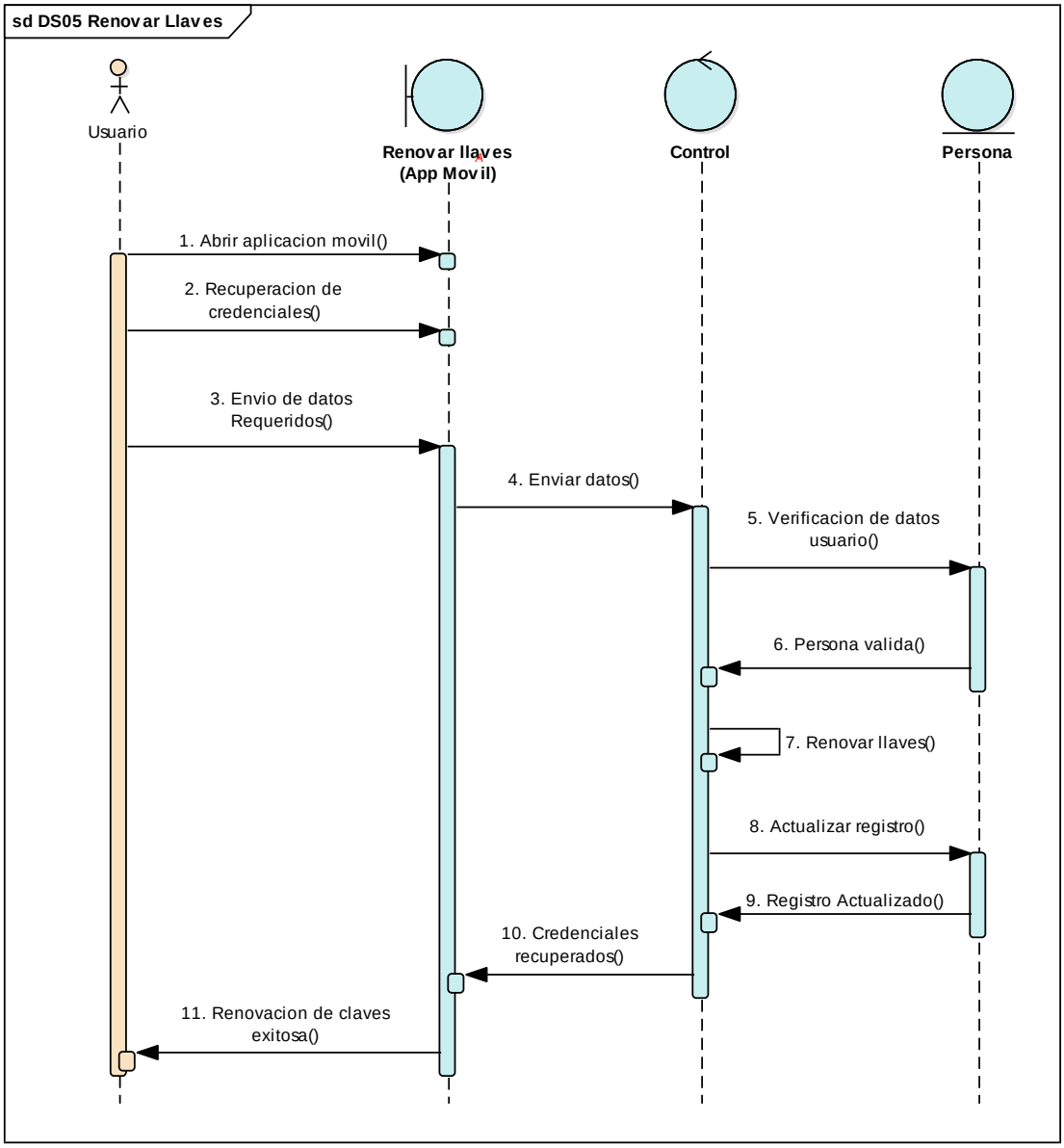


Figura 27 DS05 Renovación de Llaves

A continuación, se muestran los diagramas de secuencia del CRUD de Tipo de documento:

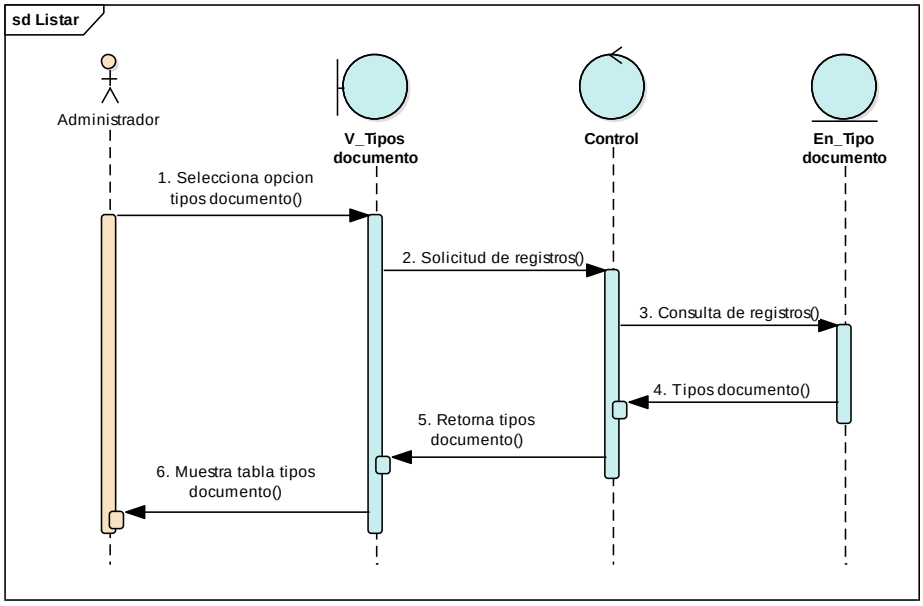


Figura 28 DS06-1 Listar Tipo Documento

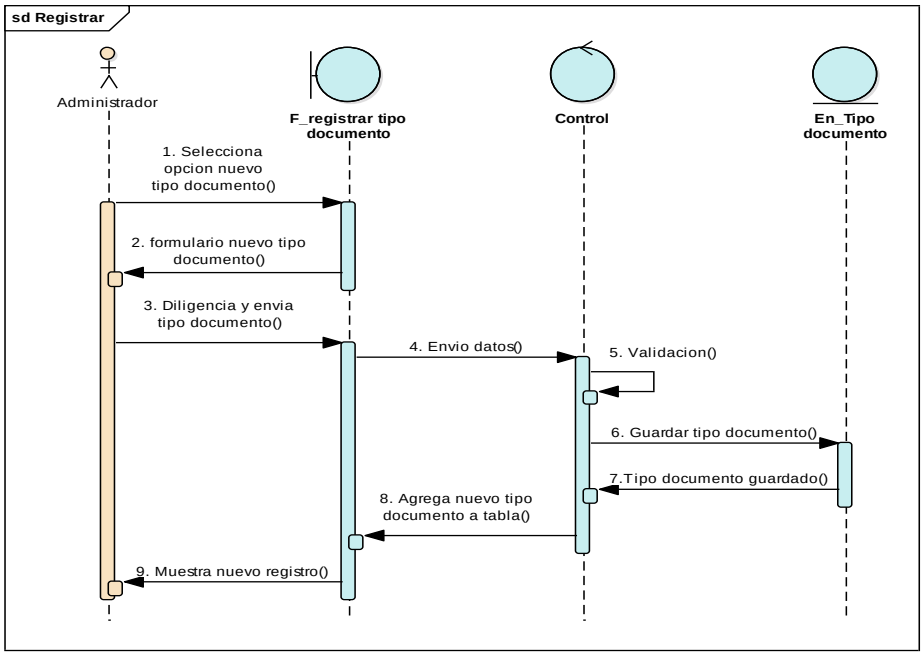


Figura 29 DS06-2 Registrar Tipo Documento

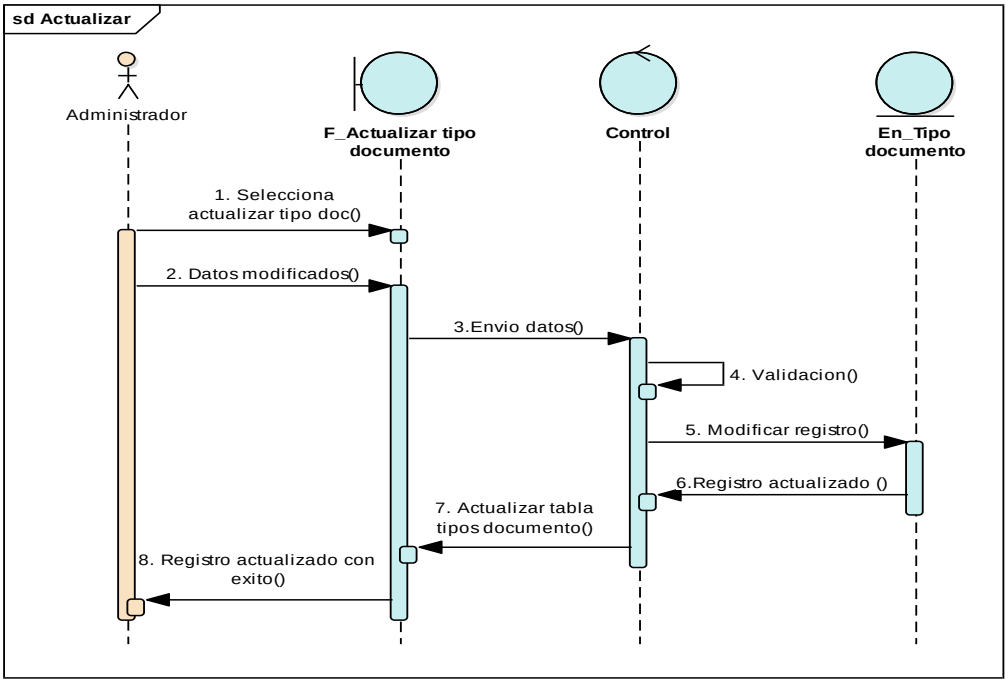


Figura 30 DS06-3 Actualizar Tipo Documento

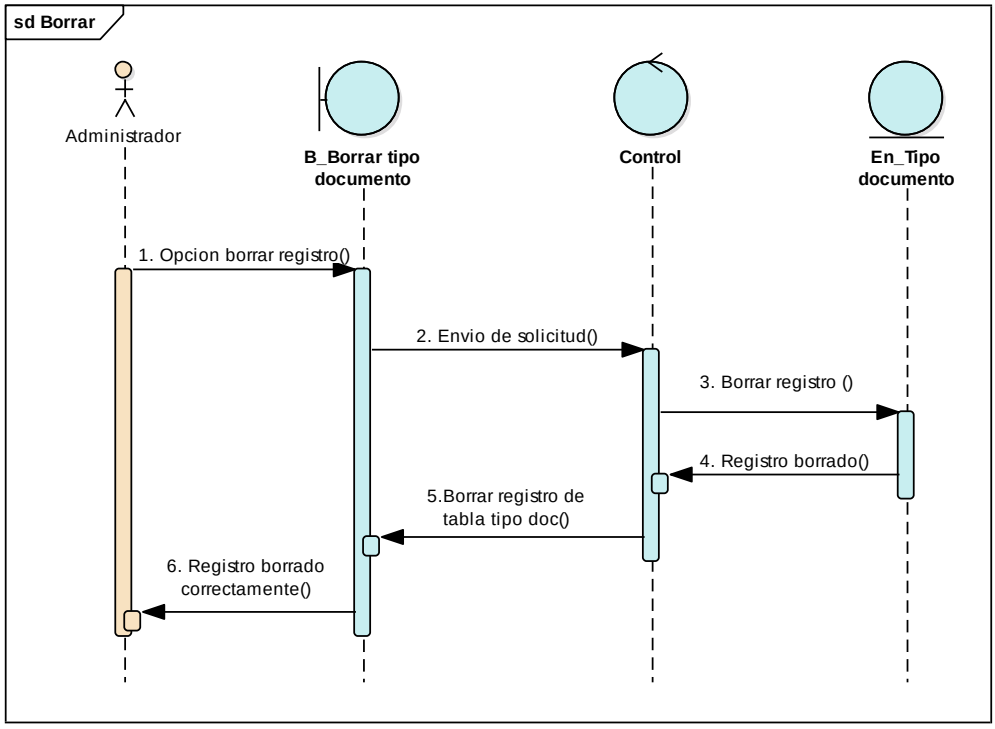


Figura 31 DS06-4 Borrar Tipo Documento

A continuación, se muestran los diagramas de secuencia del CRUD de Tipo de Persona:

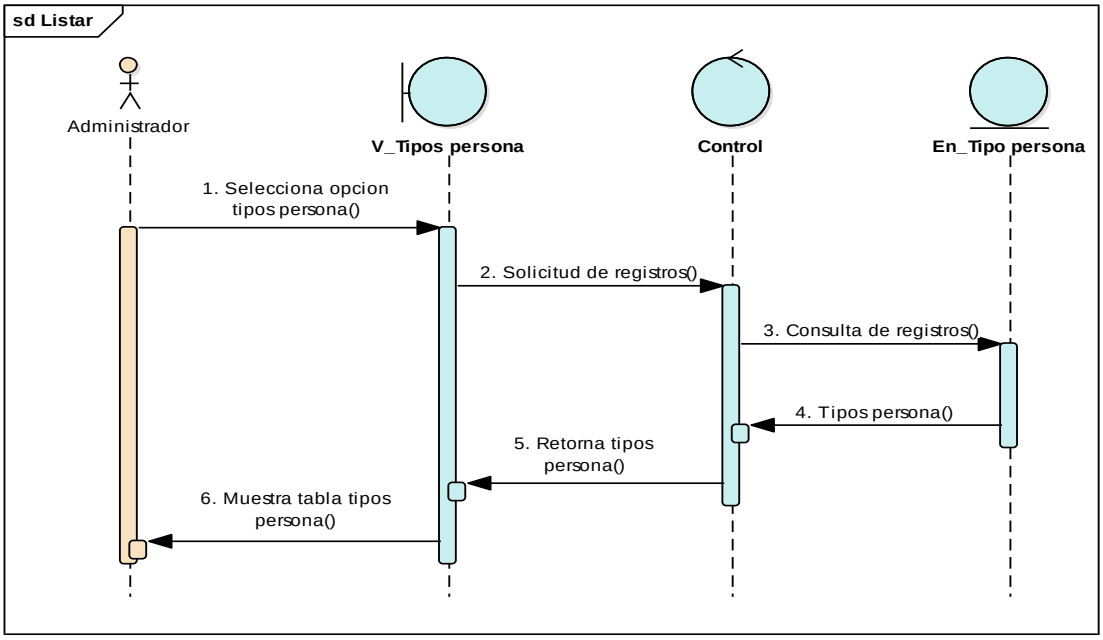


Figura 32 DS07-1 Listar Tipo Persona

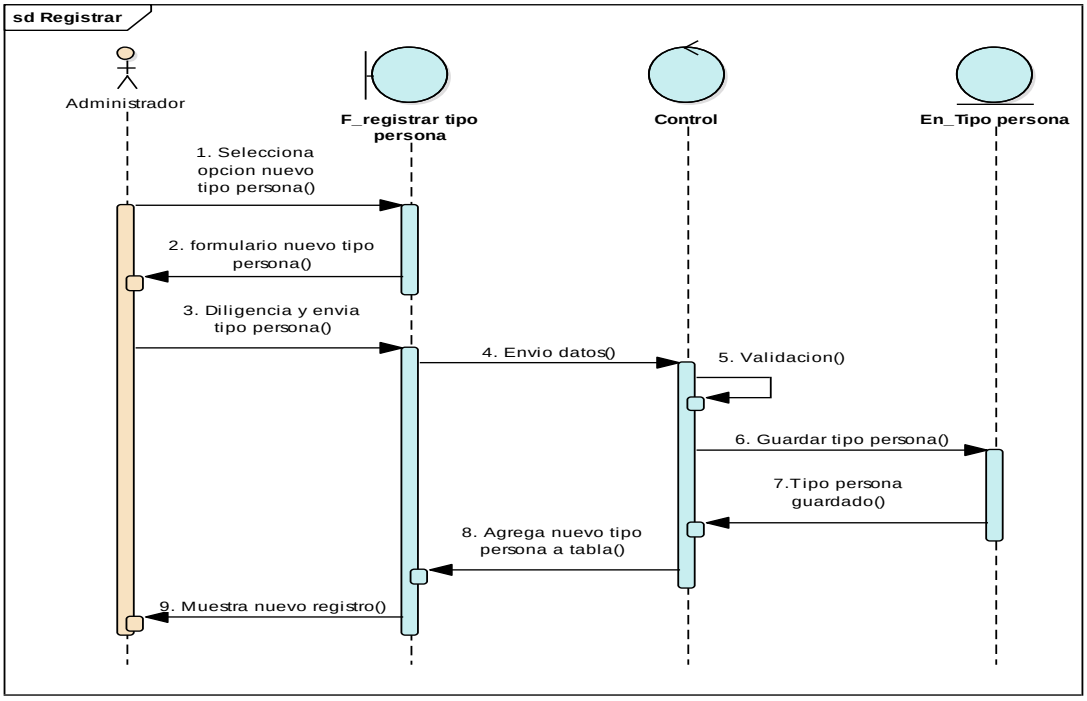


Figura 33 DS07-2 Registrar Tipo Persona

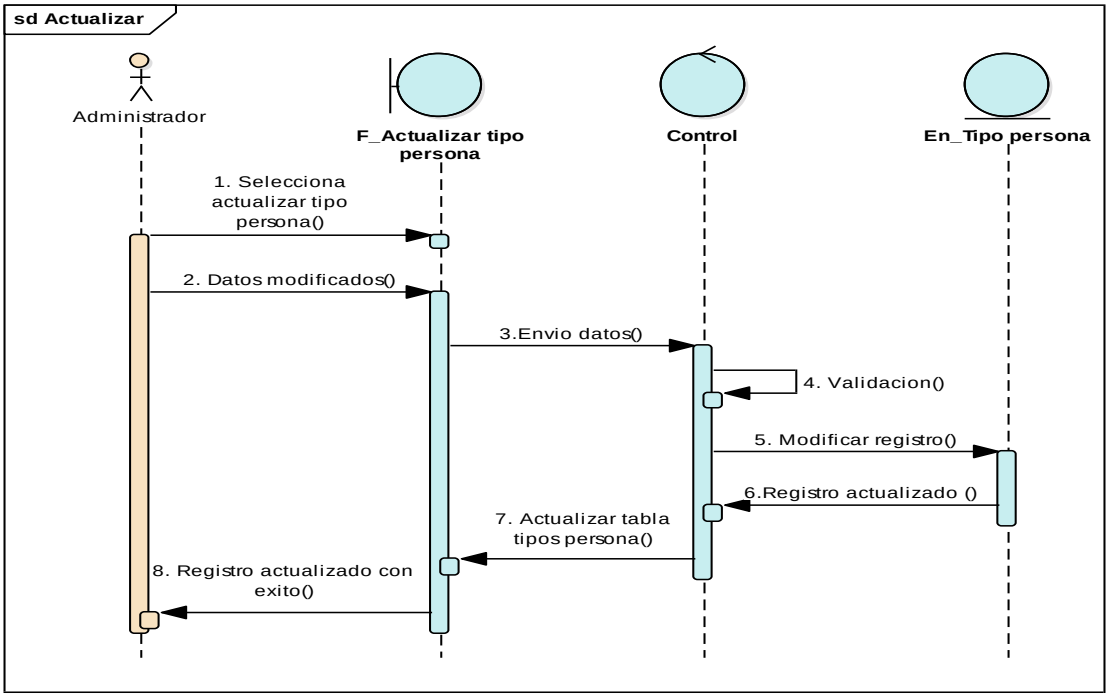


Figura 34 DS07-3 Actualizar Tipo Persona

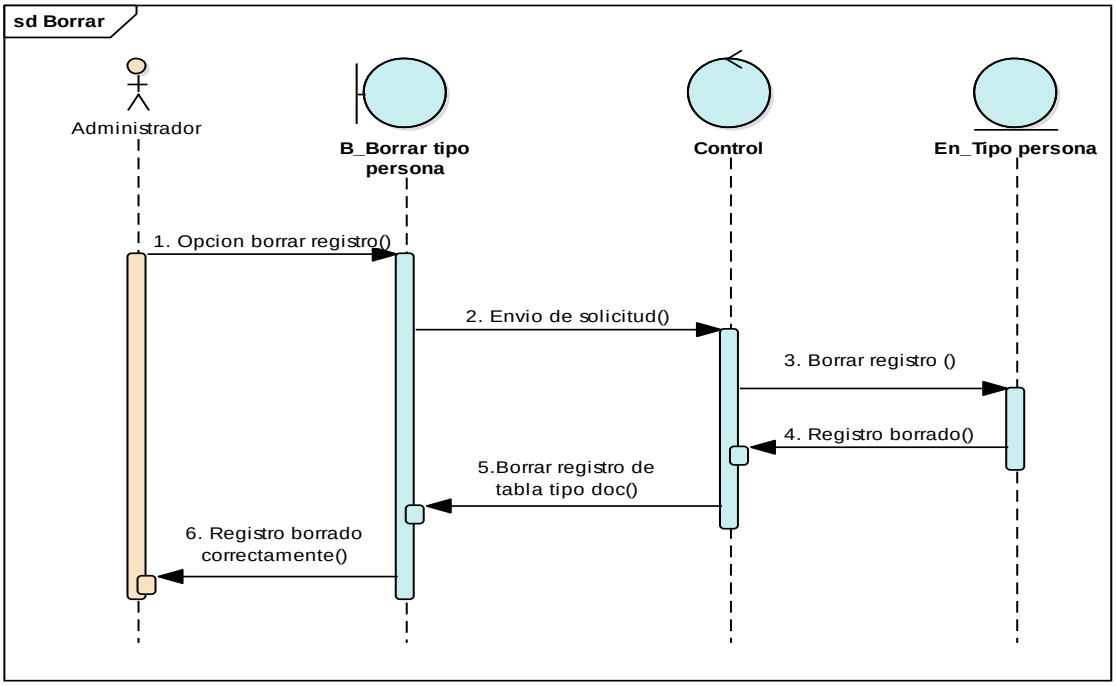


Figura 35 DS07-4 Borrar Tipo Persona

A continuación, se muestran los diagramas de secuencia del CRUD de Programa:

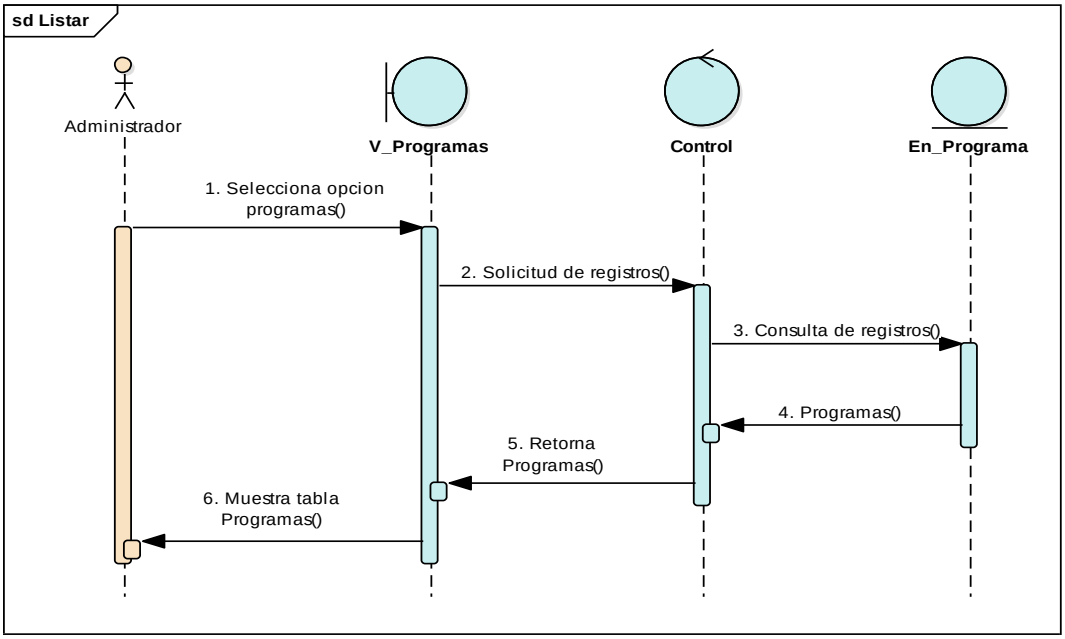


Figura 36 DS08-1 Listar Programa

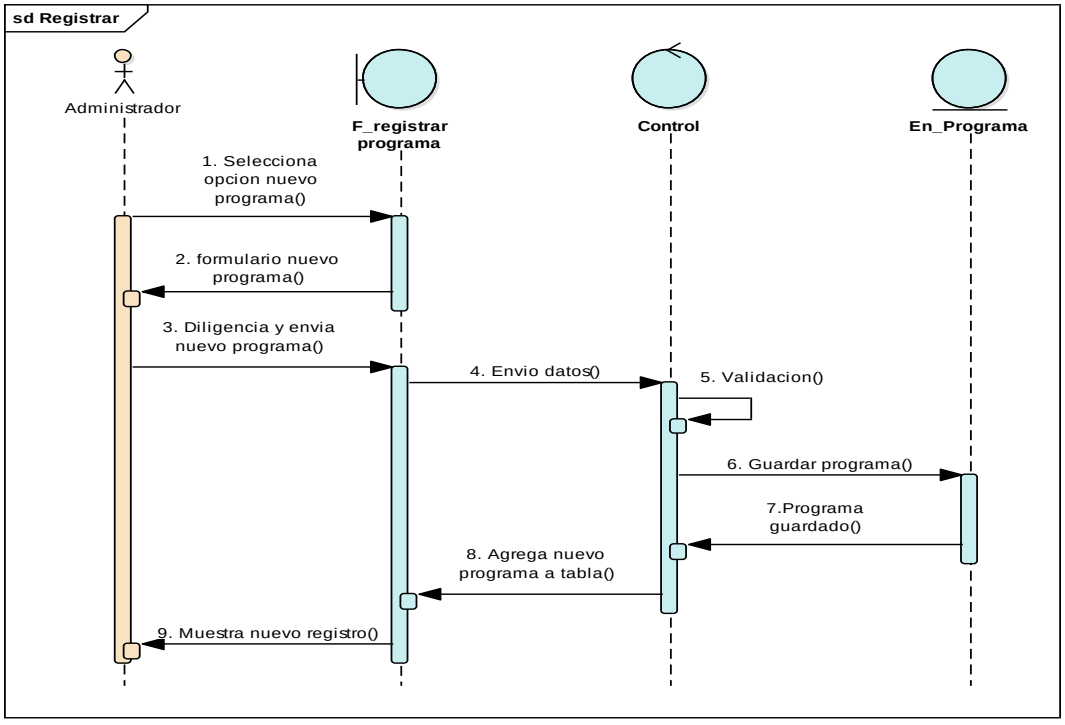


Figura 37 DS08-2 Registrar Programa

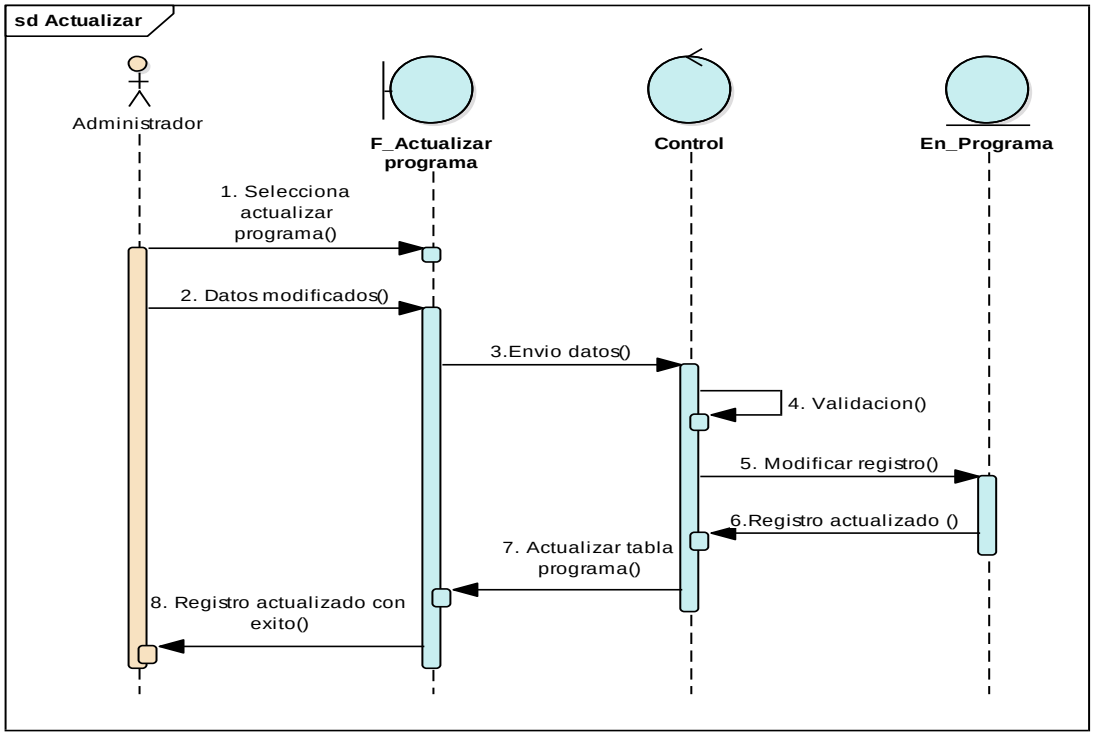


Figura 38 DS08-3 Actualizar Programa

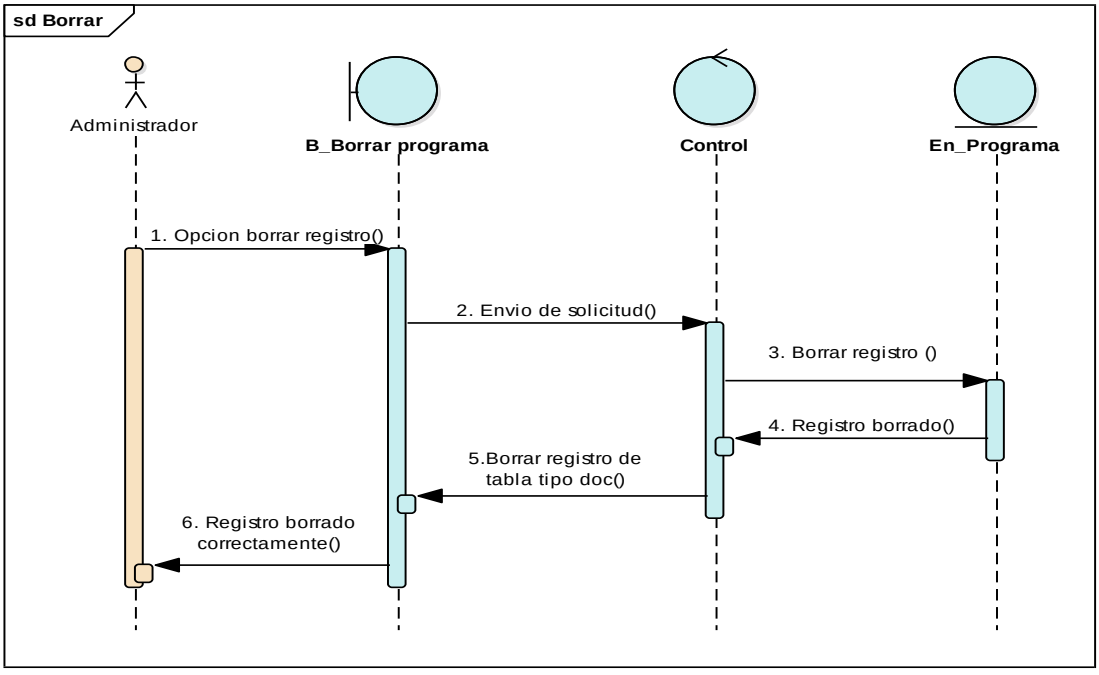


Figura 39 DS08-4 Borrar Programa

A continuación, se muestran los diagramas de secuencia del CRUD de Sede:

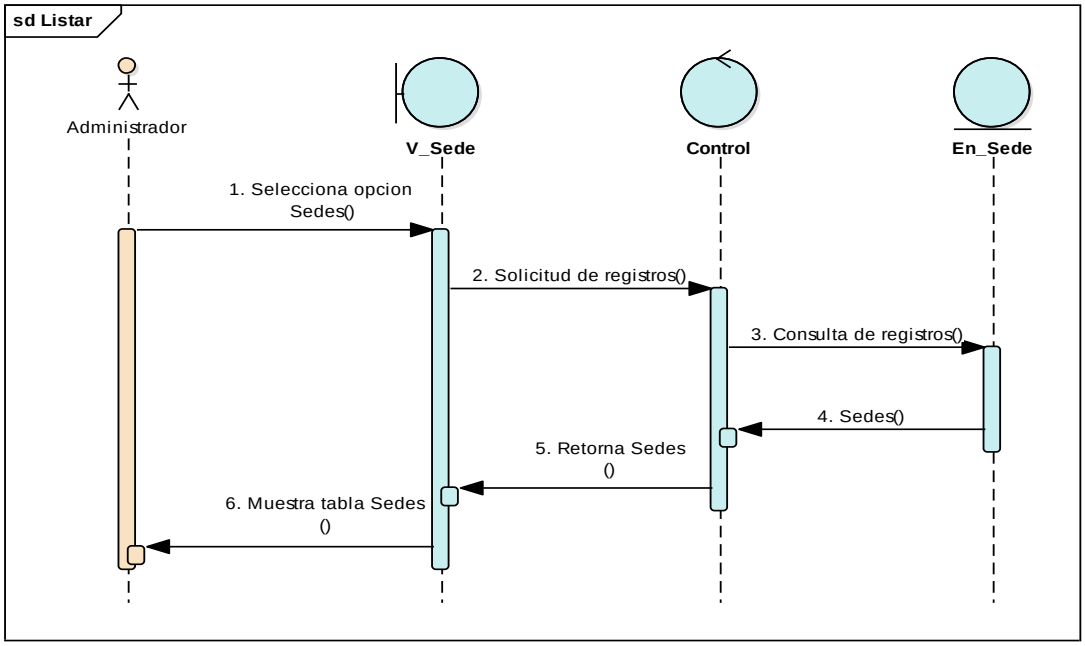


Figura 40 DS09-1 Listar Sede

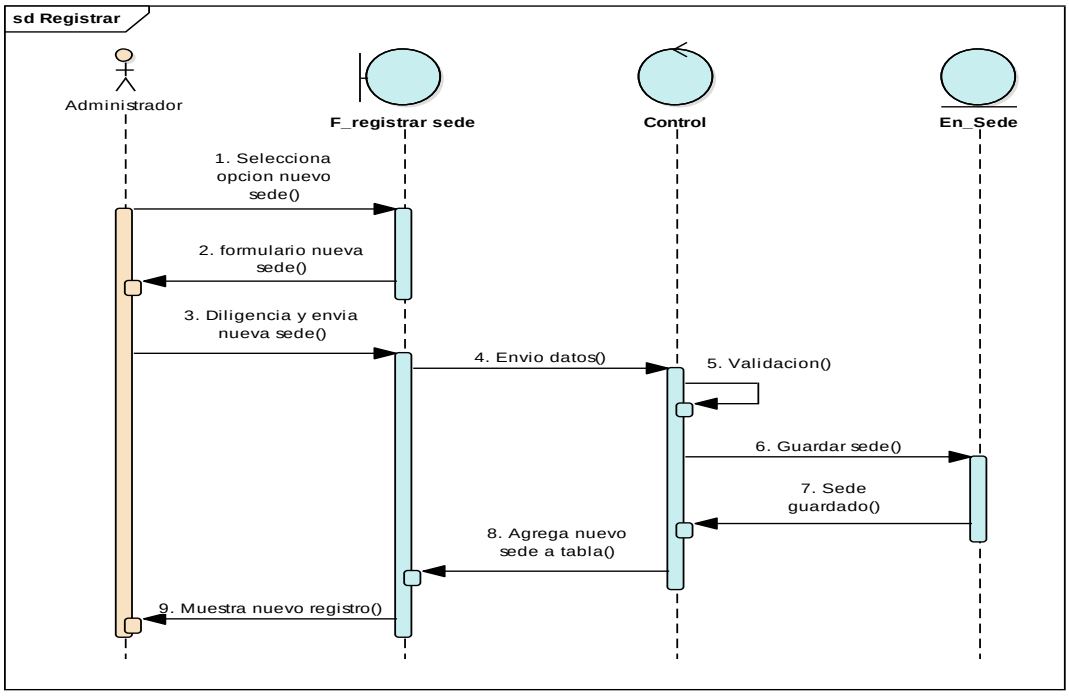


Figura 41 DS09-2 Registrar Sede

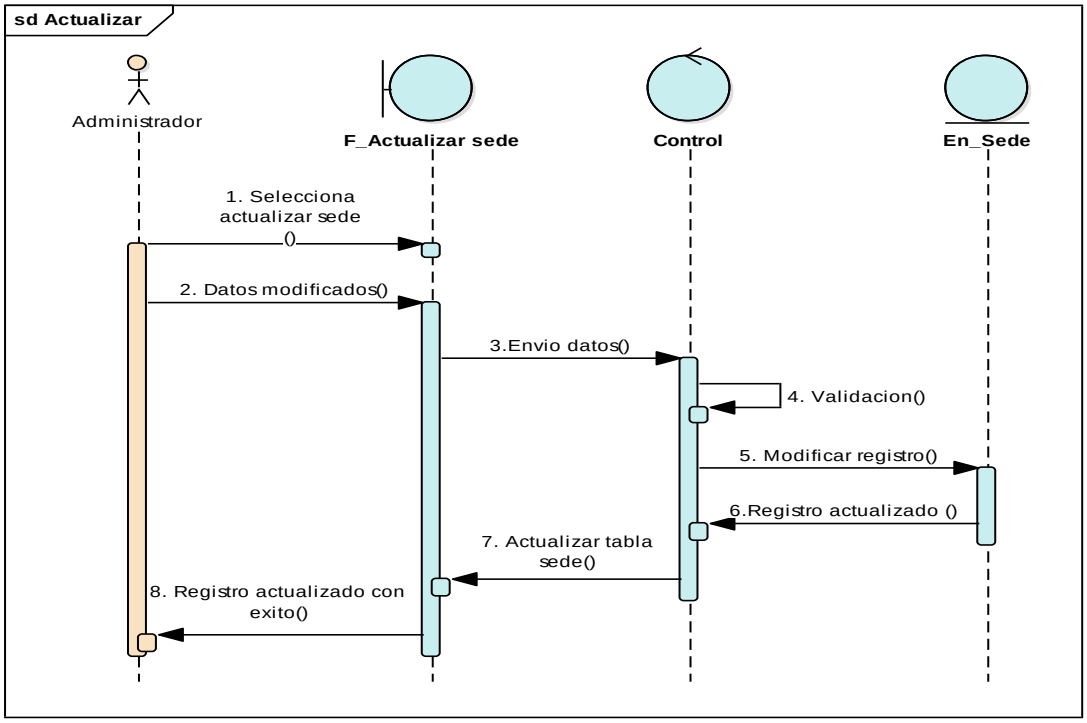


Figura 42 DS09-3 actualizar Sede

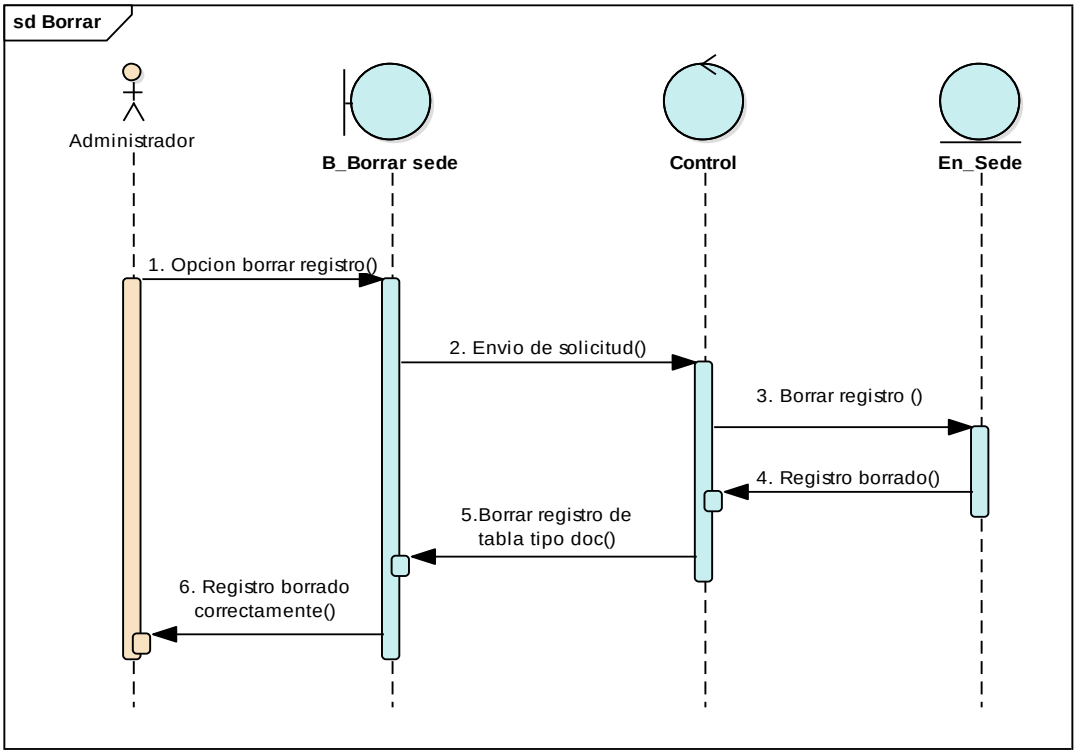


Figura 43 DS09-4 Borrar Sede

A continuación, se muestran los diagramas de secuencia del CRUD de Administrador:

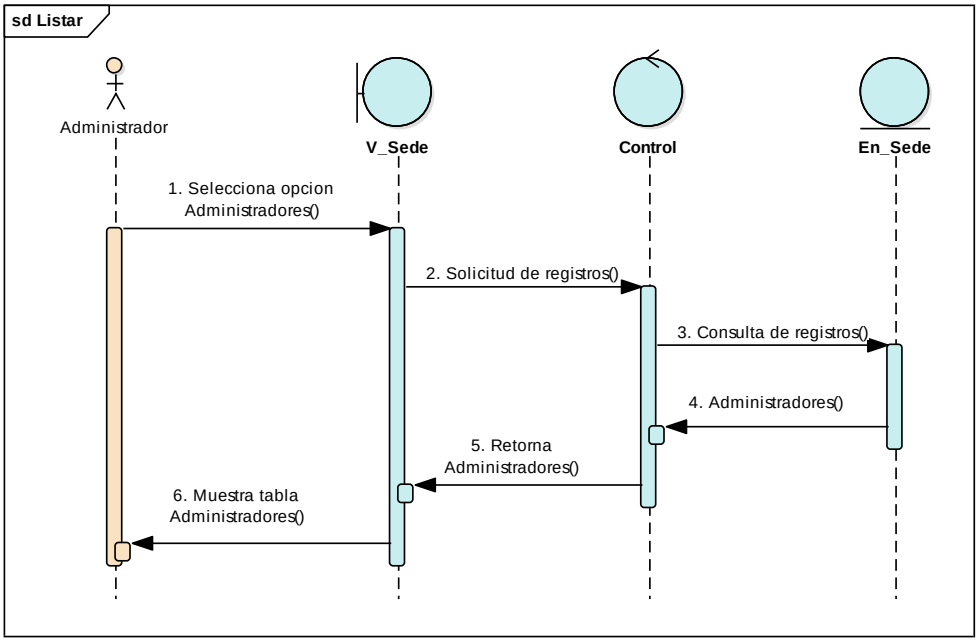


Figura 44 DS10-1 Listar Administrador

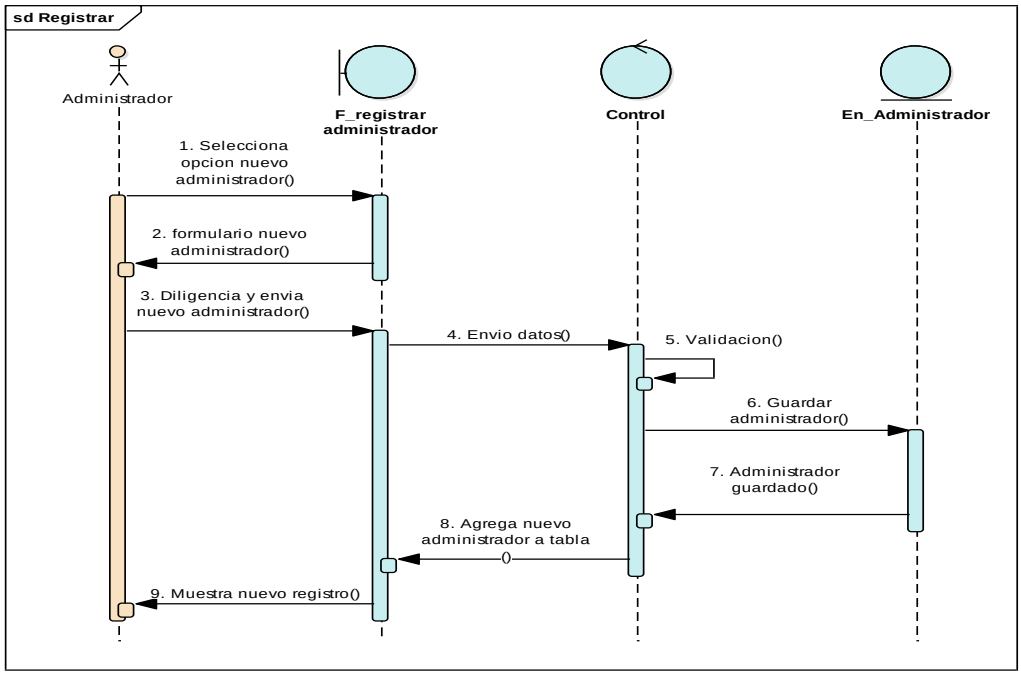


Figura 45 DS10-2 Registrar Administrador

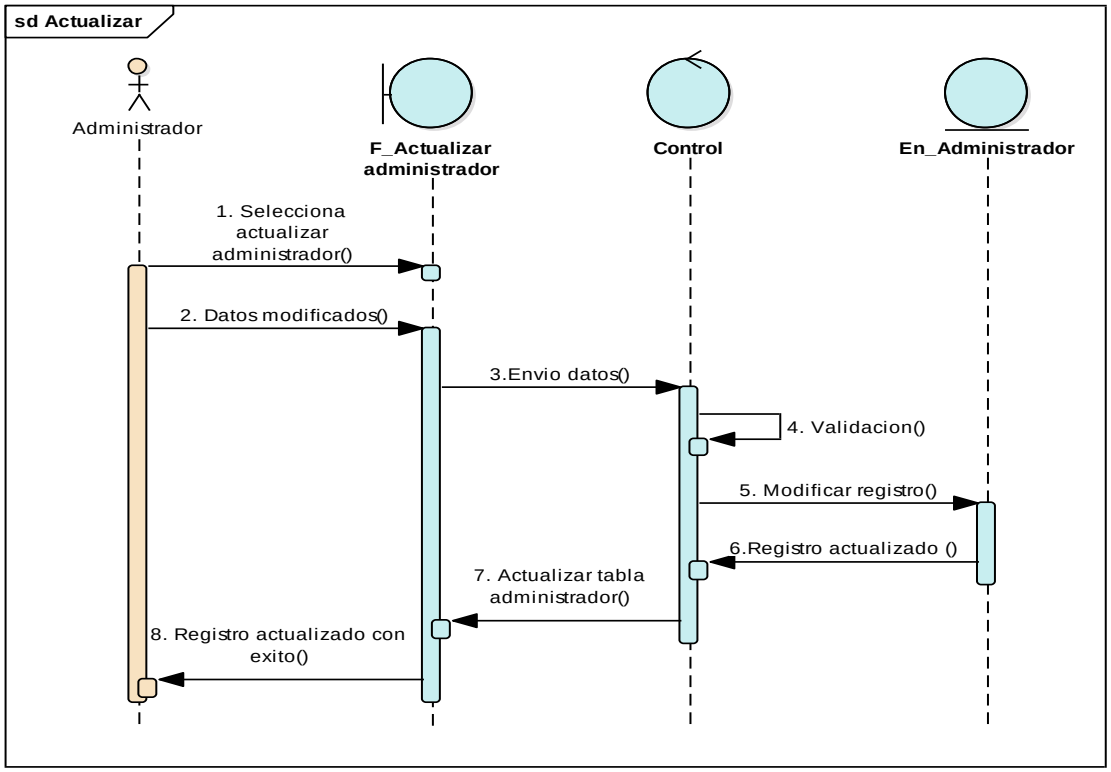


Figura 46 DS10-3 Actualizar Administrador

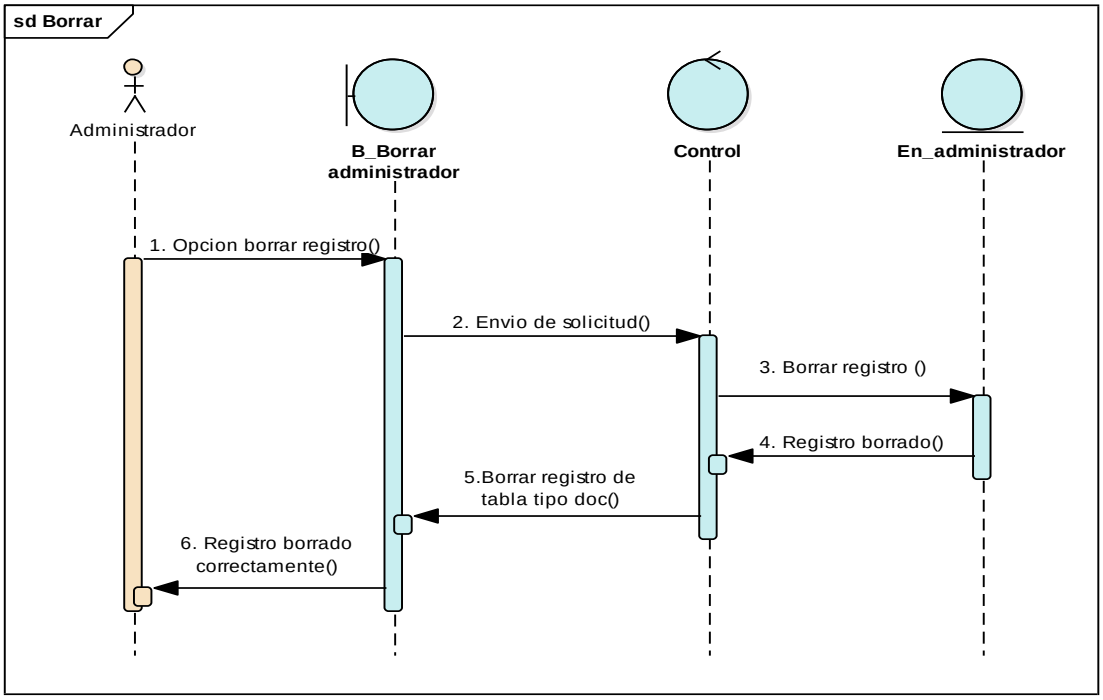


Figura 47 DS10-4 Borrar Administrador

A continuación, se muestran el diagrama de secuencia del caso de uso en el que el administrador puede buscar la información de votantes registrados en el módulo:

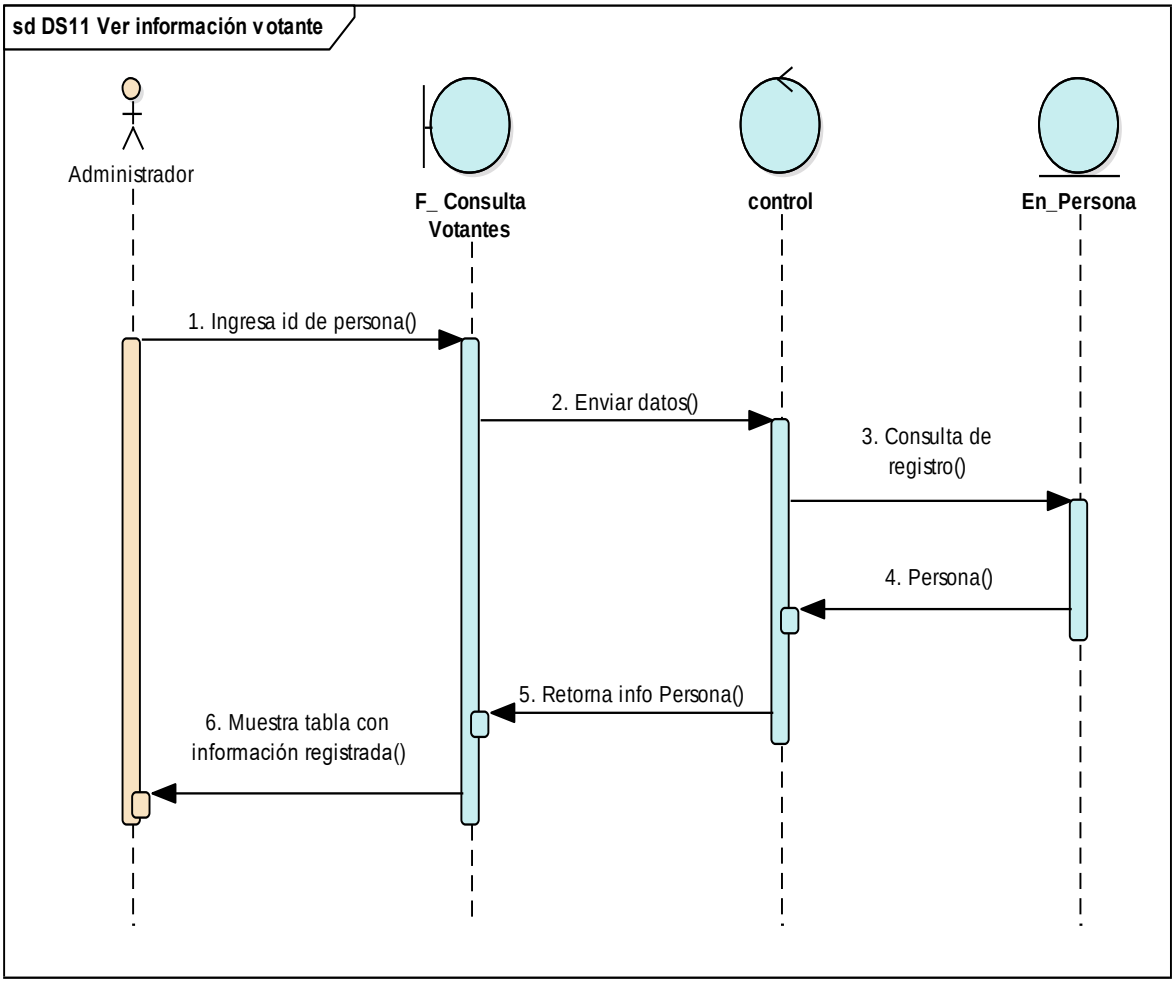


Figura 48 DS11 Ver Información Votante

2.3.5 Diagramas de actividades

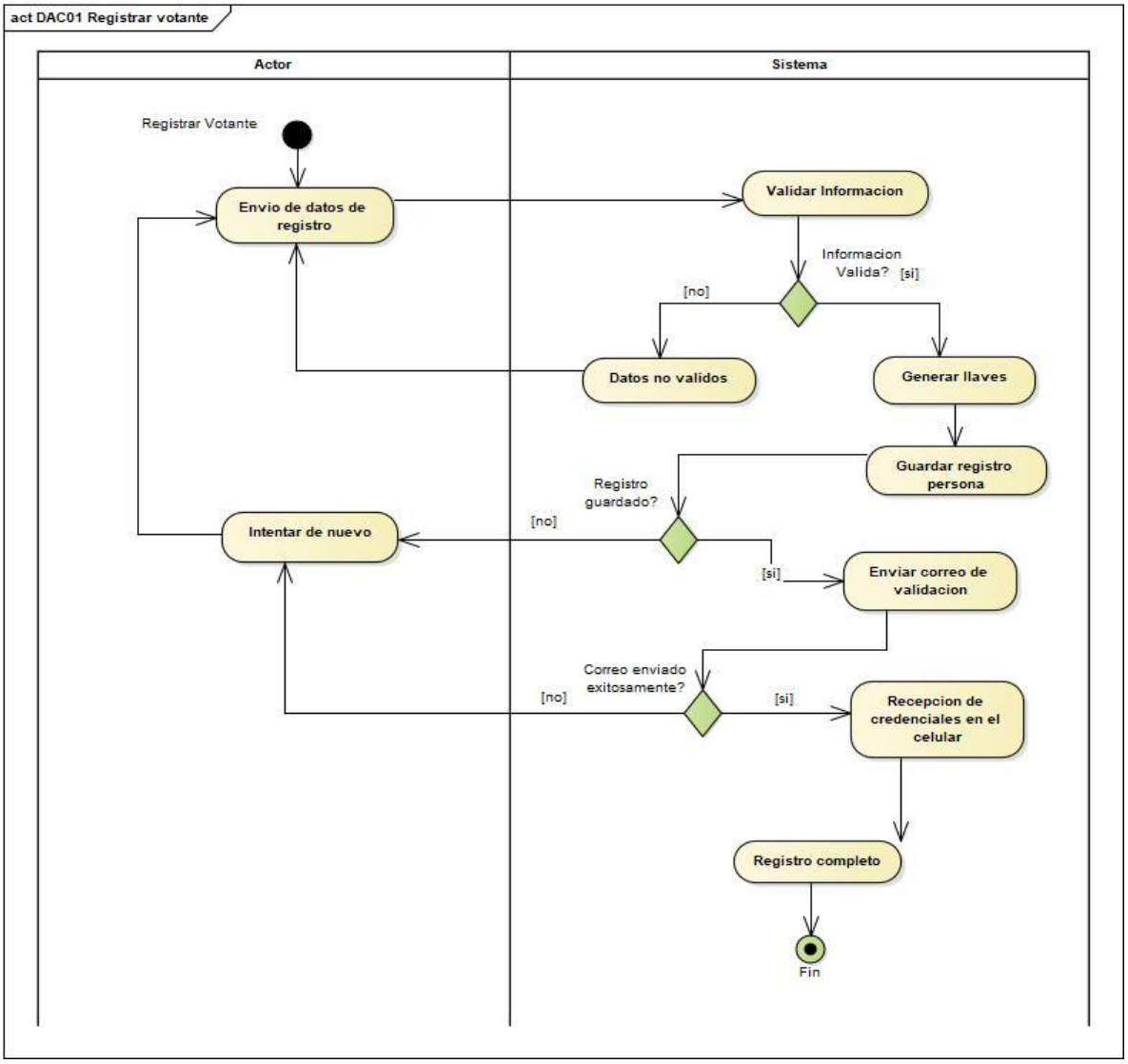


Figura 49 DAC01 Registrar Votante

Tabla 20 DAC01 Registrar Votante

Actividad	Descripción
Envió de datos de registro	El usuario diligencia el formulario y envía los datos necesarios para el registro.
Validar información	El sistema valida que los datos ingresados tengan un formato correcto, cumplan con los parámetros establecidos y que no existan registros con información repetida.
Datos no validos	El sistema devuelve mensaje “datos no validos”

Generar llaves	Genera par de llaves asimétricas
Guardar registro persona	El sistema almacena la información del usuario registrado en la base de datos
Valida base de datos	Se confirma que la información fue almacenada correctamente.
Enviar correo de validación	El sistema envía un correo con un código de validación a cada usuario que se registra
Almacenar llave privada	Se almacena localmente la llave privada en el teléfono móvil del usuario.
Intentar de nuevo	El usuario debe realizar nuevamente el proceso de registro.
Recepción de credenciales en el celular	El usuario ha obtenido y almacenado correctamente sus credenciales de acceso a la plataforma de voto por internet.

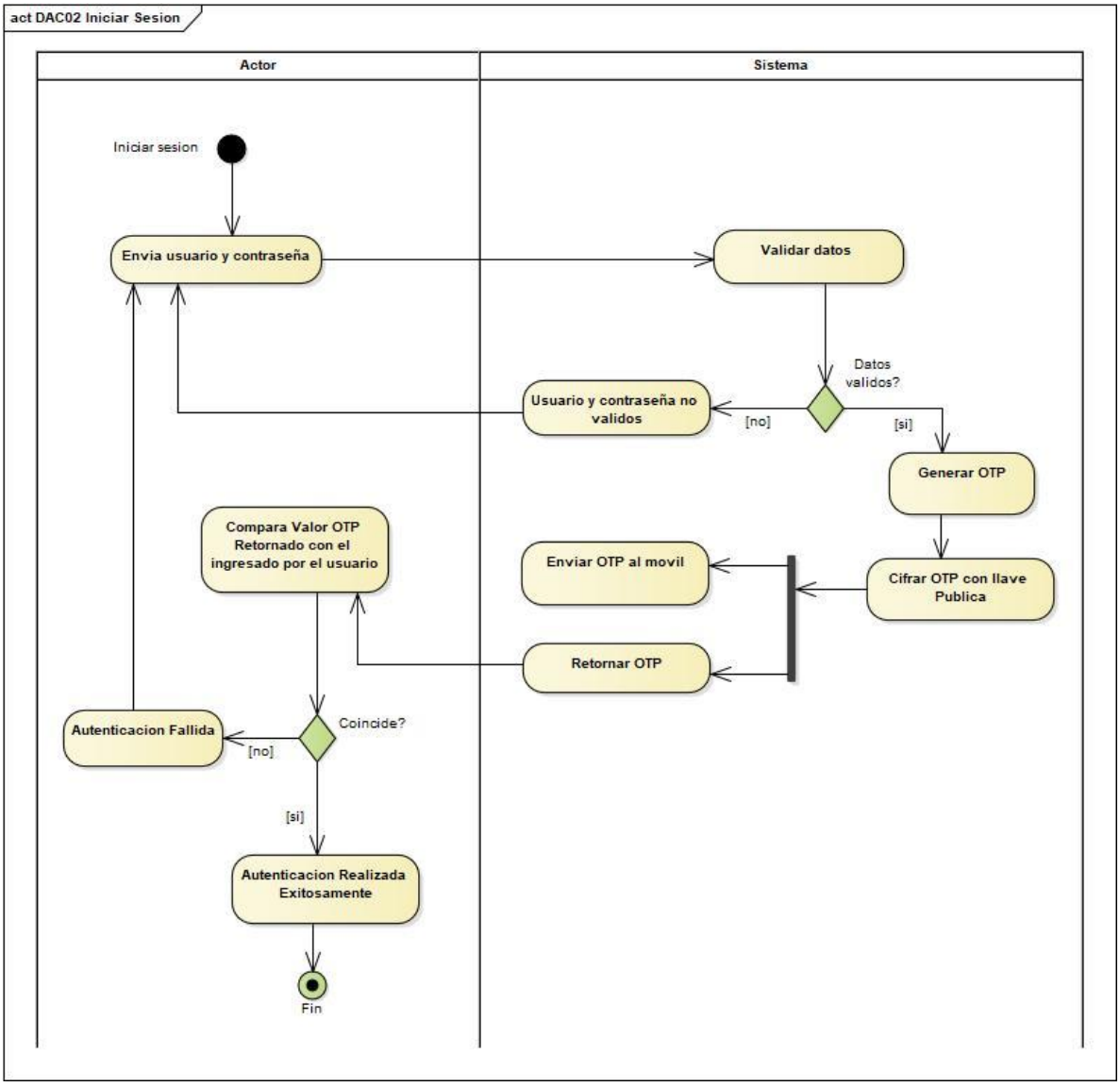


Figura 50 DAC02 Iniciar Sesión

Tabla 21 DAC02 Iniciar Sesión

Actividad	Descripción
Envió de usuario y contraseña	El usuario envía los datos necesarios para el inicio de sesión, en este caso inicialmente envía usuario (Numero de cedula) y contraseña.
Usuario y contraseña no validos	Retorna mensaje" Usuario y contraseña no validos"
Generar OTP	El sistema genera una OTP o clave de único uso.
Cifrar OTP con llave publica	Cifra la OTP generada con la llave publica del usuario.
Enviar OTP al móvil	Envió de la OTP cifrada al móvil del usuario para protocolo de desafío respuesta.
Retornar OTP	El servicio web retorna el valor de la OTP generada para el usuario que está tratando de acceder al sistema.
Comparar valor OTP retornado con el ingresado por el usuario	Protocolo de desafío respuesta en el que se válida la clave que fue cifrada y enviada al usuario
Autenticación fallida	El proceso de autenticación no se completó correctamente
Autenticación realizada exitosamente	El proceso de autenticación de usuario se realizó correctamente.

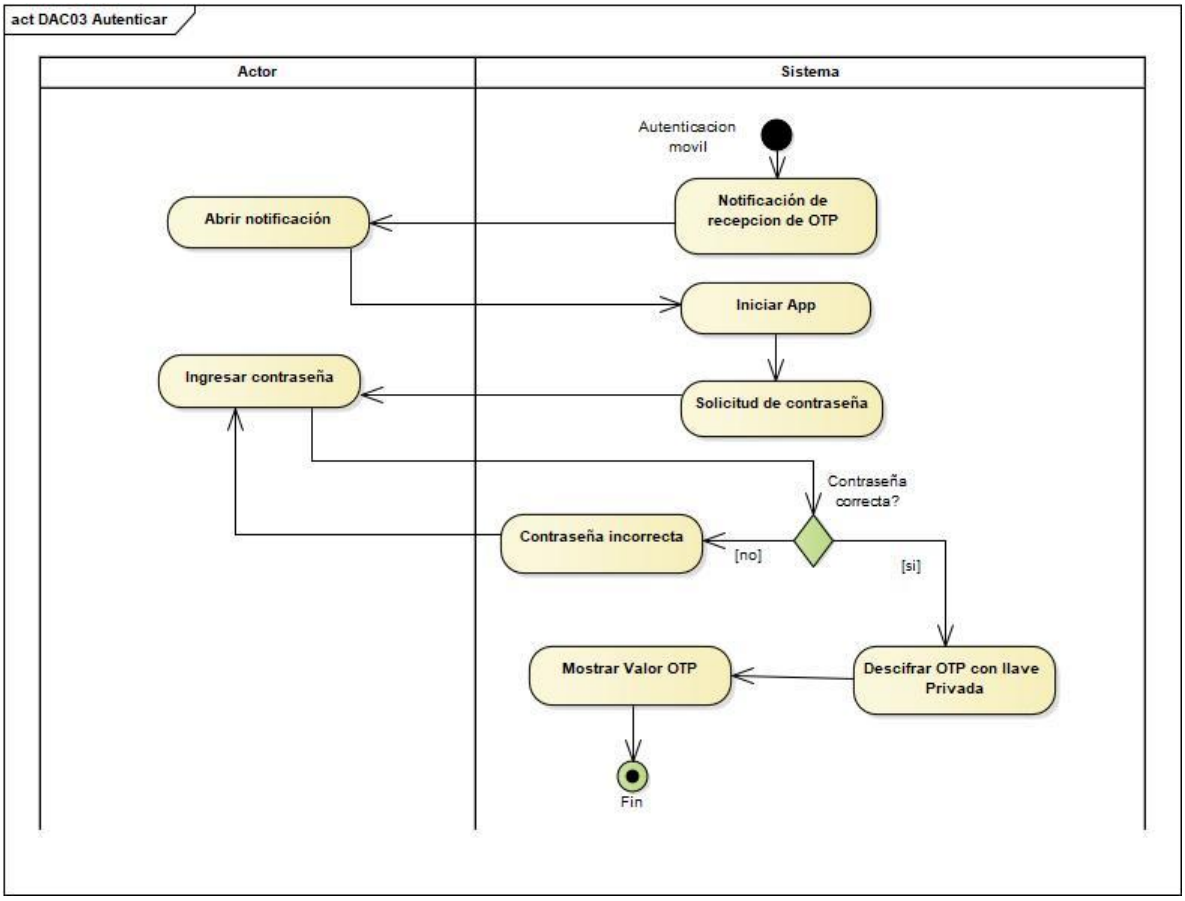


Figura 51 DAC03 Autenticar Votante

Tabla 22 DAC03 Autenticar Votante

Actividad	Descripción
Notificación de recepción de OTP	La aplicación móvil notifica que ha llegado la clave de acceso a la plataforma web.
Abrir notificación	El usuario presiona sobre la notificación del celular.
Iniciar App	La aplicación móvil se inicia en primer plano.
Solicitud de contraseña	La aplicación muestra campo para que el usuario ingrese su contraseña.
Ingresar contraseña	El usuario ingresa su contraseña.
Contraseña incorrecta	La contraseña no coincide.
Recepción de OTP cifrada	La aplicación móvil se encuentra en espera de la clave OTP para el proceso de autenticación.
Descifrar OTP con llave privada	Cuando La aplicación recibe una OTP, automáticamente la descifra con la llave privada del usuario.
Muestra Valor OTP	La aplicación muestra el valor de la OTP descifrada al usuario.

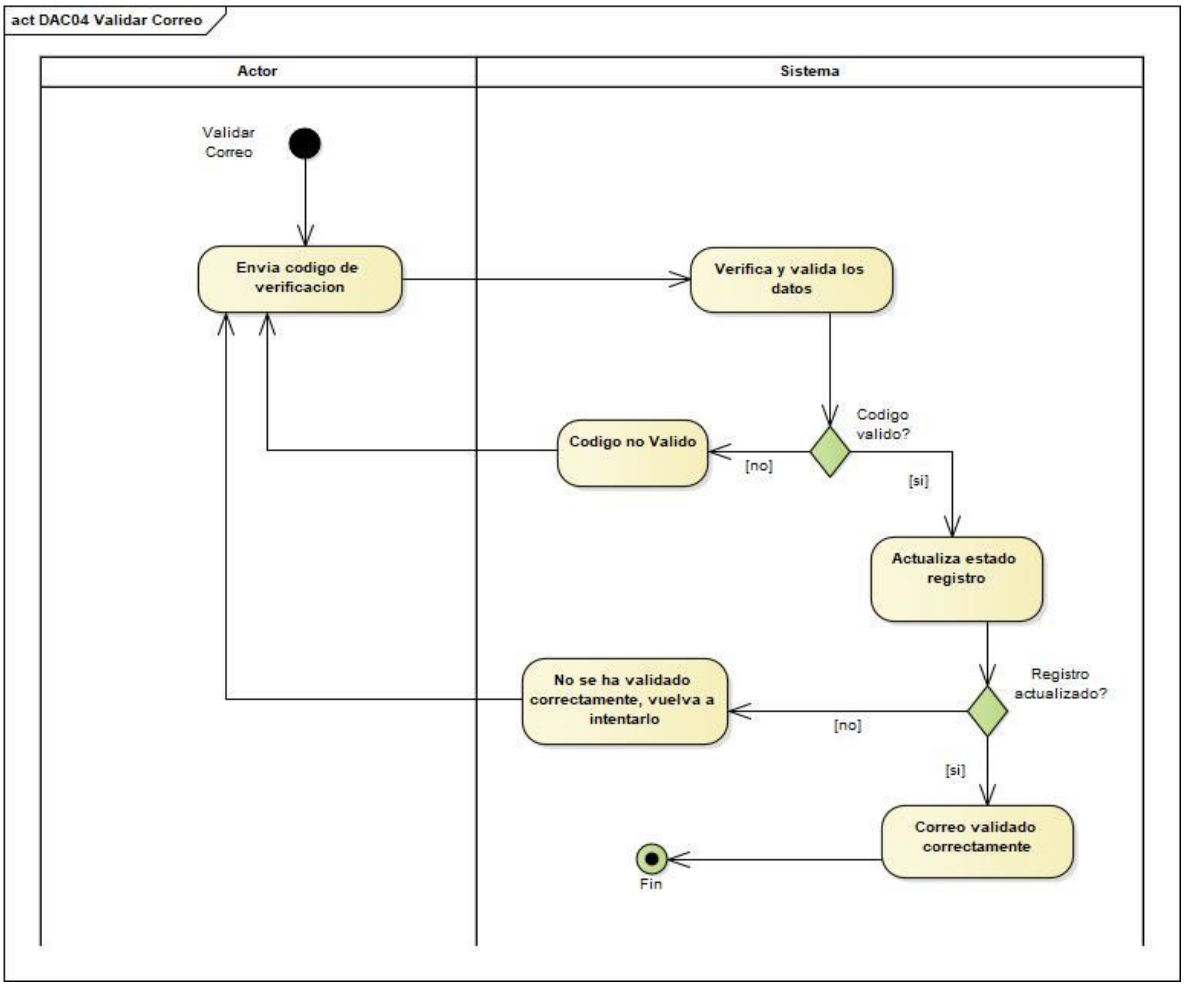


Figura 52 DAC04 Validar Correo

Tabla 23 DAC04 Validar Correo

Actividad	Descripción
Enviar Código de verificación	El usuario ingresa el código de verificación que fue enviado al correo electrónico asociado a su cuenta.
Verifica y valida los datos	Valida que coincida el código de verificación con los datos del usuario.
Código no valido	Retorna mensaje “el código de verificación no es válido”.
Actualiza el estado del registro.	El sistema actualiza el estado del usuario registrado de: “Inactivo” a: “Activo”.
No se ha validado correctamente, vuelva a intentarlo	No se ha podido actualizar estado del usuario, retorna mensaje “Vuelva a intentarlo”
Correo validado correctamente	El proceso de validación de correo se ha completado correctamente. Retorna mensaje “Correo validado exitosamente”

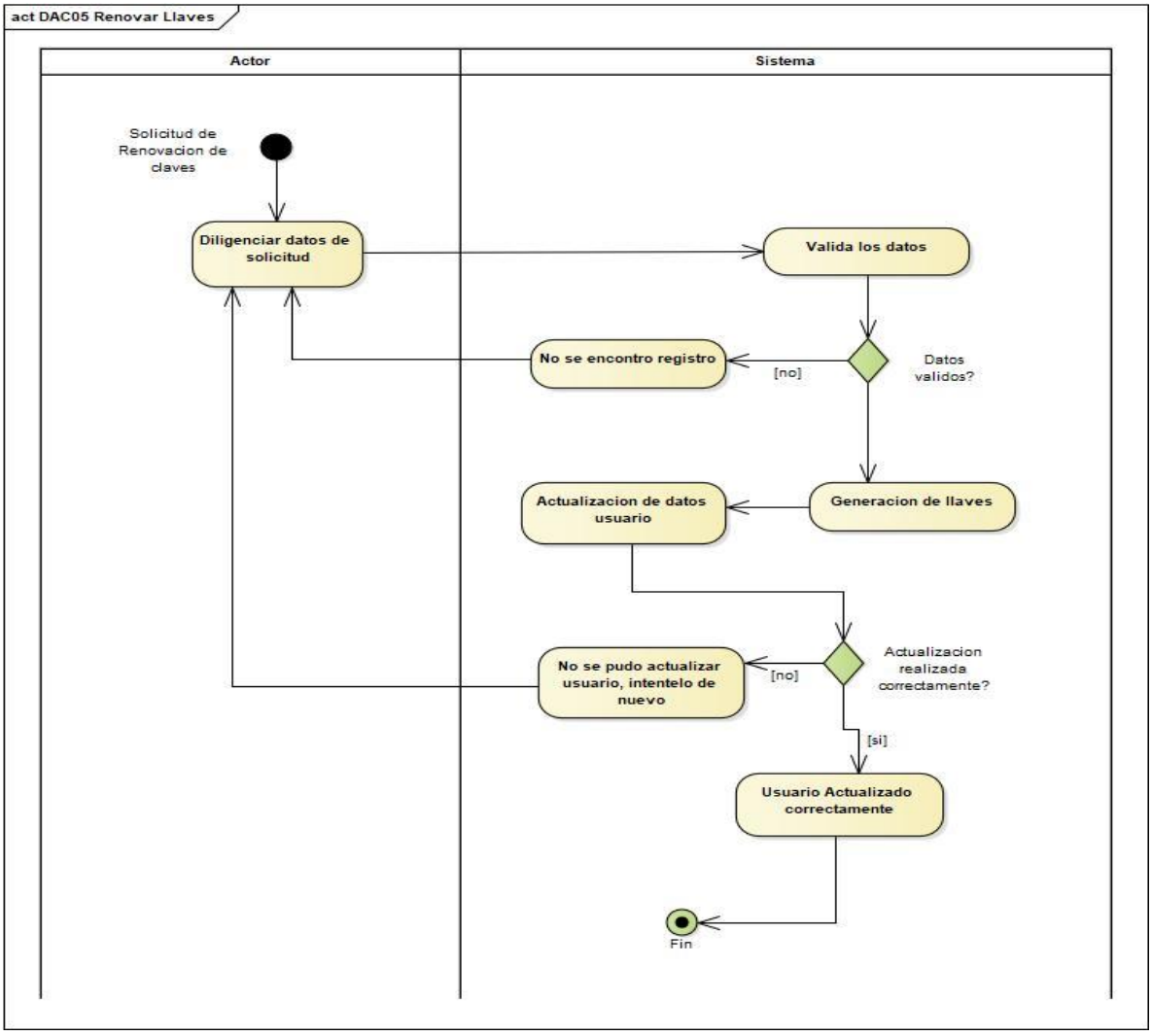


Figura 53 DAC05 Renovar Llaves

Tabla 24 DAC05 Renovar Llaves

Actividad	Descripción
Diligenciar datos de solicitud	El usuario envía los datos requeridos para la solicitud de renovación de claves
Valida los datos	Verifica que exista registro de la persona que solicita la renovación de claves.
No se encontró registro	En caso de no encontrar registro del usuario que solicita la renovación de claves retorna mensaje “No se encontró registro”
Generación de llaves	Genera nuevo par de llaves para el usuario.
Actualización de datos del usuario	El sistema actualiza los datos del usuario relacionados con la llave asimétrica y el número telefónico.
No se ha podido actualizar usuario	No se han realizado los cambios en la base de datos.
Usuario actualizado correctamente	Los cambios en el registro del usuario se han realizado correctamente en la base de datos.

A continuación, se presentan los diagramas de actividades relacionados con los CRUD que realiza el administrador desde la plataforma web del módulo de autenticación.

DAC06 CRUD Tipo Documento

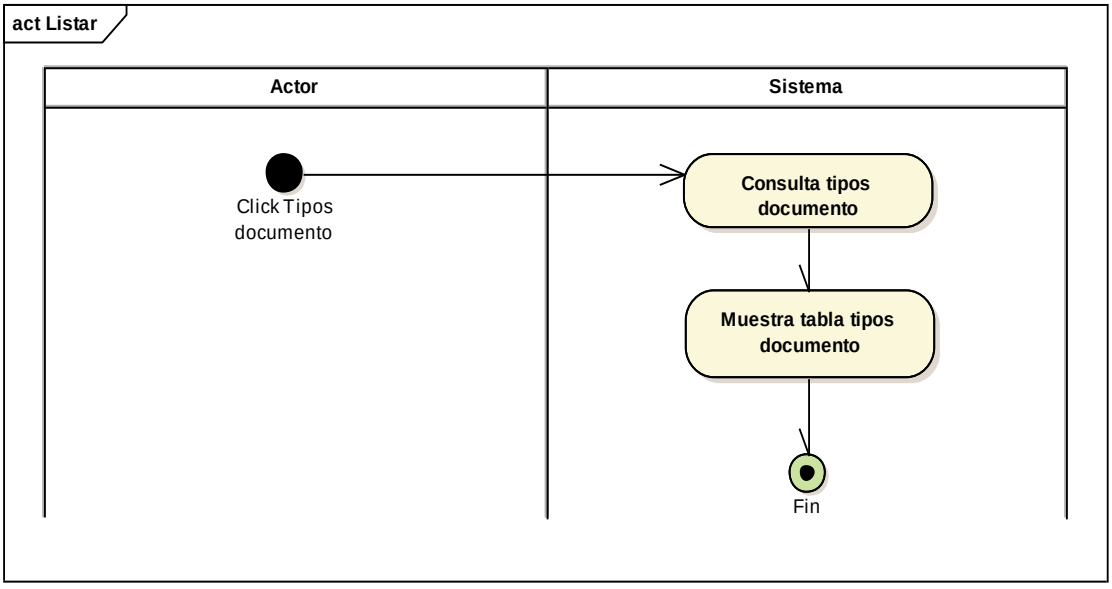


Figura 54 DAC06-1 Listar Tipo Documento

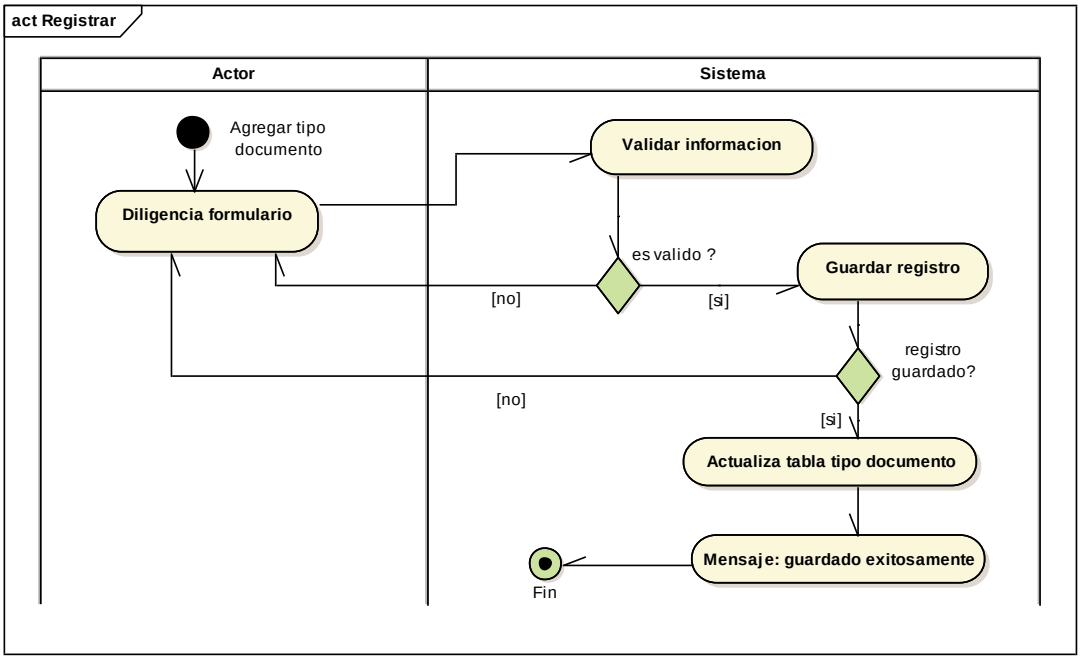


Figura 55 DAC06-2 Registrar Tipo Documento

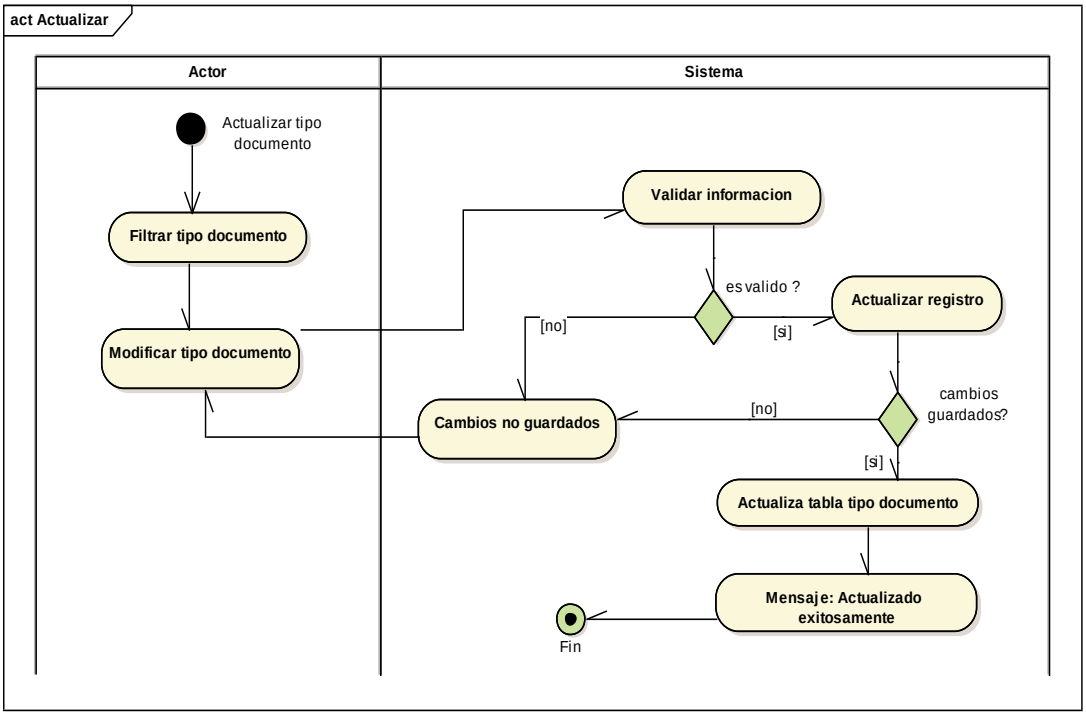


Figura 56 DAC06-3 Actualizar Tipo Documento

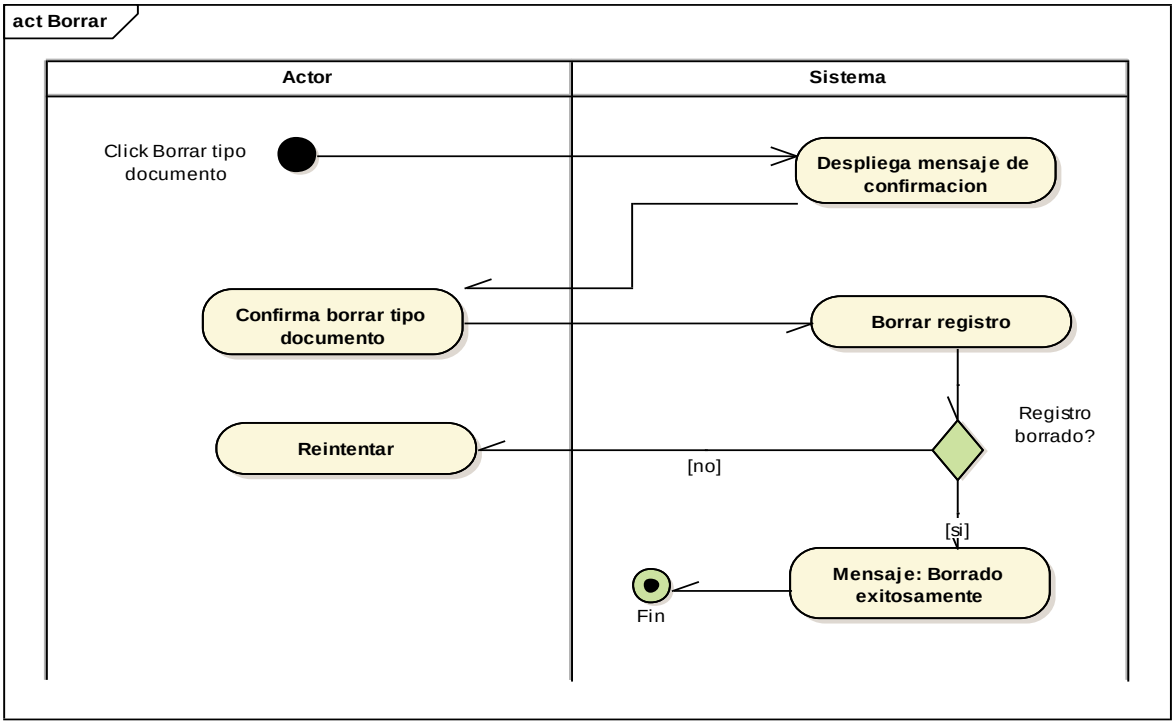


Figura 57 DAC06-4 Borrar Tipo Documento

DAC07 CRUD Tipo Persona

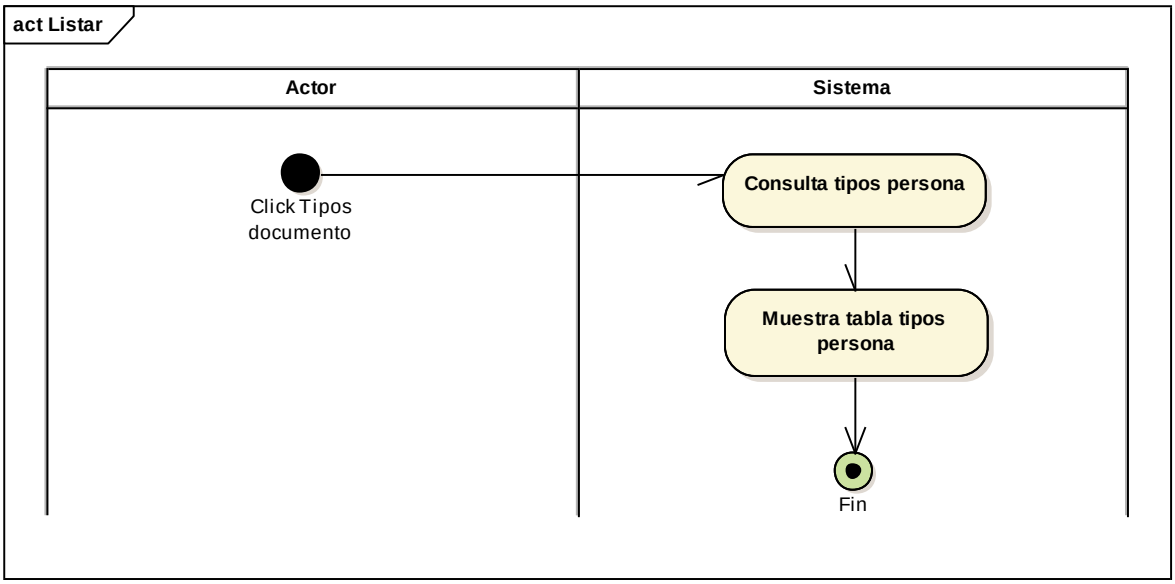


Figura 58 DAC07-1 Listar Tipo Persona

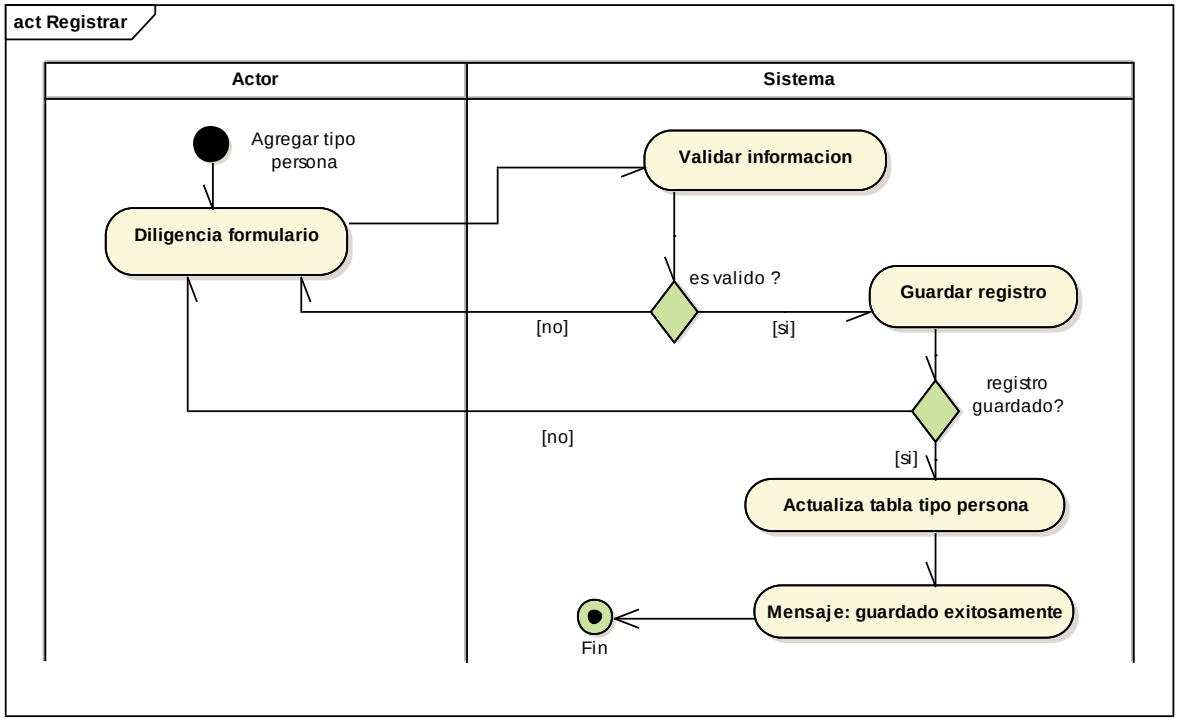


Figura 59 DAC07-2 Registrar Tipo Persona

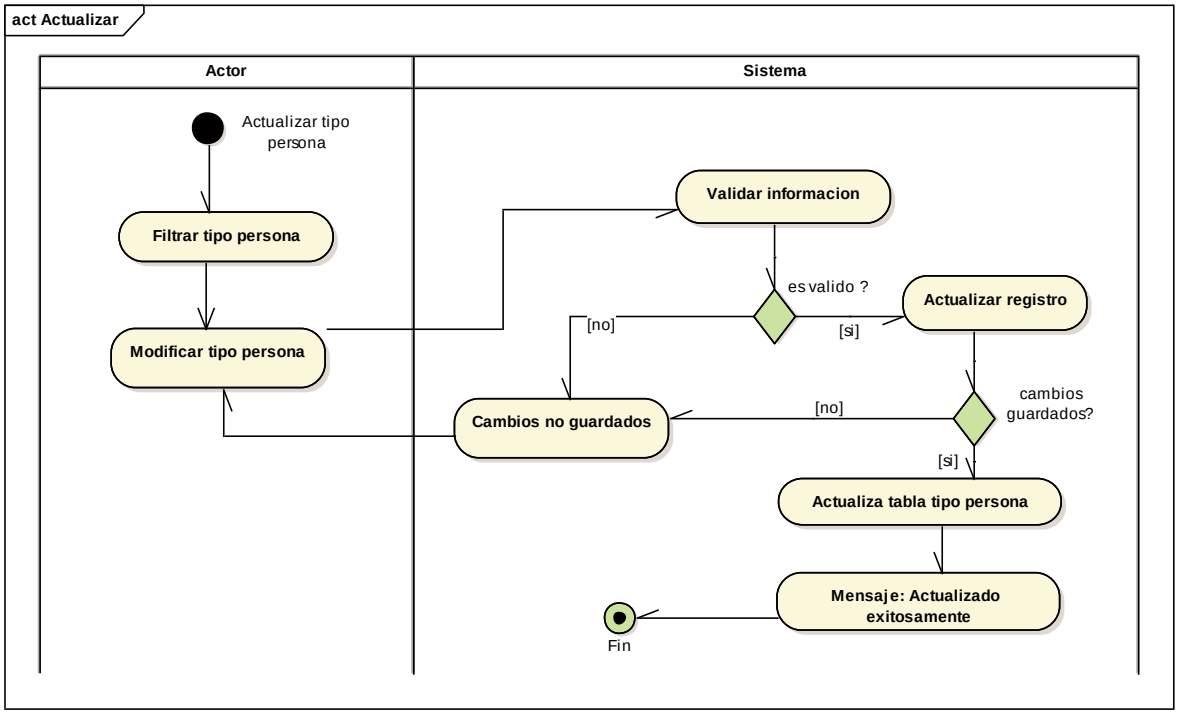


Figura 60 DAC07-3 Actualizar Tipo Persona

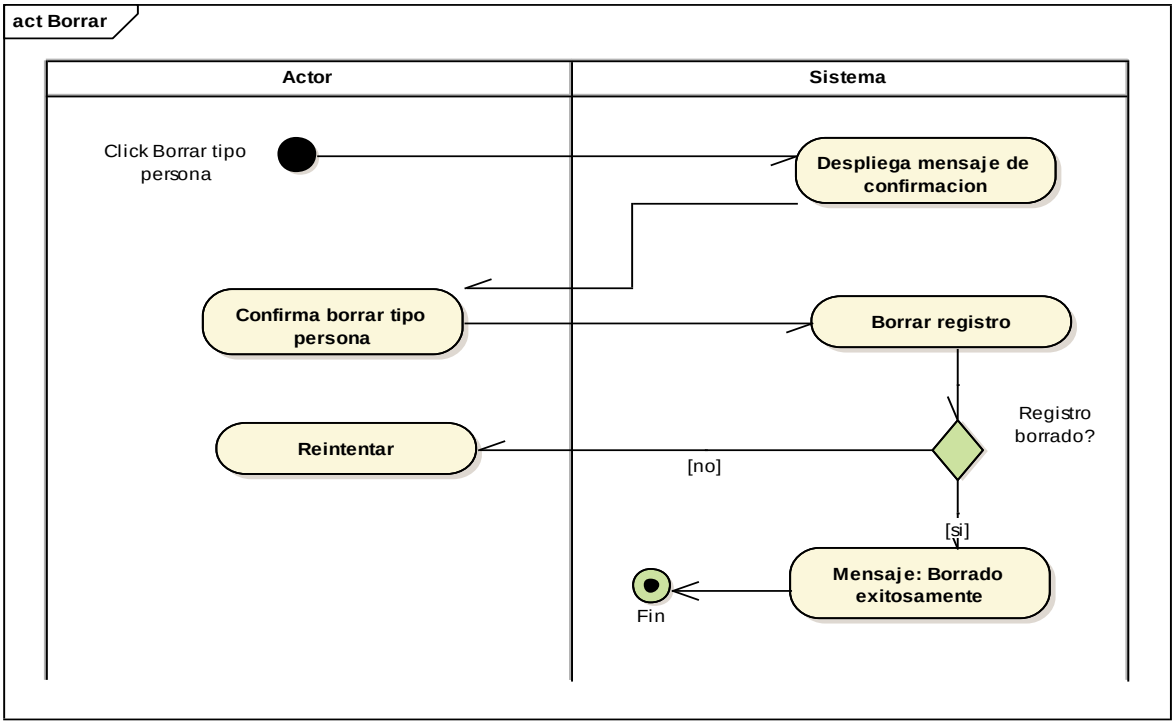


Figura 61 DAC07-4 Borrar Tipo Persona

DAC08 CRUD Programa

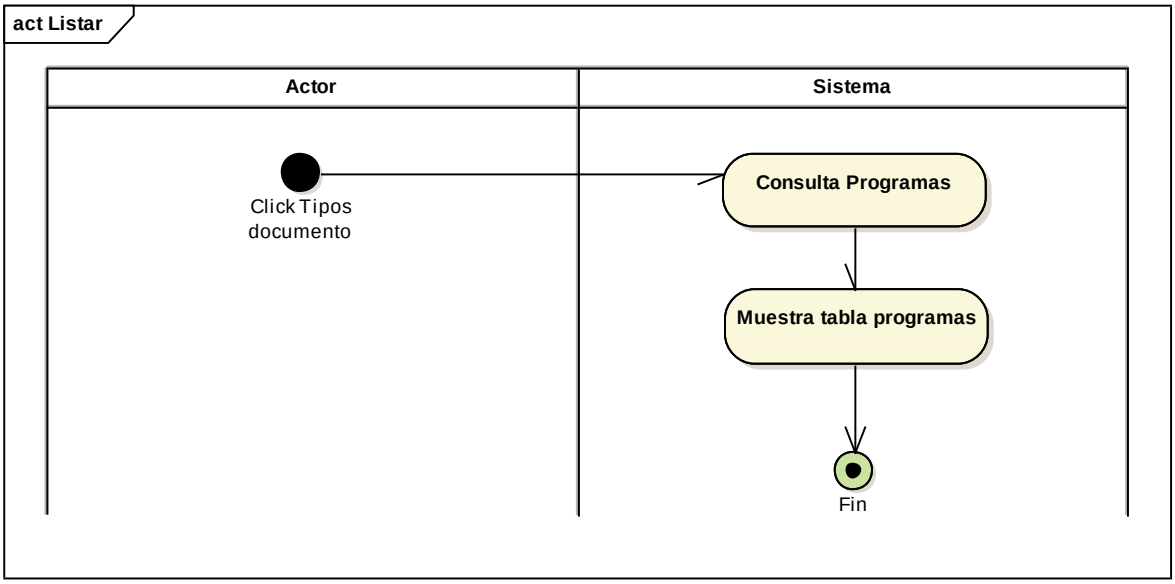


Figura 62 DAC08-1 Listar Programa

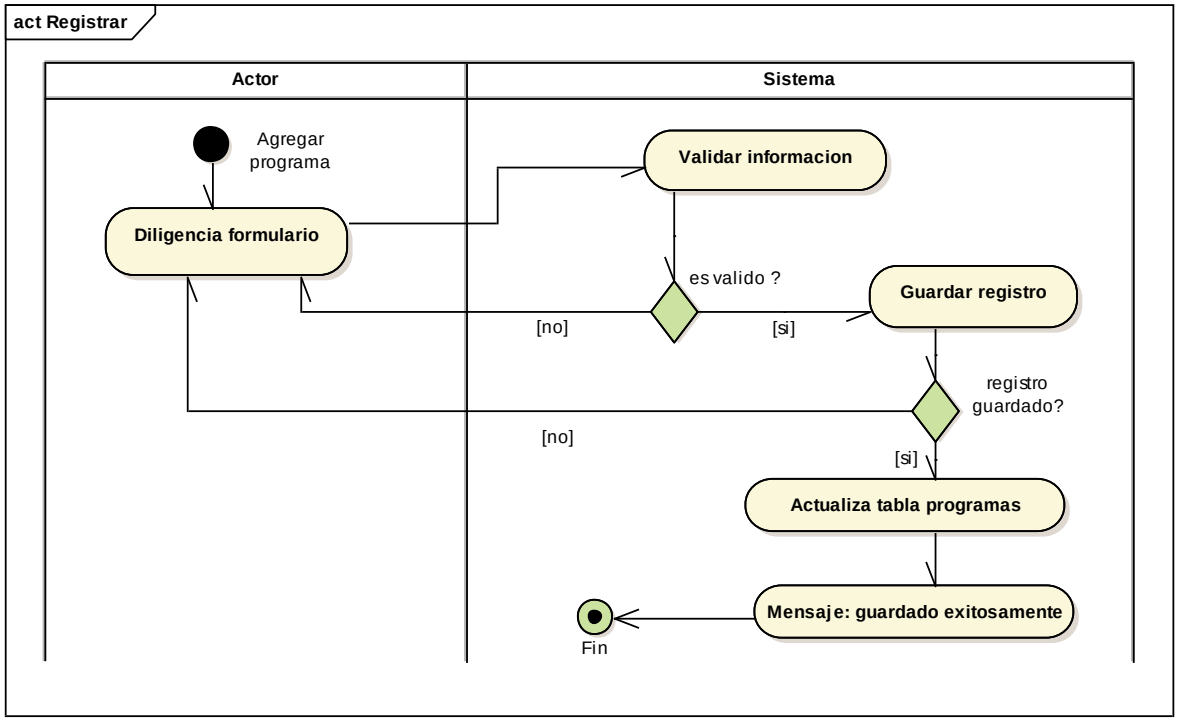


Figura 63 DAC08-2 Registrar Programa

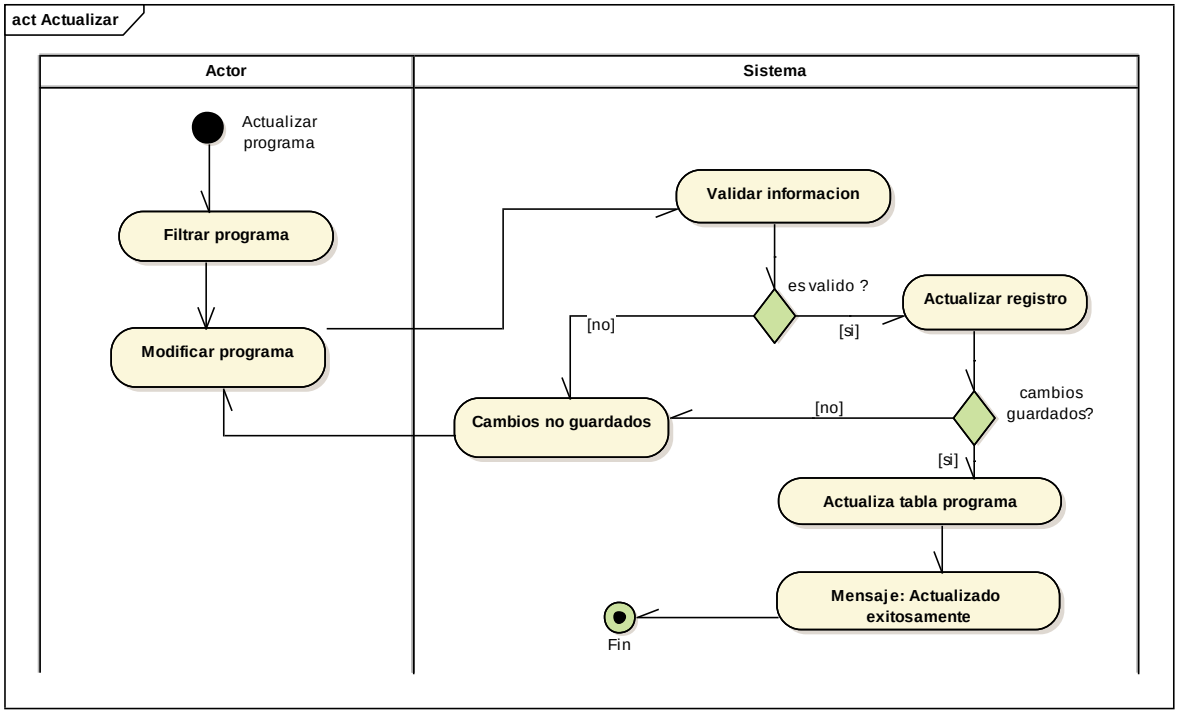


Figura 64 DAC08-3 Actualizar Programa

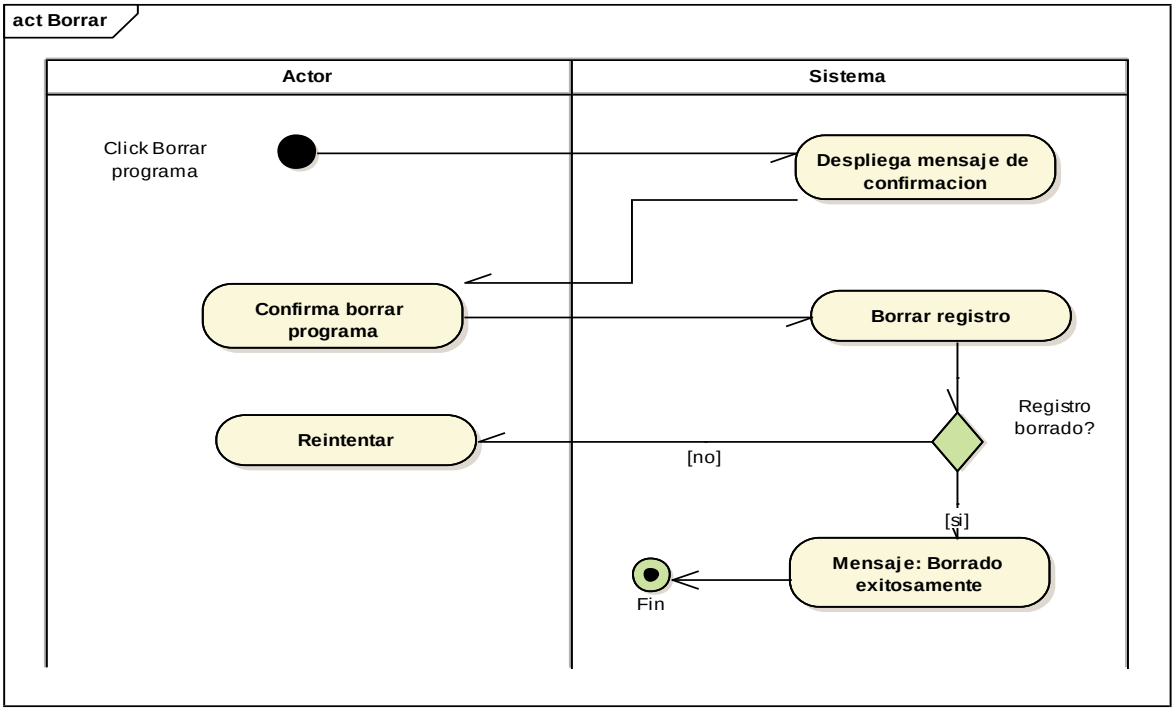


Figura 65 DAC08-4 Borrar Programa

DAC09 CRUD Sede

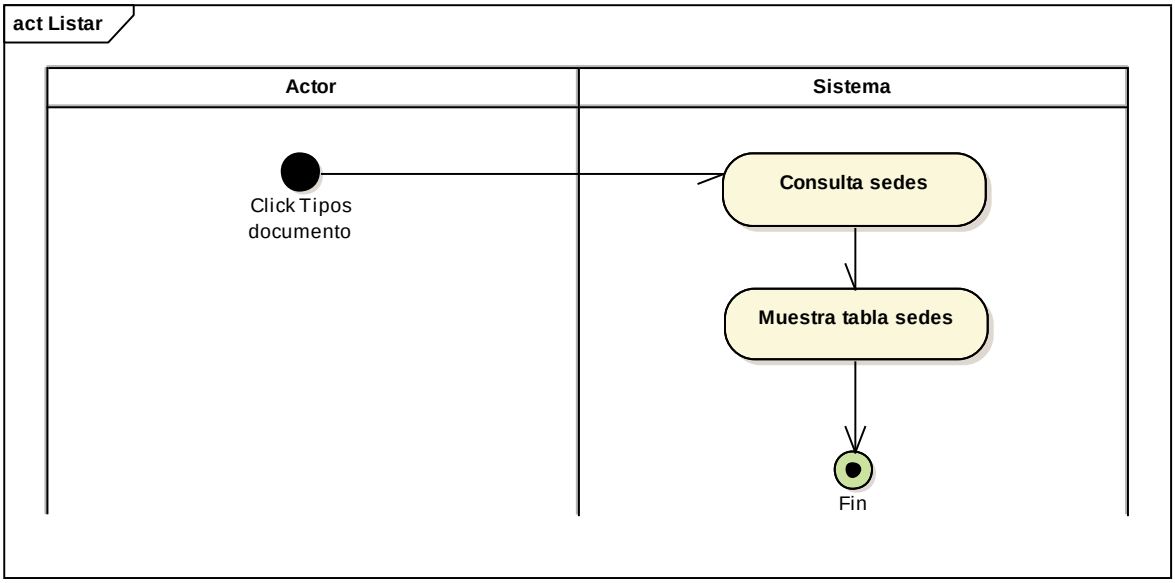


Figura 66 DAC09-1 Listar Sede

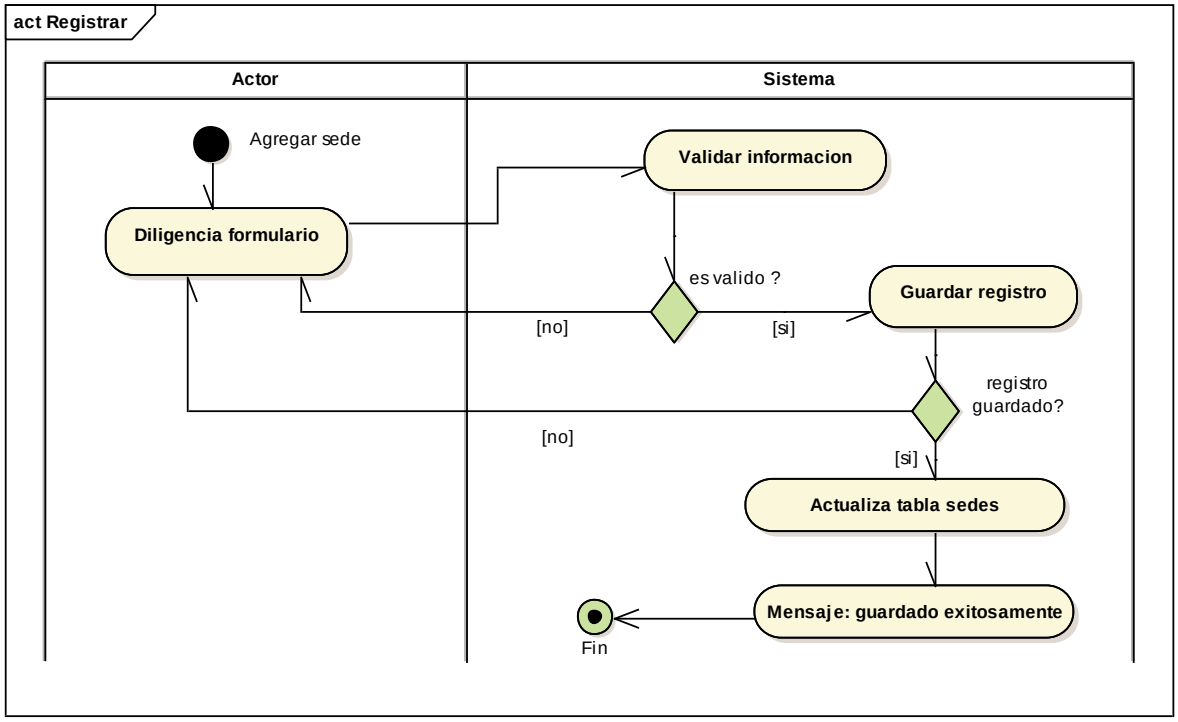


Figura 67 DAC09-2 Registrar Sede

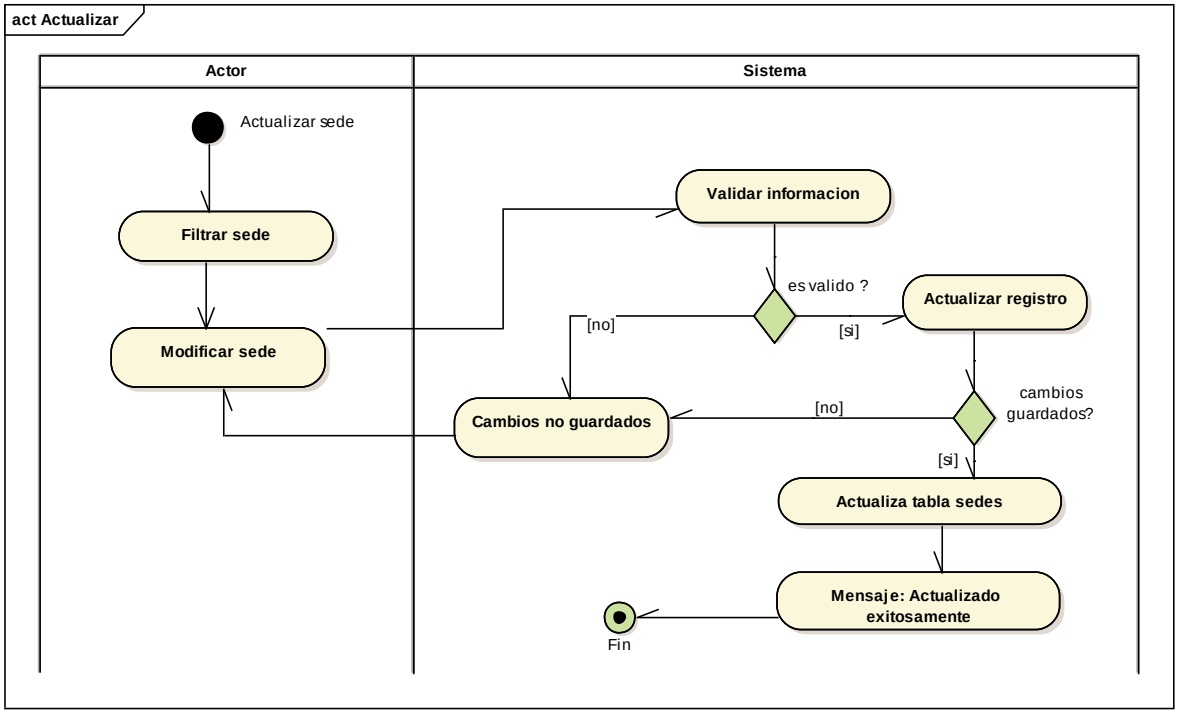


Figura 68 DAC09-3 Actualizar Sede

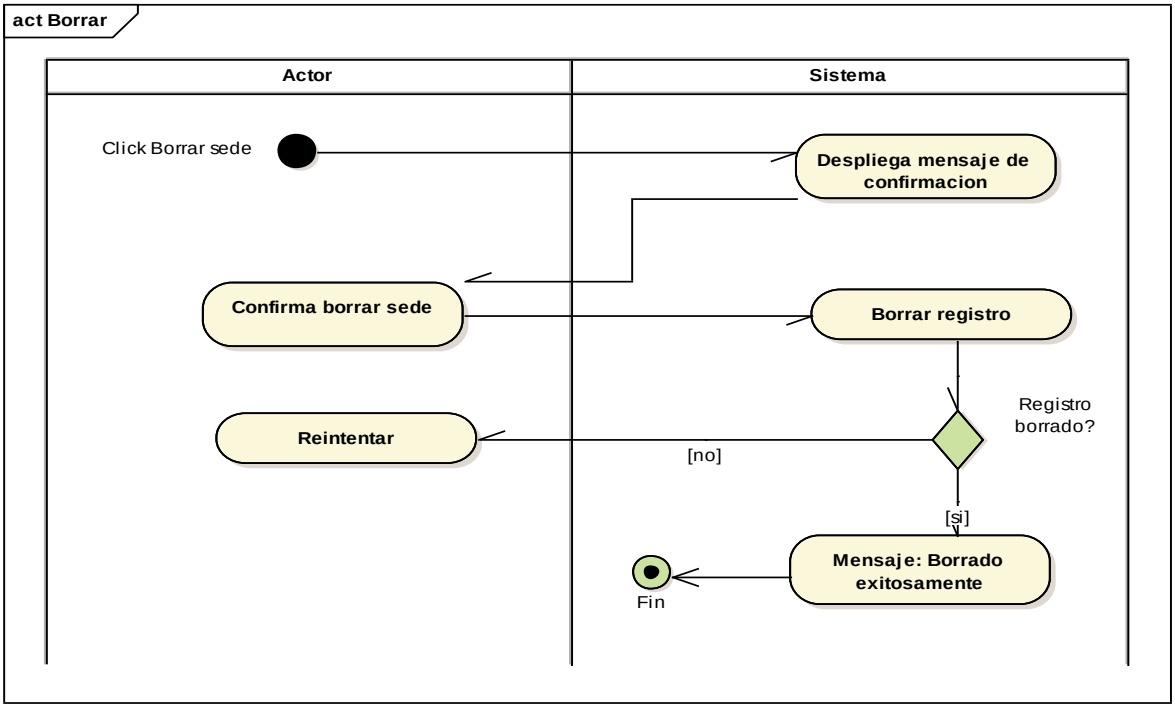


Figura 69 DAC09-4 Borrar Sede

DAC10 CRUD Administrador

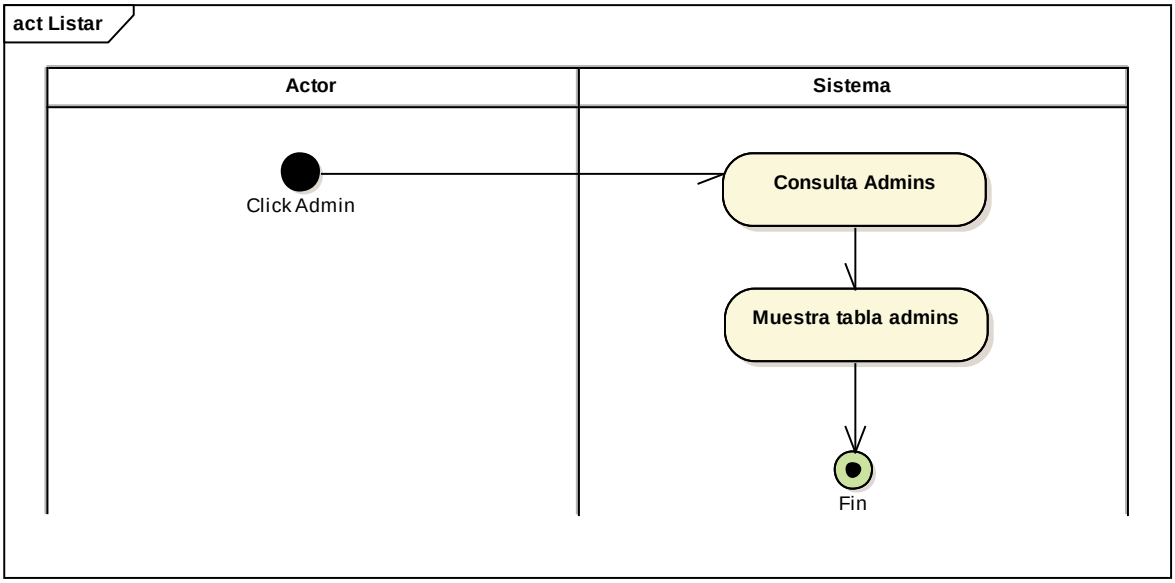


Figura 70 DAC10-1 Listar Administrador

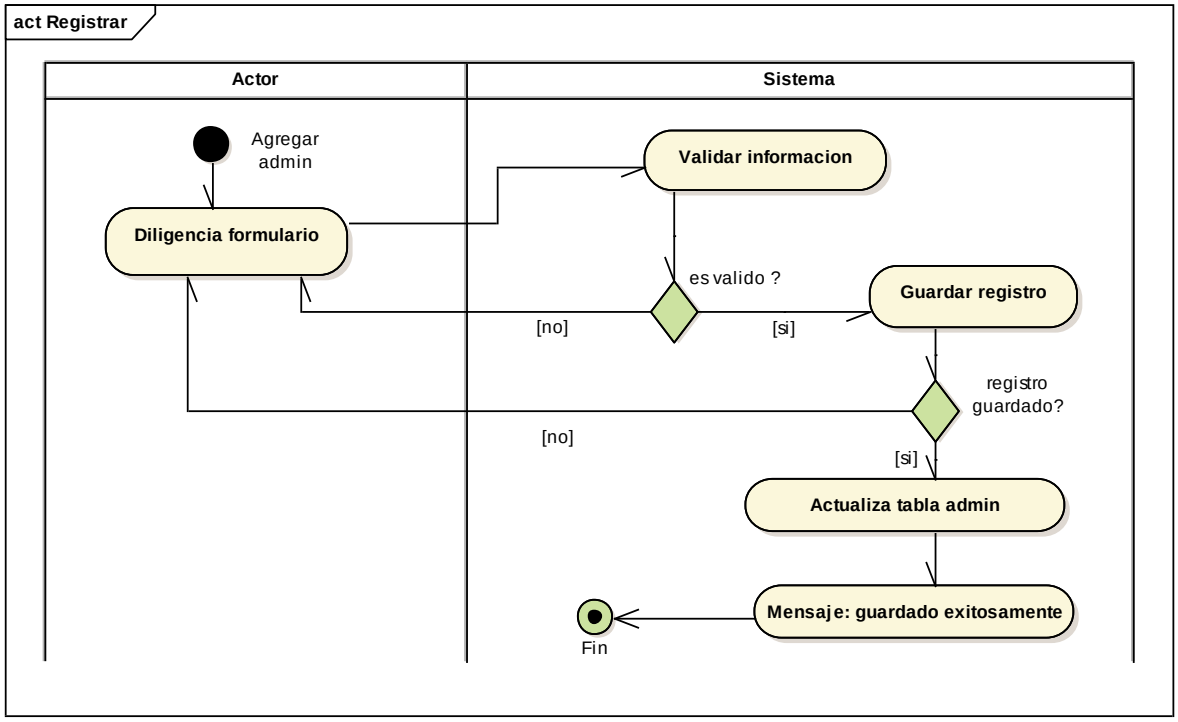


Figura 71 DAC10-2 Registrar Administrador

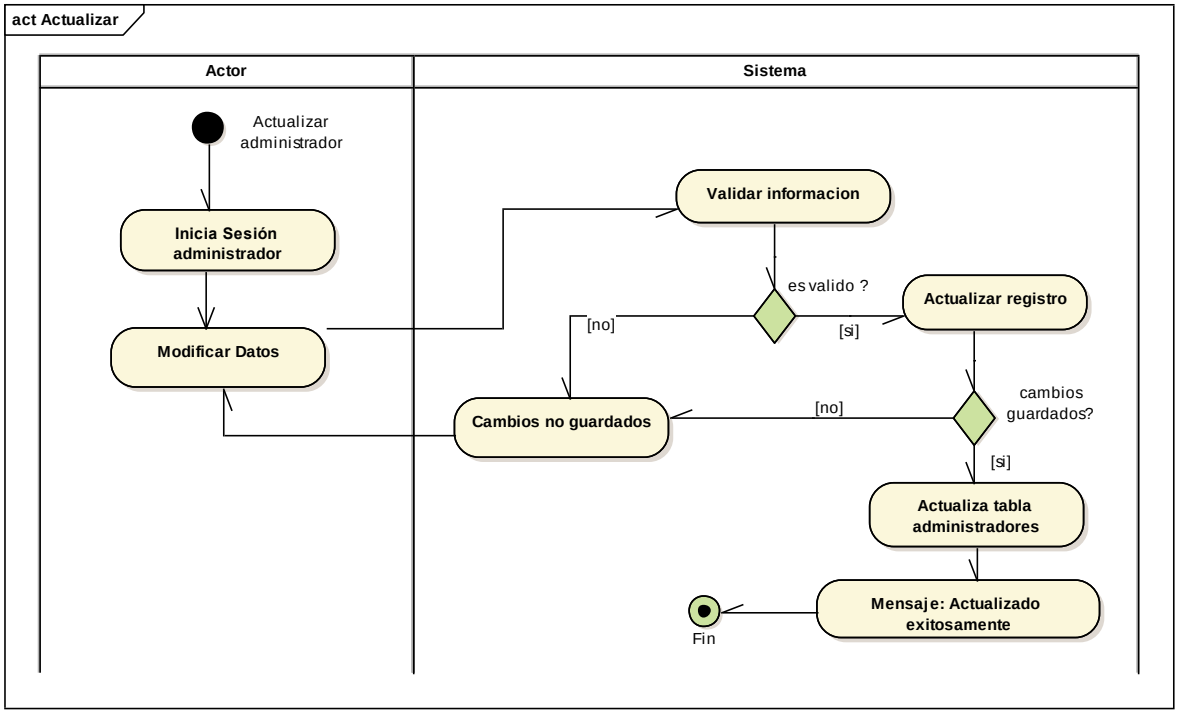


Figura 72 DAC10-3 Actualizar Administrador

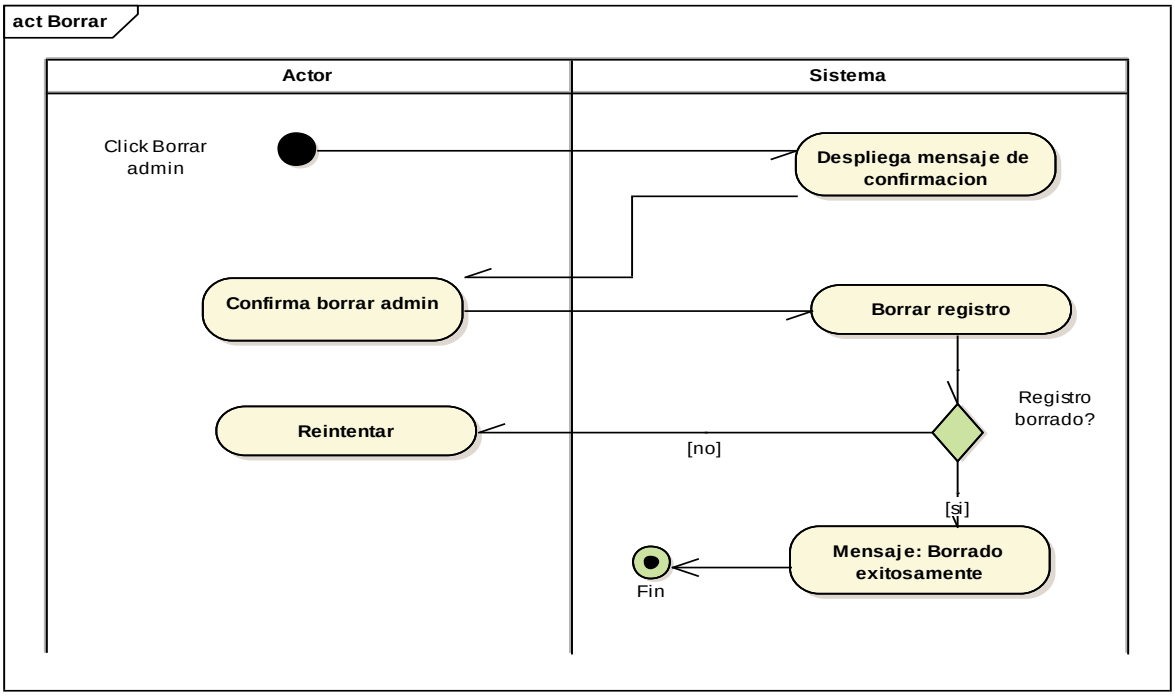


Figura 73 DAC10-4 Borrar Administrador

DAC11 Ver Informacion Votante

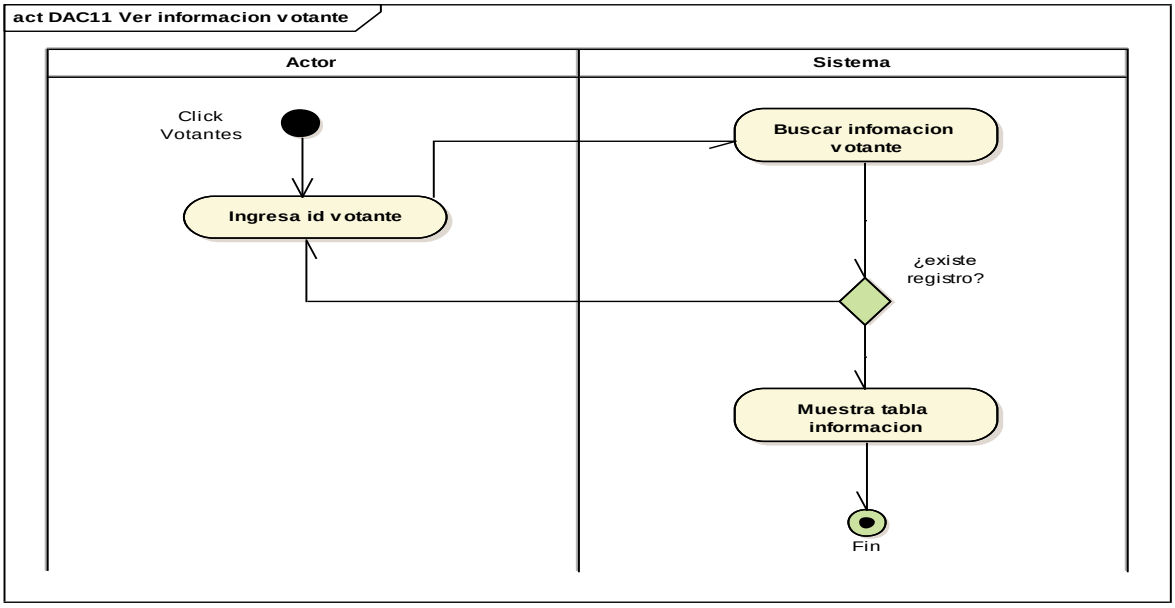


Figura 74 DAC11 Ver Información Votante

2.3.6 Diagrama de clases

El diagrama de clases para el módulo de autenticación es el siguiente:

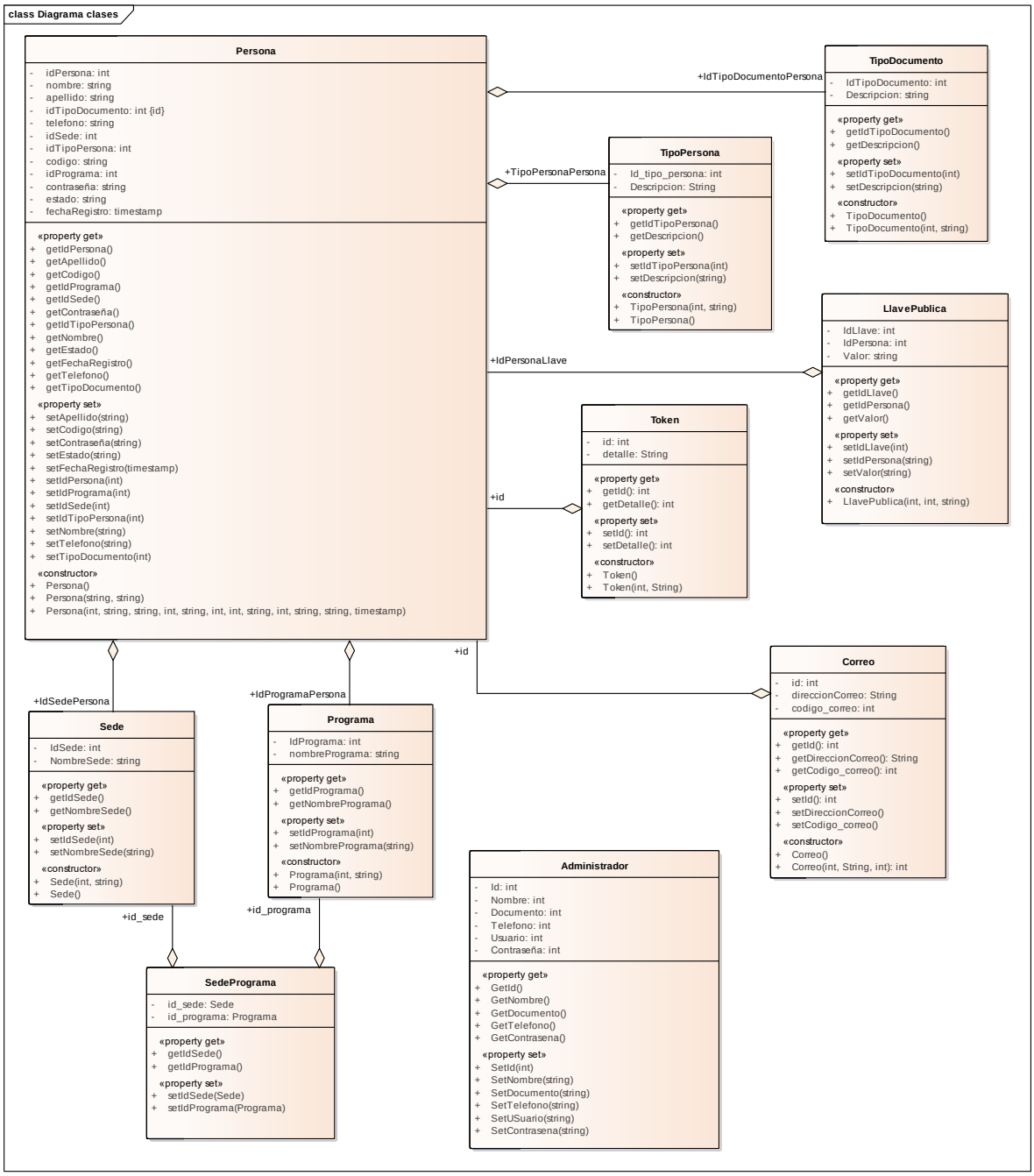


Figura 75 Diagrama de clases

- **Persona:** En esta clase se realiza el mapeo de la entidad persona conforme a la tabla que se encuentra en la base de datos, además se establecen sus atributos y métodos.
- **TipoDocumento:** En esta clase se realiza el mapeo de la entidad Tipo Documento conforme a la tabla de la base de datos, además se establecen sus atributos y métodos.
- **TipoPersona:** En esta clase se realiza el mapeo de la entidad Tipo Persona conforme a la tabla de la base de datos, además se establecen sus atributos y métodos.
- **LlavePublica:** En esta clase se realiza el mapeo de la entidad Llave publica conforme a la tabla de la base de datos que almacena la clave publica para identificar a cada uno de los usuarios, además se establecen sus atributos y métodos.
- **Token:** En esta clase se realiza el mapeo de la entidad Token conforme a la tabla de la base de datos que almacena el token del teléfono móvil para él envió desde el servicio de notificaciones, además, se establecen sus atributos y métodos.
- **Correo:** En esta clase se realiza el mapeo de la entidad Correo conforme a la tabla de la base de datos en la cual se almacena la información del correo electrónico de los usuarios, además se establecen sus atributos y métodos.
- **Programa:** En esta clase se realiza el mapeo de la entidad Programa conforme a la tabla de la base de datos, además se establecen sus atributos y métodos.
- **Sede:** En esta clase se realiza el mapeo de la entidad Sede conforme a la tabla de la base de datos, además se establecen sus atributos y métodos.
- **SedePrograma:** Esta clase es intermedia entre sedes y programas, allí se mapea la entidad de la tabla de base de datos en la cual se almacena la relación entre las sedes y los programas académicos que ofrece la institución.
- **Administrador:** En esta clase se realiza el mapeo de la entidad Administrador conforme a la tabla de la base de datos, además se establecen sus atributos y métodos.

2.3.7 Flujo de navegación aplicación móvil

El módulo de autenticación consta de una aplicación móvil en la cual se almacenan las credenciales únicas de acceso de cada uno de los usuarios, principalmente la llave privada con la cual se realiza el proceso de autenticación. Esta consta de la siguiente estructura y flujo de pantallas o vistas.

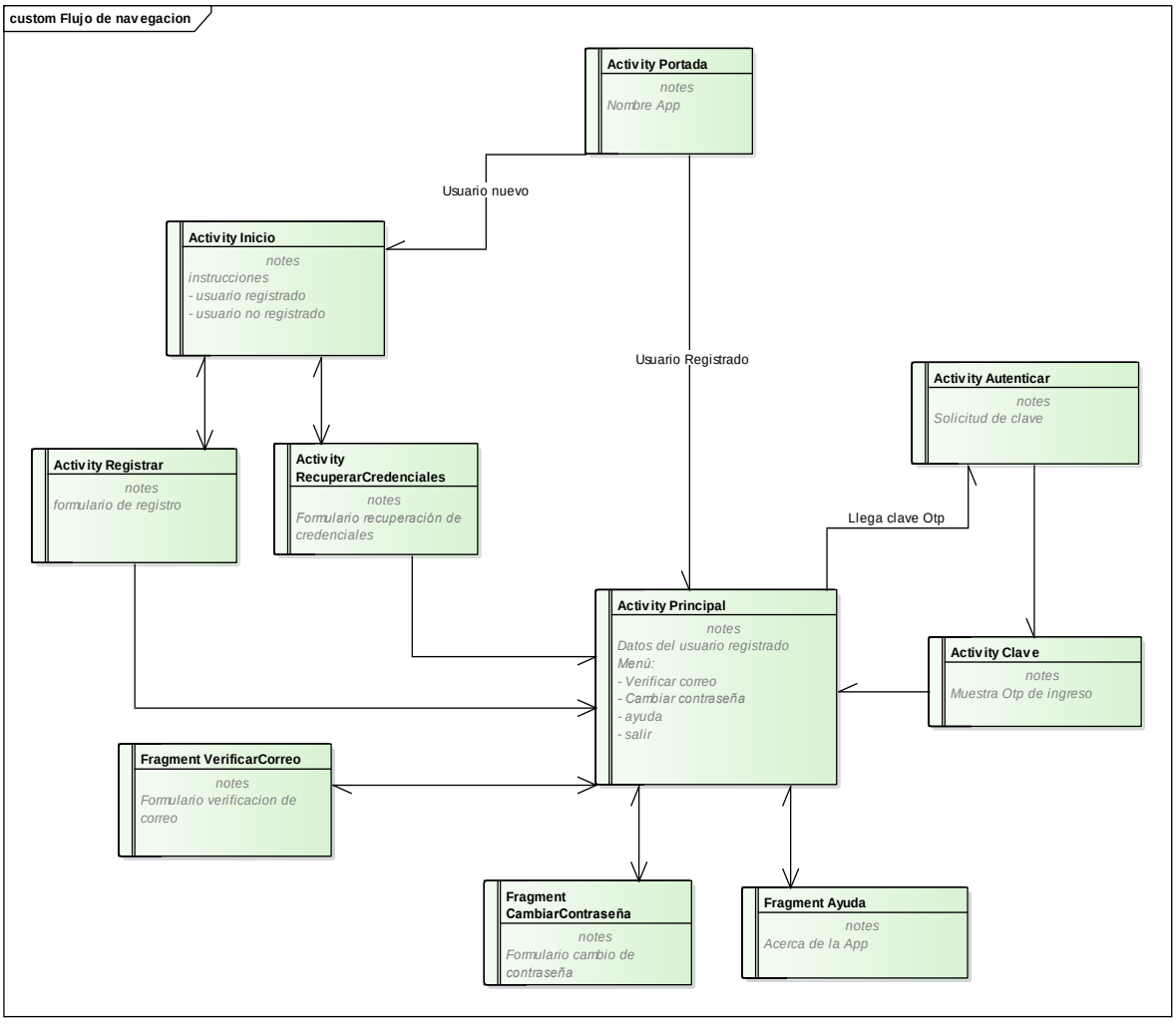


Figura 76 Flujo Navegación App Móvil

2.4 Diseño de los casos de prueba

2.4.1 Pruebas de calidad del código fuente

Se realizaron pruebas de calidad del código fuente mediante la implementación de la herramienta SonarQube, a partir de un análisis estático, lo que quiere decir que analiza el código sin que el programa este en ejecución, permitiendo evaluar la calidad de la codificación y mejorar los estándares de acuerdo con las buenas prácticas para el desarrollo de software, además de proporcionar métricas en materia de fiabilidad, seguridad, mantenibilidad y porcentaje de código duplicado.

Tabla 25 Criterio Fiabilidad, SonarQube

Calificación	Definición Criterio
A	0 errores
B	Al menos 1 error menor
C	Al menos 1 error mayor
D	Al menos 1 error critico
E	Al menos 1 bloque de error

Tabla 26 Criterio Seguridad, SonarQube

Calificación	Definición Criterio
A	0 vulnerabilidades
B	Al menos 1 vulnerabilidad menor
C	Al menos 1 vulnerabilidad mayor
D	Al menos 1 vulnerabilidad critica
E	al menos 1 vulnerabilidad de bloque

Tabla 27 Criterio Mantenibilidad, SonarQube

Calificación	Definición Criterio
A	< = 5%
B	6 al 10%
C	11 al 20%
D	21 al 50%
E	Más del 50%

A continuación, se muestra una tabla con el resumen de los resultados de la evaluación realizada al componente web de administración del módulo y los servicios REST:

Tabla 28 Evaluación Código Fuente Componente Web

Criterio	Calificación	Justificación
Fiabilidad	A	Se evidencia que se tiene la calificación más alta de fiabilidad. Por lo tanto, se establece que el código ofrece una operación libre de bugs o fallos.
Seguridad	A	Tiene la calificación más alta, por lo tanto, el software cuenta con un nivel aceptable frente a amenazas exteriores como ataques malintencionados o virus.
Mantenibilidad	A	Tiene la calificación más alta, debido a que el software tiene la capacidad de ser modificado o actualizado de manera eficiente, con respecto a cambios que se requieran hacer en un futuro.

A continuación, se muestra una tabla con el resumen de los resultados de la evaluación realizada a la codificación de la aplicación móvil para la autenticación:

Tabla 29 Evaluación Código Fuente Aplicación Móvil

Criterio	Calificación	Justificación
Fiabilidad	A	Se evidencia que se tiene la calificación más alta de fiabilidad. Por lo tanto, se establece que el código ofrece una operación libre de bugs o fallos.
Seguridad	C	Tiene una calificación regular. Esto se debe a que presenta algunas vulnerabilidades en materia de seguridad, sin embargo, al revisar el análisis, se pudo establecer que la causa es principalmente la forma en que se está realizando el cifrado y descifrado de la llave privada que se almacena en el momento del registro, más específicamente a la instancia de cifrado de datos establecida. Por lo tanto, es uno de los aspectos importantes a corregir y mejorar del software. Aun así, se considera que esto no influye en un nivel de gravedad fatal para el funcionamiento de la aplicación y el proceso de autenticación de usuarios.
Mantenibilidad	A	Tiene la calificación más alta, debido a que el software tiene la capacidad de ser modificado o actualizado de manera eficiente, con respecto a cambios que se requieran hacer en un futuro.

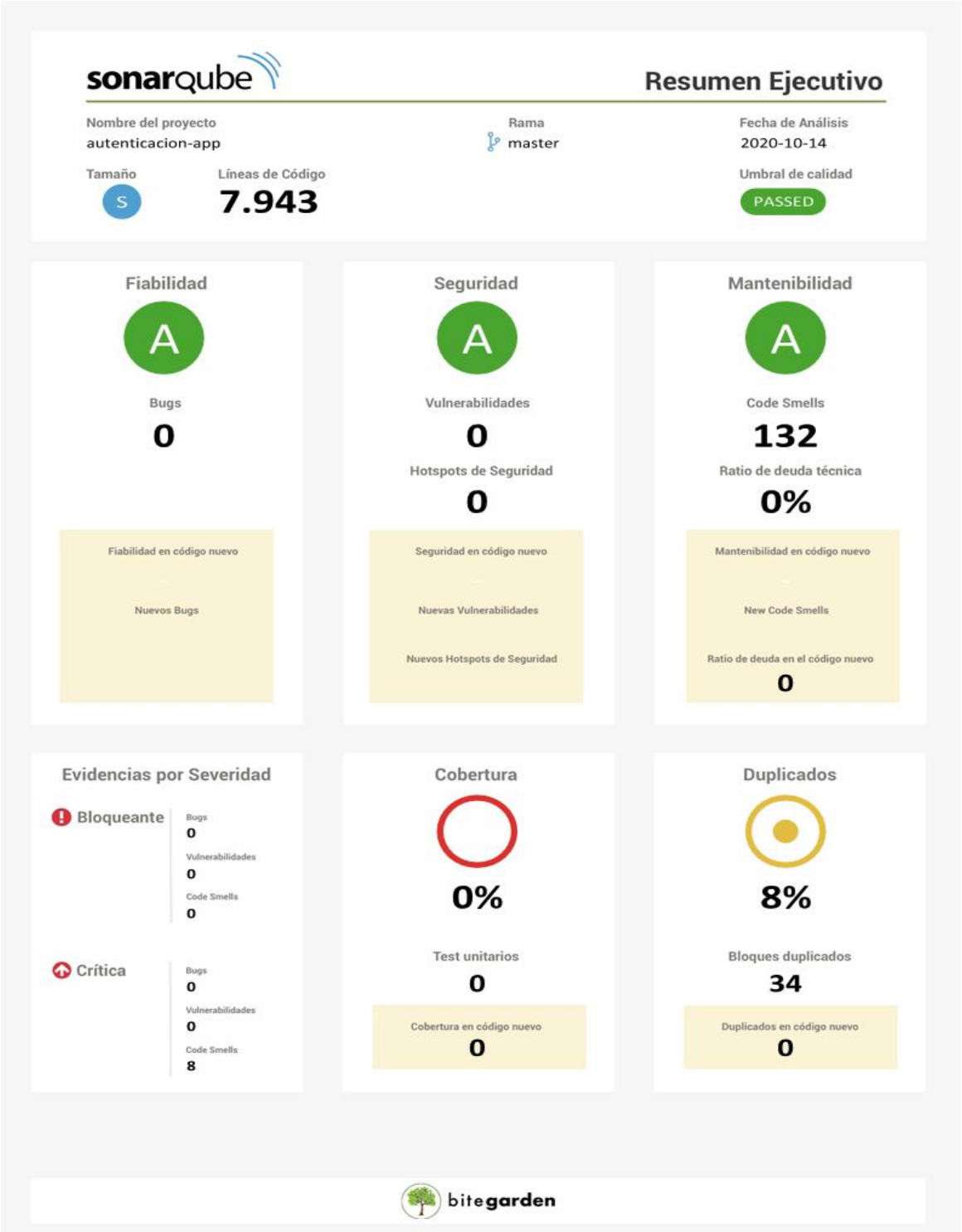


Figura 77 Resumen Ejecutivo Calidad Código, Servicios y componente Web

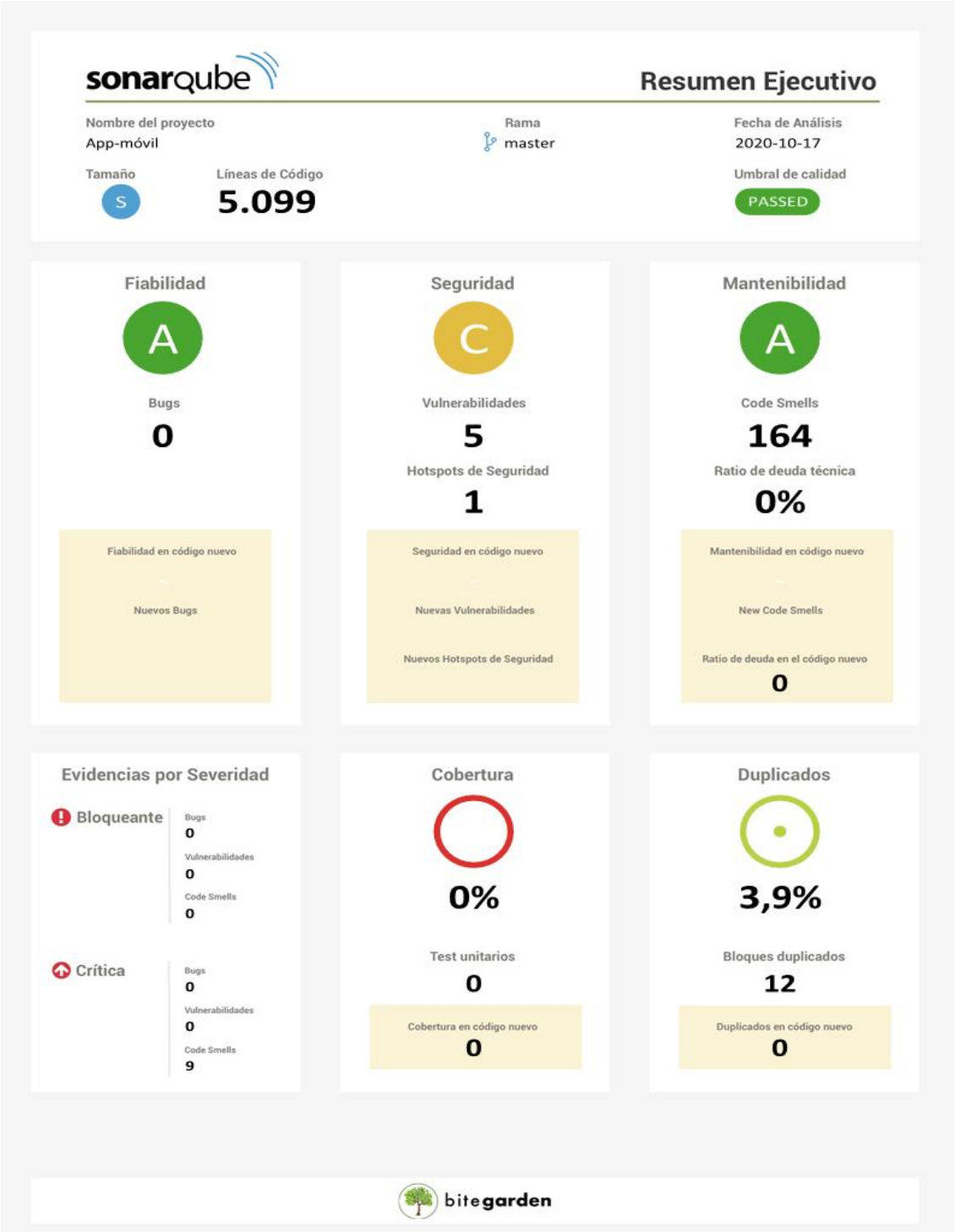


Figura 78 Resumen Ejecutivo Calidad Código Aplicación Móvil

2.5 Estimación de Recursos

Para la estimación de recursos necesarios para el desarrollo del proyecto se recurrió a la estimación de esfuerzo por puntos de caso de uso, una metodología la cual se basa en la utilización de casos de uso como dato de entrada para calcular el esfuerzo en horas- hombre que son necesarias para el desarrollo de un proyecto de software (C.Remón & P.Thomas, 2010).

El cálculo de los Puntos Casos de Uso sin ajustar (UUCP) a partir de la relación entre los casos de uso y los actores.

Tabla 30 Factor de peso de los actores

Actor	Tipo de Interacción	Factor de Peso
Administrador	Complejo	3
Usuario	Complejo	3

Para calcular pesos de los actores sin ajustar:

$$UAW = \sum (Cantidad\ de\ un\ tipo\ de\ actor^{*}\ factor\ de\ peso)$$

$$UAW = 6$$

Tabla 31 Factor de peso casos de uso

Caso de Uso	Tipo (Número de Transacciones)	Factor de Peso
Registrar votantes CU01	Promedio	10
Iniciar sesión CU02	Promedio	10
Autenticar votante CU03	Promedio	10
Validar correo CU04	Simple	5
Renovar llaves CU05	Promedio	10
CRUD tipo documento CU06	Simple	5
CRUD tipo persona CU07	Simple	5
CRUD programa CU08	Simple	5
CRUD sede CU09	Simple	5
CRUD administrador CU10	Simple	5
Ver información votante CU11	Simple	5

Para calcular pesos de los casos de uso sin ajustar:

UUCW = ∑ (Cantidad tipos de caso de uso factor de peso)*

UUCW= 75

Una vez hallado el valor de los pesos de los actores sin ajustar (UAW) y el valor de los pesos de caso de uso sin ajustar (UUCW):

UUCP = UAW + UUCW UUCP = 75 + 6 = 81

Ahora se procede a calcular el valor de TCF o factor de complejidad técnica del software por medio de la clasificación de los factores que se muestran en la siguiente tabla:

Tabla 32 Factor de complejidad técnica

Factor	Descripción	Peso	Valor (Impacto percibido 0 - 5)	Factor
T1	Sistema Distribuido	2	1	2
T2	Tiempo de respuesta	1	1	1
T3	Eficiencia por el usuario	1	3	3
T4	Proceso interno complejo	1	3	3
T5	Reusabilidad	1	2	2
T6	Facilidad de instalación	0,5	1	0.5
T7	Facilidad de uso	0,5	4	2
T8	Portabilidad	2	3	6
T9	Facilidad de cambio	1	3	3
T10	Concurrencia	1	3	3
T11	Objetivos especiales de seguridad	1	4	4
T12	Acceso directo a terceras partes	1	2	2
T13	Facilidad de entrenamiento a usuarios finales	1	1	1

Para hallar el valor TCF se usa la siguiente formula:

*TCF = 0.6 + 0.01 * ∑ (Peso * Valor)*

*TCF = 0.6 + 0.01 * 32.5 TCF= 0.925*

Posteriormente se procede a determinar el valor del factor ambiente EF que indica la influencia del factor humano en el software a desarrollar:

Tabla 33 Factor Ambiente

Factor	Descripción	Peso	Valor (Impacto percibido 0 - 5)	Factor
E1	Familiaridad con el modelo del proyecto usado	1.5	3	4.5
E2	Experiencia en la aplicación	0.5	3	1.5
E3	Experiencia POO	1	4	4
E4	Capacidad del analista líder	0.5	2	1
E5	Motivación	1	5	5
E6	Estabilidad de los requerimientos	2	3	6
E7	Personal media jornada	-1	1	-1
E8	Dificultad en lenguaje de programación	-1	3	-3

Para hallar el valor TCF se usa la siguiente formula:

*EF = 1.4 - 0.03 * ∑ (Peso * Valor)*

*EF = 1.4 - 0.03 * 18 EF = 0.86*

A continuación, para el cálculo de los puntos de caso de uso ajustados, se utiliza la siguiente formula:

*UCP = UUCP * TCF * EF*

*UCP = 81 * 0.925 * 0.86 UCP = 64.435*

Cálculo de esfuerzo se realiza teniendo en cuenta el valor de los puntos de casos de uso ajustados que se han determinado anteriormente y el factor de conversión CF (20 horas/hombre), como se muestra a continuación.

*E = UCP * CF E = 64.435 * 20*

E = 1288.7 horas-hombre

Una vez encontrado el valor del esfuerzo en horas- hombre para el desarrollo del software, se procede a determinar el tiempo total estimado para terminar con el aplicativo.

Tiempo desarrollo = E / Cantidad de hombres (En este caso 1 ingeniero)

Tiempo desarrollo = 1288.7 / 1 = 1288.7 horas

Considerando que se trabajen 8 horas diarias:

Tiempo desarrollo (Días) = Tiempo desarrollo / 8 horas / día

Tiempo desarrollo (Días) = 1288.7 horas / 8 horas / día

Tiempo desarrollo (Días) = 161 días

Finalizamos con el cálculo del costo total para el desarrollo del software, en base a el esfuerzo y las horas de trabajo que se deben invertir para terminarlo.

*Costo Total = E * número de desarrolladores * TH tarifa horaria*

*Costo Total = 1288.7 * 1 * $ 8000*

Costo Total = $ 10’309.600

En conclusión, se estima que el desarrollo del software se puede realizar en un tiempo aproximado de cinco meses y medio, con un solo desarrollador y con un costo de $ 10’309.600 pesos colombianos.

2.6 Resultados

2.6.1 Impacto Social mediante NVivo 20.2

El día 23 de octubre de 2020 se realizó un simulacro de votaciones implementando la plataforma que web que integra los módulos de autenticación y Blockchain, en el que participaron algunos estudiantes de la Universidad de Cundinamarca. Se realizo una encuesta a diez (10) de las personas que hicieron uso de la plataforma y la aplicación móvil, con el objetivo de conocer su opinión acerca del software y medir el impacto social. Esto mediante el software NVivo, que es una herramienta para el apoyo de la investigación y que permite el análisis cualitativo de la información recolectada.

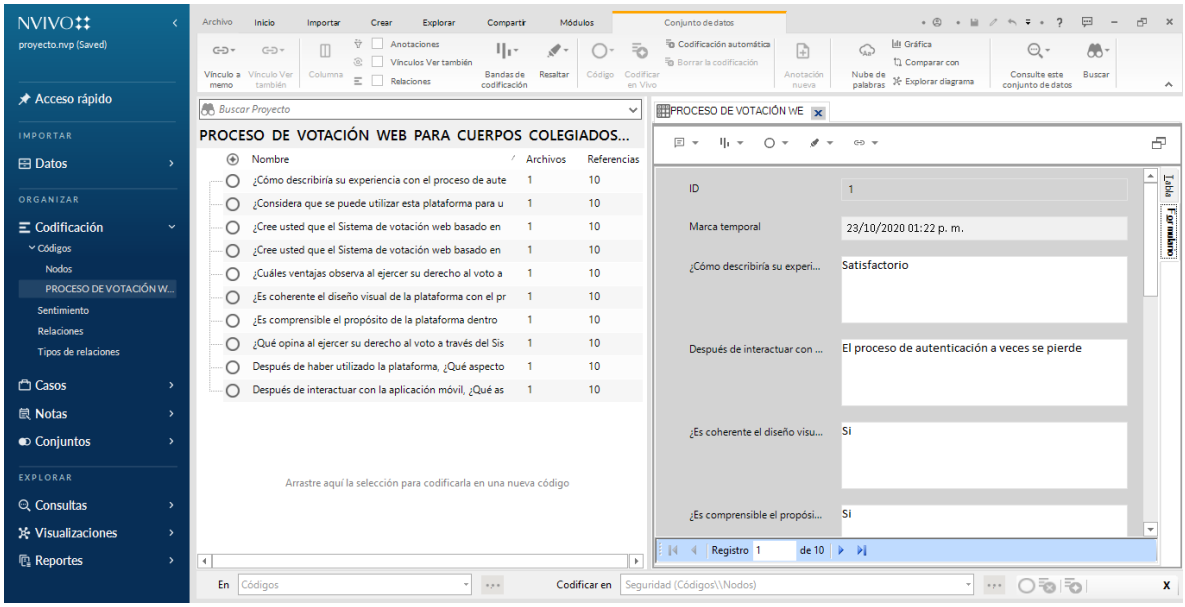


Figura 79 Plataforma de Votación para los Cuerpos Colegiados - NVivo

La encuesta tenía un total de diez (10) preguntas abiertas relacionadas con la funcionalidad, la usabilidad y la eficiencia de la plataforma, vinculando los diferentes módulos.

Codificación y análisis de resultados

Los resultados de la encuesta se almacenaron en un documento Excel, para posteriormente ser cargado en la plataforma NVivo y realizar el respectivo análisis. Inicialmente se aplicó un filtro para obtener las palabras que se habían mencionado con más frecuencia, como se muestra a continuación:

Figura 80 Nube de Palabras

Figura 81 Mapa Ramificado

Se obtuvo una nube de palabras y un mapa ramificado en el cual se puede evidenciar las palabras que fueron utilizadas con más frecuencia en las respuestas entregadas por parte de las personas encuestadas. Entre ellas se destaca a palabra “Seguridad”, siendo este uno de los aspectos más importantes para los usuarios que usan la plataforma, tanto en la forma en que se realiza el proceso de autenticación, el almacenamiento de los datos personales y la votación en sí. Otra de las palabras más mencionadas fue “Buena”, que representa una opinión positiva en el funcionamiento general del software para las votaciones, sin embargo, cabe destacar que entre las palabras que más se mencionaron también se encuentra “Debería”, dando a entender que hay aspectos o funcionalidades dentro del sistema que pueden ser mejorados o incluidos en nuevas versiones de la solución, por lo que también es muy importante atender estas observaciones que se realizaron.

Otras palabras que se destacan en la nube de palabras y en el mapa ramificado son: “buena”, “votos”, “Registro”, “Proceso”.

Como paso siguiente se crearon nodos con las palabras que más importancia tuvieron dentro de la encuesta y se asociaron las respuestas a cada una de ellas según correspondiera, como se muestra en la siguiente figura.

Nombre	Archivos	Referencias
Autenticación	1	5
Buena	1	19
Coherente	1	10
Debería	1	10
Fraude	1	8
Práctico	1	15
Proceso	1	2
Seguridad	1	25
Votaciones	1	4
Votos	1	4

Figura 82 Creación de Nodos

A continuación, se muestran las gráficas de la relación entre los casos o votantes encuestados y los nodos resultantes de la codificación de las respuestas de la encuesta, permitiéndonos evidenciar que la “seguridad” fue uno de los aspectos en común que fue mencionado por todos los encuestados, junto a la palabra “Buena” que nos permite concluir que en general se llevaron una impresión positiva en algún aspecto del aplicativo.

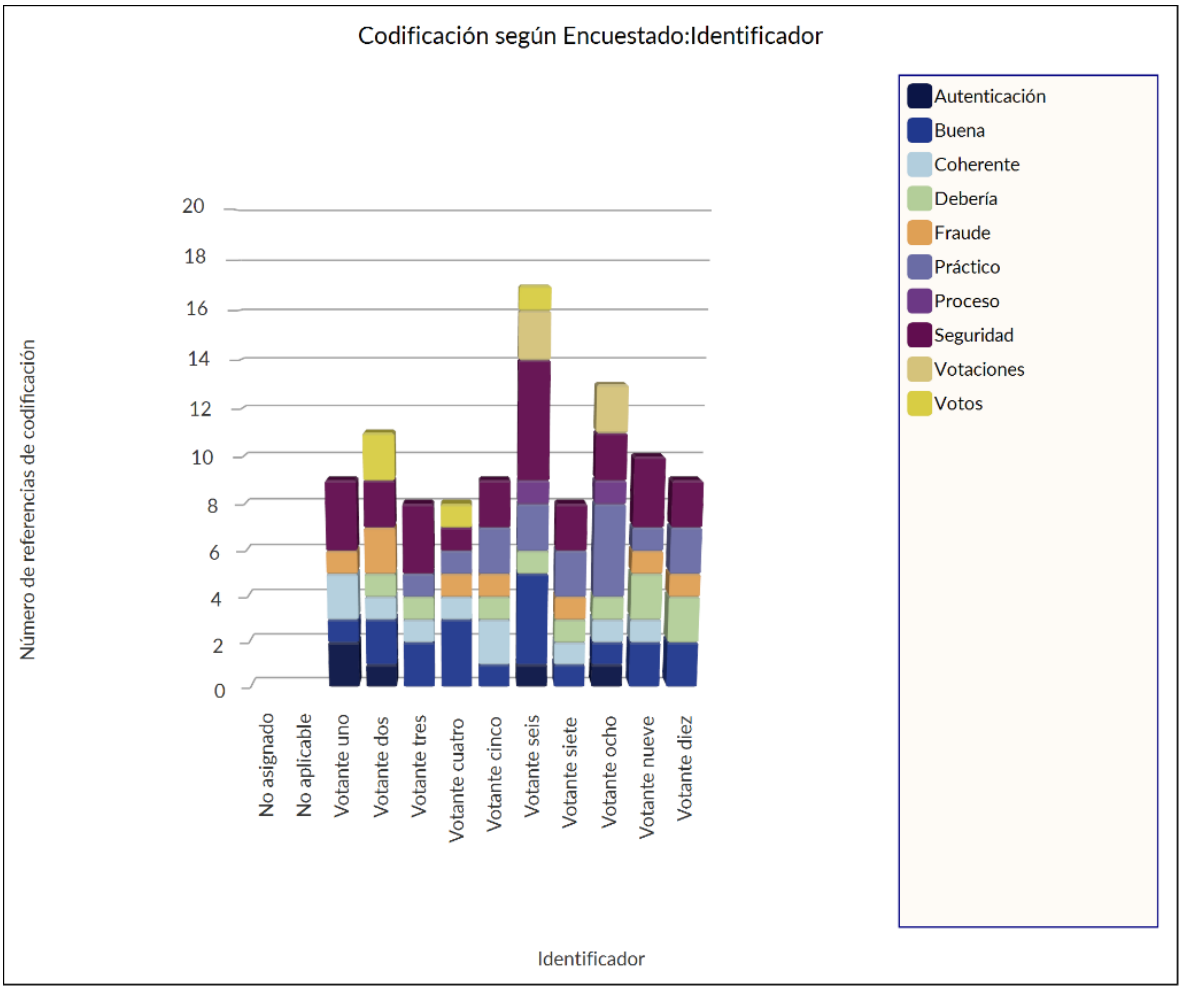


Figura 83 Codificación según Votantes Encuestados

A partir del software de NVivo, también se pudo establecer la relación entre las opiniones que dieron los encuestados y un sentimiento positivo o negativo que reflejaban sus respuestas. Esto se muestra en la siguiente tabla en donde se puede visualizar un total de veintiún (21) referencias asociadas como comentarios muy

positivos, treinta y cinco (35) moderadamente positivos y dieciséis (16) como moderadamente negativos.

Nombre	Archivos	Referencias
Positivo	1	56
Muy positivo	1	21
Moderadamente positivo	1	35
Negativo	1	16
Moderadamente negativo	1	16
Muy negativo	0	0

Figura 84 Sentimiento de Usuarios

A continuación, se muestra un mapa jerárquico en el que se relaciona los usuarios que fueron encuestados y el sentimiento frente a la plataforma, el cual fue en mayor porcentaje positivo.

Figura 85 Mapa Jerárquico Sentimiento Casos

También se obtuvo un mapa jerárquico de la comparación entre los nodos y el número de referencias de codificación de sentimientos (Verde: positivo, Rojo: negativo, Amarillo: mixto, Gris: neutral).

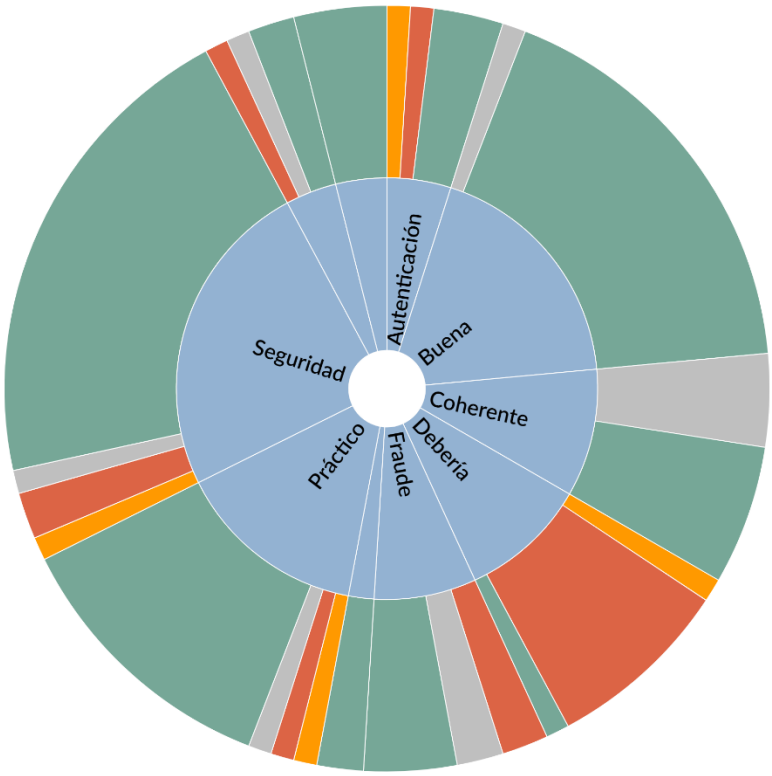


Figura 86 Mapa jerárquico Sentimiento Codificado para Nodos

Para finalizar, se realizó un análisis de conglomerados en el que se puede ver la relación entre los nodos o palabras que se usaron con más frecuencia en la encuesta, por ejemplo; la palabra “autenticación” y buena se encuentran relacionadas, lo que significa que el proceso que se realiza para el acceso a la plataforma fue visto de manera positiva. La palabra “proceso” encuentra relacionada con “practico” y “votaciones” lo que significa que, para los usuarios encuestados, la plataforma es una alternativa más eficiente y se destaca por la facilidad que brinda para la ejecución del voto.

La palabra “debería” es muy importante, teniendo en cuenta que se relaciona con la mayoría de los diferentes nodos, dando a entender que, aunque en términos generales tanto la plataforma web de votación y la aplicación para la autenticación fueron vistos de manera positiva, se podría incorporar algunas funcionalidades y mejorar aún más la experiencia del usuario con el software.

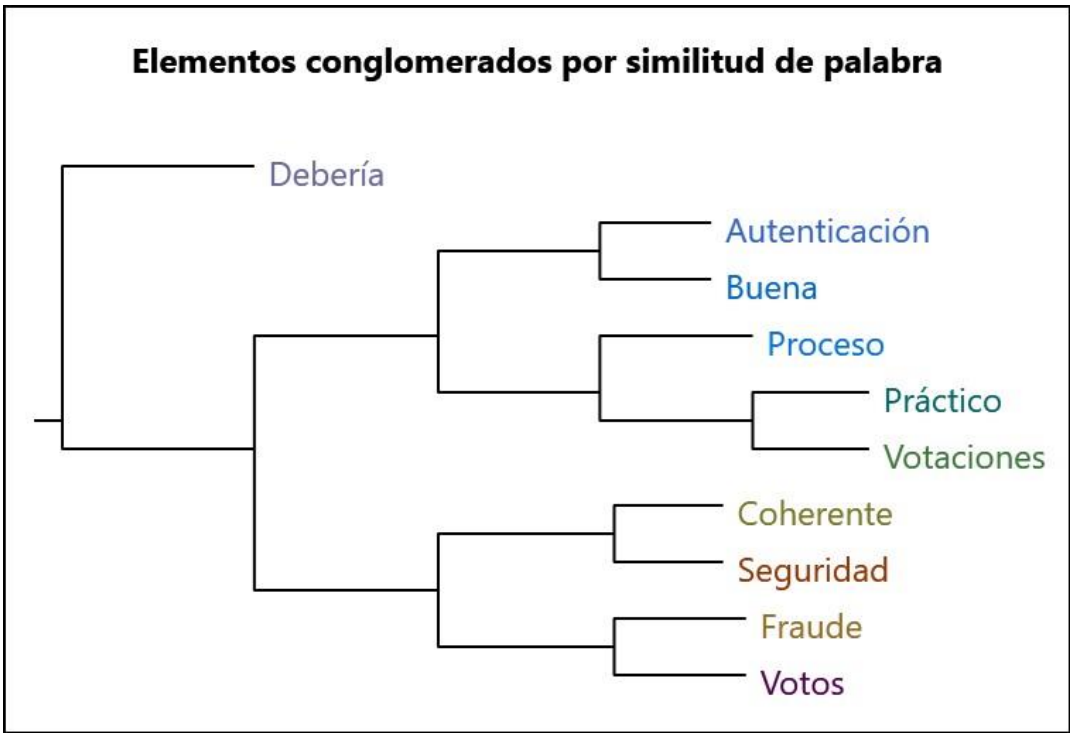


Figura 87 Elementos Conglomerados por Similitud de Palabra

En conclusión, a partir del análisis que se realizó de las opiniones de la plataforma en general, para los usuarios es una buena alternativa para la administración del proceso electoral dentro de la Universidad de Cundinamarca, ya que permite agilizar todo el proceso de ejecución del voto y la obtención de los resultados. Sin embargo, queda claro que hay cosas por mejorar y funciones que pueden ser incluidas en versiones futuras.

2.7 Conclusiones y recomendaciones

La ejecución del voto es un mecanismo indispensable dentro de una democracia y generalmente se traduce en poder político o influye en la toma de decisiones, por lo tanto, es importante garantizar la transparencia del proceso electoral, lo que supone un reto para el uso de los sistemas informáticos, ya que es constante el riesgo de fraude o suplantación de identidad.

La seguridad y la veracidad de los resultados se convierten en los aspectos más importantes y a la vez los más cuestionados a la hora de optar el uso de herramientas tecnológicas para la ejecución y administración del proceso electoral.

La implementación de la criptografía de clave asimétrica para el proceso de autenticación a partir del protocolo de desafío respuesta, es una alternativa inicial que nos permite establecer que la persona que va a acceder a la plataforma de votaciones es quien se registró y quien posee el dispositivo móvil con las respectivas credenciales.

La arquitectura basada en servicios web, establecida para el módulo de autenticación, facilito el proceso de integración con la plataforma web y la aplicación móvil, independientemente del lenguaje de programación.

La implementación de la API de Google para el servicio de notificaciones permitió realizar él envió de las claves OTP cifradas de manera efectiva y segura, en el momento en el que se realizaba el proceso para el inicio de sesión en la plataforma de votación.

Para versiones futuras se recomienda la implementación de un factor más de autenticación, por ejemplo, a partir de las características biométricas del usuario, que permita fortalecer el nivel de seguridad de autenticación de entidad.

2.8 Bibliografía

Andress, J., & Winterfeld, S. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition. In *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition*. Retrieved from https://www.academia.edu/32643426/Andress_Jason_Basics_of_Information_Security_Second_Edition

Branddocs. (2018). Autenticación de identidad: ¿son las personas quiénes dicen que son? Retrieved February 23, 2020, from https://branddocs.com/blog/autenticacion-de-identidad/

Burr, William E, Dodson, Donna F, Newton, Elaine M, … Emad A. (2013). *Archived NIST Technical Series Publication Superseding Publication(s) Electronic Authentication Guideline*. 54. https://doi.org/10.6028/NIST.SP.800-63-2

C.Remón, & P.Thomas. (2010). *Análisis de Estimación de Esfuerzo aplicando Puntos de Caso de Uso*. Retrieved from http://sedici.unlp.edu.ar/bitstream/handle/10915/19290/Documento_completo.pdf?sequence=1&isAllowed=y%0Ahttp://sedici.unlp.edu.ar/bitstream/handle/10915/19290/Documento_completo.pdf?sequence=1

Casado Santos. (2017). *Memoria del Trabajo Fin de Máster IMPLANTACIÓN DE UN SISTEMA MES*. Retrieved from http://digibuo.uniovi.es/dspace/bitstream/10651/43550/4/TFM_AlvaroCasadoSantos.pdf

Chuang, J., Nguyen, H., Wang, C., & Johnson, B. (2013). I think, therefore I am: Usability and security of authentication using brainwaves. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7862 LNCS*, 1–16. https://doi.org/10.1007/978-3-642-41320-9_1

Dussan, C. (2006). Politicas de la Seguridad Informatica. *Entramado Universidad Libre Colombia.*, *2*(1.), 86-92.

Evidian. (2015). *Los 7 métodos de Autentificación más utilizados*.

Fandiño Casas, L. J. (2012). Análisis De Los Alcances Y Limitaciones De La Implementación Del Voto Electrónico En América Latina, Lecciones Para Colombia Estudio De Caso: Elecciones Generales De Perú 2006. *Reponame:Repositorio Institucional EdocUR*. Retrieved from http://repository.urosario.edu.co/handle/10336/4760

Fernández, S. (2004). LA CRIPTOGRAFÍA CLÁSICA. In *Sigma: revista de matemáticas* (pp. 119–142).

Franchi, M. R. (2012). Algoritmos De Encriptación De Clave Asimétrica. *UNIVERSIDAD NACIONAL DE LA PLATA*.

Gayoso, V., Hernandez, L., & Sanchez, C. (2010). A survey of the elliptic curve integrated encryption scheme. *Journal of Computer Science and Engineering*, *2*(2), 7–13.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines: revision 3*. https://doi.org/10.6028/NIST.SP.800-63-3

Hernández Sampieri, R., Fernández-Collado Baptista Lucio McGraw-Hill México, C. P., & Edición, ª. (2006). *Metodología de la investigación*.

Kalvet, T. (2012). Innovation: A factor explaining e-government success in Estonia. *Electronic Government*, *9*(2), 142–157. https://doi.org/10.1504/EG.2012.046266

Legal Information Institute. (2014). U.S. Code Title 44. PUBLIC PRINTING AND DOCUMENTS Chapter 35. COORDINATION OF FEDERAL INFORMATION POLICY Subchapter II. INFORMATION SECURITY. Retrieved February 23, 2020, from https://www.law.cornell.edu/uscode/text/44/3552

Madise, Ü., & Martens, T. (2006). E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. *Electronic Voting 2006 - 2nd International Workshop*, 15–26. Retrieved from http://www.id.ee/pages.php/030301

Marrero Travieso, Y. (2003). La Criptografía como elemento de la seguridad informática. *ACIMED*, *11*(6). Retrieved from http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

Medina, T., & Miranda, A. (2015). Comparison of Algorithms Based Cryptography Symmetric DES, AES and 3DES. *Revista Mundo Fesc*, *9*, 14–21.

Paredes, G. (2006). *INTRODUCCIÓN A LA CRIPTOGRAFÍA*. *7*, 1–17. Retrieved from http://www.revista.unam.mx/vol.7/num7/art55/int55.htm

Pareja, A., Pedak, M., Gómez, C., & Barros, A. (2017). *La gestión de la identidad y su impacto en la economía digital*. https://doi.org/10.18235/0000786

Peacock, A., Ke, X., & Wilkerson, M. (2004). Typing Patterns: A Key to User Identification. *The IEEE Computer Society*. Retrieved from http://csdl.computer.org/comp/mags/sp/2004/05/

Pesado, P., Pasini, A., Ibañez, E., Galdámez, N., Chichizola, F., Rodríguez, l., … De Giusti, A. (2008). E-Government: El voto electrónico sobre Internet. *XIV*

Congreso Argentino de Ciencias de La Computación, 11. Retrieved from http://sedici.unlp.edu.ar/bitstream/handle/10915/21971/Documento_completo.pdf?sequence=1

Purificacion, L. A. (2010). *Seguridad informática*. Retrieved from https://books.google.com.co/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=seguridad+informática&ots=PqrlTBFLS0&sig=C71FQuvthu_yxYAZtp0gJMR8sZY&redir_esc=y#v=onepage&q=seguridad informática&f=false

Ristić, I. (2015). *BULLETPROOF SSL AND TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications Free*. Retrieved from www.feistyduck.com

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., … Castillo Merino, M. A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. In *Introducción a la seguridad informática y el análisis de vulnerabilidades*. https://doi.org/10.17993/ingytec.2018.46

Schwaber, K., & Sutherland, J. (2011). The Scrum Guide - The Definitive Guide to Scrum: The Rules of the Game. *Scrum. Org, October*, Vol. 2, p. 17. https://doi.org/10.1053/j.jrn.2009.08.012

searchdatacente. (2014). ¿Qué es Autenticación multifactor (MFA)? - Definición en WhatIs.com. Retrieved February 23, 2020, from https://searchdatacenter.techtarget.com website: https://searchdatacenter.techtarget.com/es/definicion/Autenticacion-multifactor-MFA

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security analysis of the estonian internet voting system. *Proceedings of the ACM Conference on Computer and Communications Security*, 703–715. https://doi.org/10.1145/2660267.2660315

2.9 Anexos

Anexo 1 Encuesta

Marca temporal	***¿Cómo describiría su experiencia con el proceso de autenticación para el ingreso a la plataforma de votación?***	***Después de interactuar con la aplicación móvil, ¿Qué aspectos resalta y que considera que puede mejorarse?***	***¿Es coherente el diseño visual de la plataforma con el propósito de esta?***	***¿Es comprensible el propósito de la plataforma dentro de su funcionamiento?***	***¿Cuáles ventajas observa al ejercer su derecho al voto a través del Sistema de votación web basado en Blockchain?***
10/23/2020 13:22:30	*Satisfactorio*	*El proceso de autenticación a veces se pierde*	*Si*	*Si*	*La información siempre estará codificada en las transacciones de red*
10/23/2020 13:23:52	*Buena*	*Interfaz entendible y práctica*	*Si*	*Si*	*Tiempo y seguridad*
10/23/2020 13:25:59	*Buena plataforma*	*Estuvo bien la forma de autenticar el usuario para poder llevar un voto fiable*	*Sí*	*Sí*	*Demuestra que el voto es de alguien de la universidad y no cualquiera podría entrar y votar para hacer fraude*
10/23/2020 13:26:17	*Es interesante, buena seguridad*	*Al realizar el registro se quedó cargando y tuve que salir de la app y volver a entrar. Al dar clic en la segunda opción recupero mis datos, pero quede con la duda de la carga del proceso del registro.*	*Es coherente*	*Si*	*Seguridad y practicidad*

10/23/2020 13:26:47	*Excelente, es muy sencillo realizar la votación*	*La seguridad de autenticación es la apropiada para realizar la votación, es bueno tener eso en cuenta.*	*Sí, lo necesario para realizar el proceso satisfactoriamente*	*Si*	*Autenticidad de voto.*
10/23/2020 13:30:15	*Rápida y eficiente*	*La fuente de letra en el código de autenticación podría ser más clara para diferenciar los números y las letras en el código*	*Si, bastante intuitiva*	*Si*	*Es más rápido, es mejor que ir hasta una ubicación física a votar*
10/23/2020 13:40:48	*Correcta*	*Ninguno en particular*	*Si*	*Si*	*Haciéndolo de esta manera agiliza la acción de ejercer la votación desde cualquier dispositivo conectado a la red*
10/23/2020 14:11:43	*Buena*	*Sencilla y cómoda debería tener más funcionalidades*	*Si*	*Si*	*Facilidad en el proceso, entornos seguros controlados por la entidad encargada, se evitan aglomeraciones*
10/23/2020 14:26:00	*Buena*	*Pues está bien estructurada y fácil de manejar*	*Si es coherente*	*Si*	*Que puedo citar fácilmente*
10/29/2020 18:32:55	*Excelente*	*Resaltó el diseño y por mejorar se debe adicionar más cosas a la aplicación de Android para que no quede solo de consulta*	*Si*	*Si*	*Seguridad y el control*

Después de haber utilizado la plataforma, ¿Qué aspectos considera que pueden mejorarse?	***¿Considera que se puede utilizar esta plataforma para una votación real dentro del ambiente de la Universidad de Cundinamarca?***	***¿Cree usted que el Sistema de votación web basado en Blockchain es seguro? y ¿Por qué?***	***¿Cree usted que el Sistema de votación web basado en Blockchain reducirá el fraude en la política colombiana? y ¿Por qué?***	***¿Qué opina al ejercer su derecho al voto a través del Sistema de votación web basado en Blockchain?***
El código de autenticación con la aplicación móvil	*Si*	*Si porque es un registro único, consensuado y distribuido en varios nodos de una red*	*Si, al ser un registro único no se podrá registrar dos o más votos con el mismo número de documento de identidad*	*Un proceso seguro*
Notificaciones guía para el usuario	*Si*	*Si, porque tiene verificación*	*Si, porque no se puede suplantar identidades para repetir votos*	*Es más práctico y rápido*
Quizás mostrar una foto del candidato	*Sí*	*Sí, porque le da una veracidad al voto, es decir, la persona que se registre debe ser de la universidad de Cundinamarca*	*Dependiendo de quienes manejen esa parte, el fraude es algo muy complicado en este país*	*Mi voto es veraz*
Entre por celular, no sé por qué pero me recargaba con zoom.	*Si*	*Si, los pasos para poder ingresar son complejos, es tedioso no hacer todo el proceso en solo la app pero considero que es seguro.*	*Si, ya que el proceso de registro enlaza el número de teléfono así que supongo que solo se puede tener un teléfono registrado por votante*	*Es novedoso y seguro*
Que me notifique al correo electrónico que realice la votación	*Claro, llevaría a cabo el proceso de votación más fácil y*	*Si, el blockhain protege la información y no existiría la*	*Si, actualmente hay corrupción en las votaciones,*	*Es mucho más ágil, desde su hogar la puede realizar*

	ágil, no habría ningún estudiante que se abstendría de hacerlo	*posibilidad de votos falsificados ni de votos perdidos*	*con el blockhain se garantiza el voto de los ciudadanos*	*sin miedo a que el voto de pierda*
Ninguna, funciona como debería	*Si*	*Si, es ampliamente utilizado en el mundo*	*No, para aplicarse a votaciones en la universidad puede funcionar, pero no sería seguro en votaciones masivas*	*Creo que la sensación de seguridad es menor pero el proceso mucho más rápido*
Más información en la app para personas que nunca han usado un sistema similar (personas de tercera edad).	*Si*	*Este sistema ofrece seguridad para la privacidad de datos de los usuarios*	*No creo*	*Rápido, sencillo y seguro*
El código de confirmación de correo debería tener una caducidad	*Si*	*Si porque es muy privado su manejo*	*Si porque evitara errores humanos que crean excusas para cometer fraudes electores*	*"Muy bueno porque es un avance para la Universidad y tal vez para el país en materia de democracia*
Ninguno, está bien así	*Si*	*Si es seguro*	*Podría ser, pero el fraude en Colombia siempre existirá*	*Que es bueno*
Poder ver los resultados en tiempo real	*Si*	*Si, cumple con todos los aspectos de seguridad*	*Si, de pronto existe más control y es más seguro*	*Bastante bueno*

Anexo 2 Manual Técnico

UDEC
UNIVERSIDAD DE CUNDINAMARCA

SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO AUTENTICACIÓN

MANUAL TÉCNICO
DESARROLLO DE SOFTWARE
UNIVERSIDAD DE CUNDINAMARCA

2020

www.unicundi.edu.co
unicundi@mail.unicundi.edu.co
Línea gratuita 018000 976000

GP-CER355041 CO-SC-CER355037 SC-CER355037

Dirección de Sistemas y Tecnología
sistemasytecnologia@mail.unicundi.edu.co
PBX: 828 14 83 Ext. 110-170
Sede Fusagasugá

TABLA DE CONTENIDO

INDICE DE IMÁGENES

INTRODUCCIÓN

El presente documento pretende servir de guía para la instalación del módulo de autenticación que hace parte de la plataforma de votaciones por internet de la Universidad de Cundinamarca. Por lo tanto, se presentan las principales características y elementos técnicos necesarios para el despliegue del software y su correcto funcionamiento.

1. REQUERIMIENTOS DEL SISTEMA

Inicialmente, cabe aclarar que el sistema se despliega en un servidor virtual en la nube a través de los servicios web de Amazon (AWS), que permiten la creación de instancias EC2, en la que inicializaremos un servidor con las siguientes características:

- Sistema operativo Linux Ubuntu Server 18.04
- Memoria RAM mínimo 1Gb.
- Disco duro de 128GB.

Además de una instancia RDS para el despliegue de la base de datos PostgreSQL.

2. INSTALACIÓN

Para empezar, se debe tener una cuenta en una plataforma de servicios en la nube para el despliegue de aplicaciones, en este caso AWS.

2.1 Instancia RDS para base de datos

Para realizar la creación de la instancia que almacenara la base de datos que se va a poner en producción, diríjase a la pestaña de servicios de AWS y seleccione la opción RDS.

Como paso siguiente, buscamos la opción “Crear base de Datos”. Allí se desplegarán todas las opciones que se disponen para la creación de una nueva base de datos en la nube. En este caso crearemos una instancia gratuita y sin mayor capacidad de recursos de la siguiente manera:

1. Método de creación de la base de datos: “Fácil de Crear”.

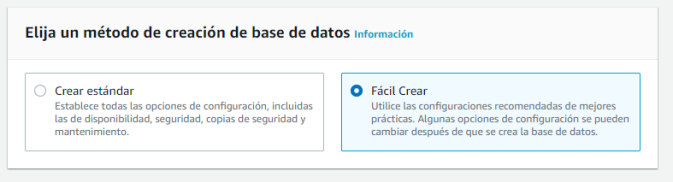


Gráfico 1 Método de Creación Base de Datos

2. Seleccionamos el motor de la base de datos, en este caso PostgreSQL.

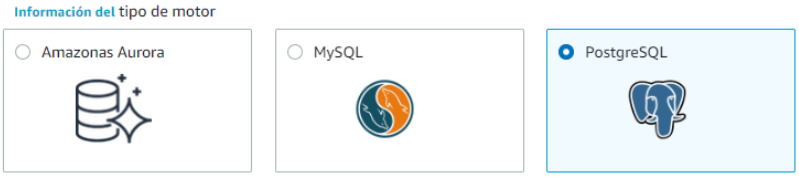


Gráfico 2 Motor Base de Datos

3. Seleccionamos la opción Free o gratuita con 1 GB de RAM y 20 GB de almacenamiento.

Gráfico 3 Tamaño Instancia Base de Datos

4. Por último, se establece el nombre de la instancia, el usuario y la contraseña con la cual se podrá acceder a esta. Al presionar el botón de crear base de datos, empezara la creación de la base de datos. Al terminar, podemos ir a la opción “DB Instancias” donde encontraremos la instancia creada como se muestra a continuación.

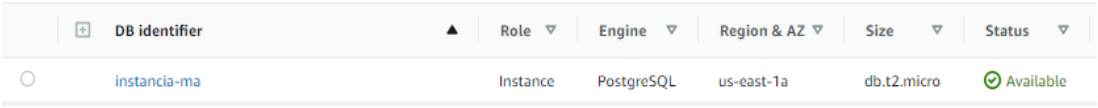


Gráfico 4 Instancia Base de Datos

5. Ahora desde pgAdmin de PostgreSQL se puede acceder a la instancia creada con el respectivo identificador y la contraseña que se haya establecido. Allí se crea la base de datos a la que se va a conectar el módulo de autenticación. Hay varias formas para ello, lo que se hizo en este caso en específico fue restaurar la base de datos desde un archivo backup.

Finalmente, la base de datos se encuentra desplegada y lista para responder a las peticiones que se realicen desde el software del módulo de autenticación.

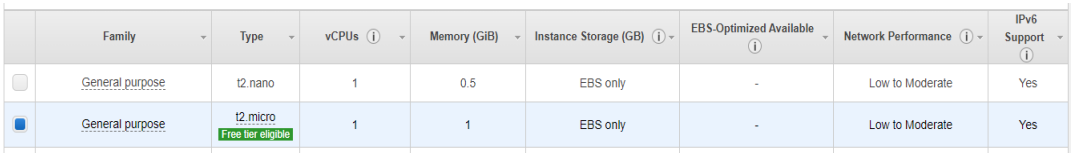
2.2 Creación de instancia EC2

Para la creación de la instancia del servidor virtual, en el panel de servicios de AWS diríjase a la pestaña servicios y posteriormente seleccione la opción “EC2”.

Como paso siguiente, buscamos la opción “Lanzar instancia”. Allí se desplegarán todas las opciones que se disponen para la creación de una instancia de servidor virtual. Para ello seleccionamos la opción para que solo nos muestre las alternativas del nivel gratuito y escogemos la opción del sistema operativo Ubuntu Server 18.04 de 64 bit(x86), como se muestra en la siguiente imagen.

Gráfico 5 Sistema Operativo Servidor

Luego debe seleccionar un tipo de instancia, en este caso la que se muestra a continuación.



	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes

Gráfico 6 Tipo de Instancia EC2

Por último, no es necesario realizar muchas más configuraciones, por lo tanto, puede darle a la opción “Revisar y lanzar” que nos enviara a una página donde se muestra en resumen las características de la instancia que se va a crear. La capa gratuita de Amazon permite hasta 30 GB de almacenamiento en el servidor EC2. Para terminar con la creación de la instancia, presiona el botón “lanzar”, que comenzara con el proceso de creación de la instancia.

Al finalizar podrá ver la instancia que se creó de en la opción de “Instancias en ejecución”, onde podrá administrar sus servidores en la nube.

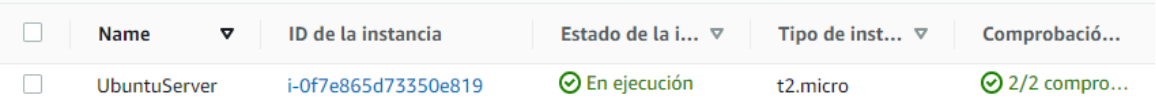


Gráfico 7 Instancia EC2 Ubuntu Server

2.3 Instalación Glassfish 4.1

Ahora se procede a instalar el servidor de aplicaciones Glassfish en la instancia de servidor que se creó anteriormente. Para conectarse al servidor es necesario la descarga e instalación del software WinSCP. Al abrir el WinSCP configuramos una nueva sesión, mediante el DNS público del servidor y el usuario.

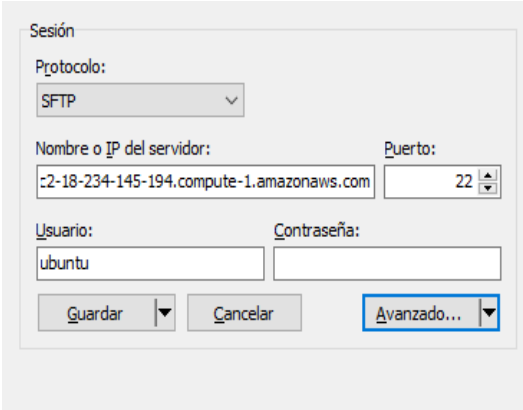


Gráfico 8 Conexión WinSCP a Servidor

Para conectarse al servidor se genera una llave privada que se almacena localmente, y con la cual se realizara siempre el proceso de autenticación para el acceso al servidor.

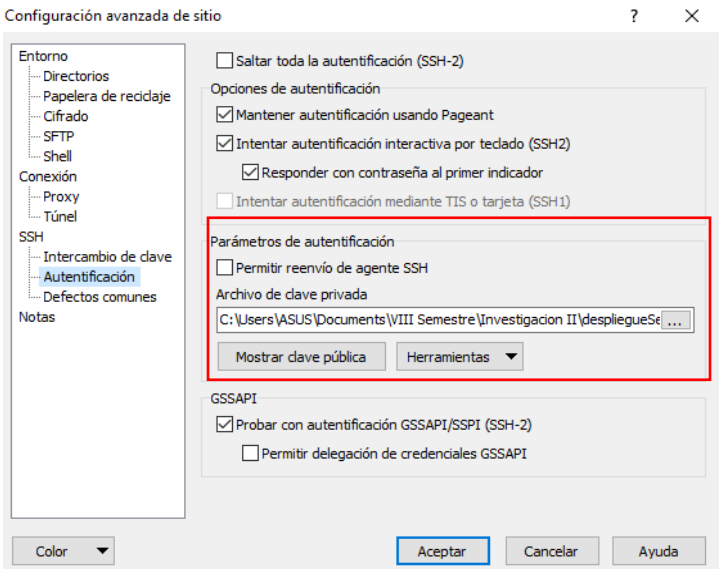


Gráfico 9 Autenticación con Llave Privada

Al guardar la configuración y conectar, se iniciará el proceso de autenticación para posteriormente acceder a la consola de administración del servidor y los archivos de este. Allí vamos a ejecutar los siguientes comandos en el orden en que se muestran:

sudo su: Para ingresar como usuario Root.

sudo apt-get update*:* Para actualizar la lista de paquetes del sistema.

sudo apt-get install unzip: Para instalar Unzip en el sistema.

sudo apt-get install openjdk-8-jdk: para instalar el JDK en el sistema.

Ir a la carpeta */tmp* del sistema y descargar Glassfish con el comando ***wget (Enlace de descarga del paquete .jar de glassfish 4.1)***

Descomprimir el archivo descargado en la carpeta */opt* del sistema mediante el comando ***sudo unzip /tmp/ (Archivo zip de glassfish)***

Ahora ejecutar los comandos que se muestran en la siguiente imagen, para la configuración de usuario del dominio, grupo de trabajo y permisos de ejecución.

```
drwxr-xr-x 8 root root 4096 Aug 21  2014 glassfish4
ubuntu@ip-172-31-27-122:/opt$ sudo useradd --system glassfish -d /opt/glassfish4
ubuntu@ip-172-31-27-122:/opt$ sudo chown -R glassfish glassfish4
ubuntu@ip-172-31-27-122:/opt$ sudo chgrp -R sudo glassfish4/
ubuntu@ip-172-31-27-122:/opt$ sudo chmod -R +x glassfish4/bin
ubuntu@ip-172-31-27-122:/opt$ sudo chmod -R +x glassfish4/glassfish/bin
ubuntu@ip-172-31-27-122:/opt$
```

Gráfico 10 Comandos Usuario, Grupo Trabajo y Permisos

Posteriormente se procede a inicializar el dominio por defecto de glassfish en el cual se despliega el proyecto.

```
ubuntu@ip-172-31-27-122:/opt/glassfish4$ sudo -u glassfish bin/asadmin start-domain domain1
Waiting for domain1 to start .......
Successfully started the domain : domain1
domain  Location: /opt/glassfish4/glassfish/domains/domain1
Log File: /opt/glassfish4/glassfish/domains/domain1/logs/server.log
Admin Port: 4848
Command start-domain executed successfully.
```

Gráfico 11 Comando Inicialización de Dominio

De esta manera ha iniciado el dominio de Glassfish, en el cual se encuentra la consola de administración por el puerto 4848. Desde allí es donde se realiza la parte del despliegue del proyecto y la configuración del pool de conexión para la base de datos, pero antes de eso, se debe habilitar el control remoto de la consola de glassfish de la siguiente manera:

```
ubuntu@ip-172-31-27-122:/opt/glassfish4$ sudo -u glassfish bin/asadmin change-admin-password
Enter admin user name [default: admin]>
Enter the admin password>
Enter the new admin password>
Enter the new admin password again>
Command change-admin-password executed successfully.
```

Gráfico 12 Comando Cambiar Contraseña Administrador

```
ubuntu@ip-172-31-27-122:/opt/glassfish4$ sudo -u glassfish bin/asadmin enable-secure-admin
Enter admin user name>  admin
Enter admin password for user "admin">
You must restart all running servers for the change in secure admin to take effect.
Command enable-secure-admin executed successfully.
ubuntu@ip-172-31-27-122:/opt/glassfish4$ sudo -u glassfish bin/asadmin stop-domain domain1
Waiting for the domain to stop .
Command stop-domain executed successfully.
ubuntu@ip-172-31-27-122:/opt/glassfish4$ sudo -u glassfish bin/asadmin start-domain domain1
Waiting for domain1 to start ......
Successfully started the domain : domain1
domain  Location: /opt/glassfish4/glassfish/domains/domain1
Log File: /opt/glassfish4/glassfish/domains/domain1/logs/server.log
Admin Port: 4848
Command start-domain executed successfully.
```

Gráfico 13 Comandos Habilitar Administración Remota y Reiniciar Dominio

De esta manera se estableció un usuario y contraseña, reiniciando el dominio de glassfish para guardar los cambios y comprobar ingresando a la consola de administración de Glassfish.

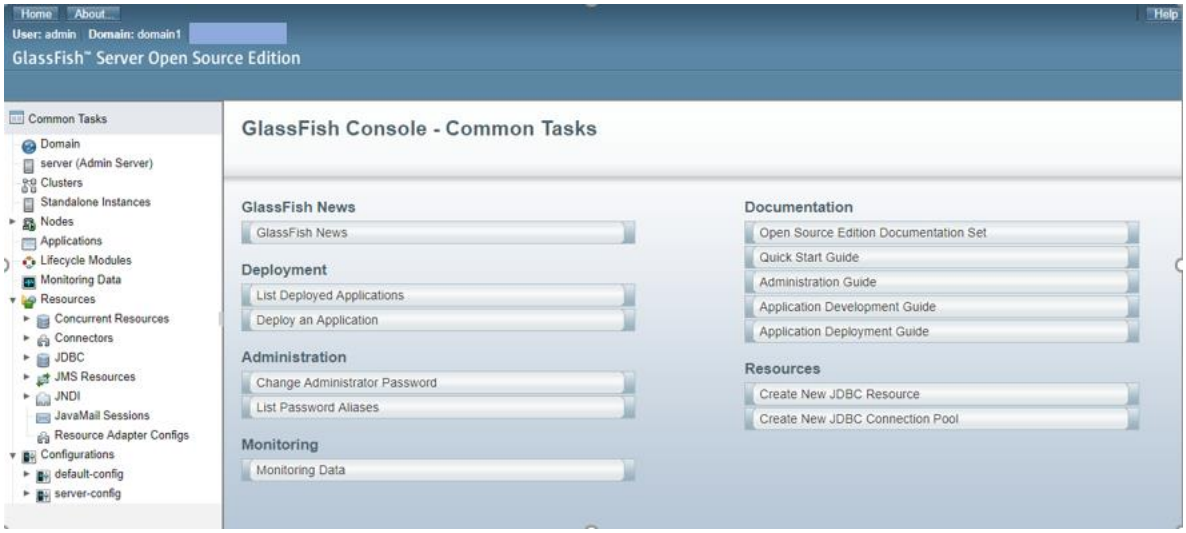


Gráfico 14 Consola de Administración Servidor de Aplicaciones Glassfish

2.4 Configuración Pool de conexiones BD

Inicialmente debe descargar el controlador de la base de datos en las siguientes ubicaciones de la carpeta de instalación de Glassfish en el servidor.

[glassfish_home]/glassfish/domains/domain1/lib/.

[glassfish_home]/glassfish/domains/domain1/lib/ext/.

[glassfish_home]/glassfish/lib/.

Se procede a configurar la conexión de base de datos a la cual se va a vincular nuestro proyecto. Esto desde la pestaña *Resources/JDBC/Connection Pools.* Allí se crea un nuevo pool de conexiones como se muestra a continuación.

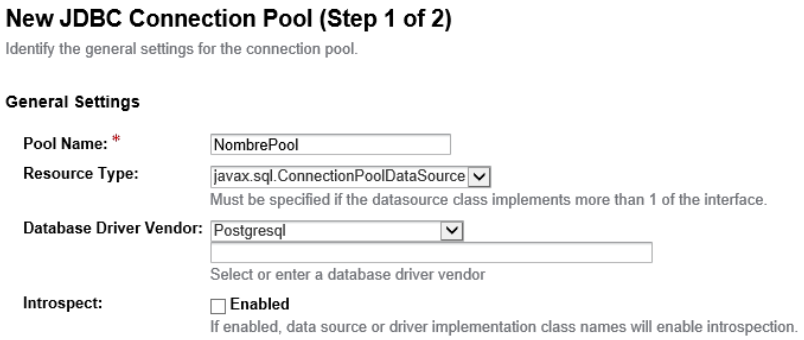


Gráfico 15 Creación Pool de Conexión con Base de Datos

Como paso siguiente se realiza la configuración relacionada con el número de conexiones y los tiempos de respuesta y a continuación agregar las siguientes propiedades con los datos de la instancia de base de datos.

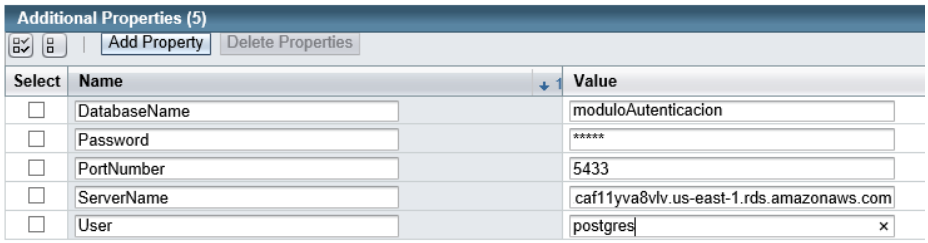


Gráfico 16 Propiedades Conexión Base de Datos

Después de creado el pool de conexiones, debe dirigirse a la pestaña *JDBC Resources* y crear un nuevo recurso con el pool de conexiones que se creó anteriormente.

Gráfico 17 Recurso de Base de Datos

Finalmente, ya tememos listo nuestra conexión a base de datos. El proyecto se conecta a esta mediante el archivo persistence.xml del proyecto Enterprise.

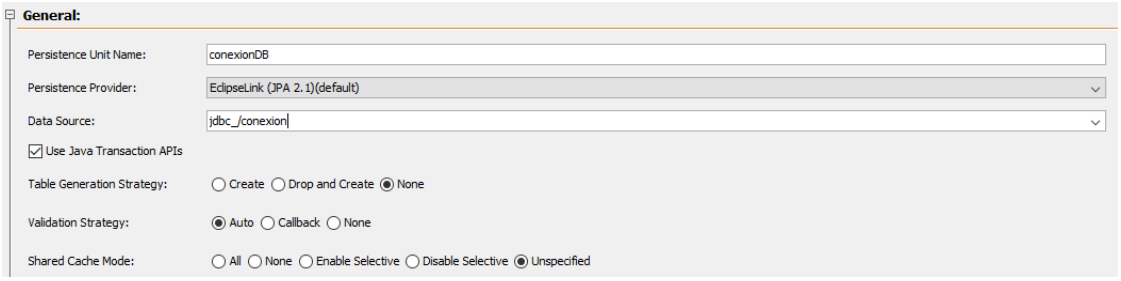


Gráfico 18 Conexión Base de Datos Archivo Persistence.xml

2.5 Despliegue proyecto archivo EAR

Para el despliegue de la aplicación, vaya a la pestaña *Aplications*. Allí en la opción *deploy.* Debe seleccionar la carpeta donde se encuentra el archivo EAR. Dentro de este selecciona el archivo WAR para ser desplegar y por último se configura la información del proyecto que se va a desplegar.

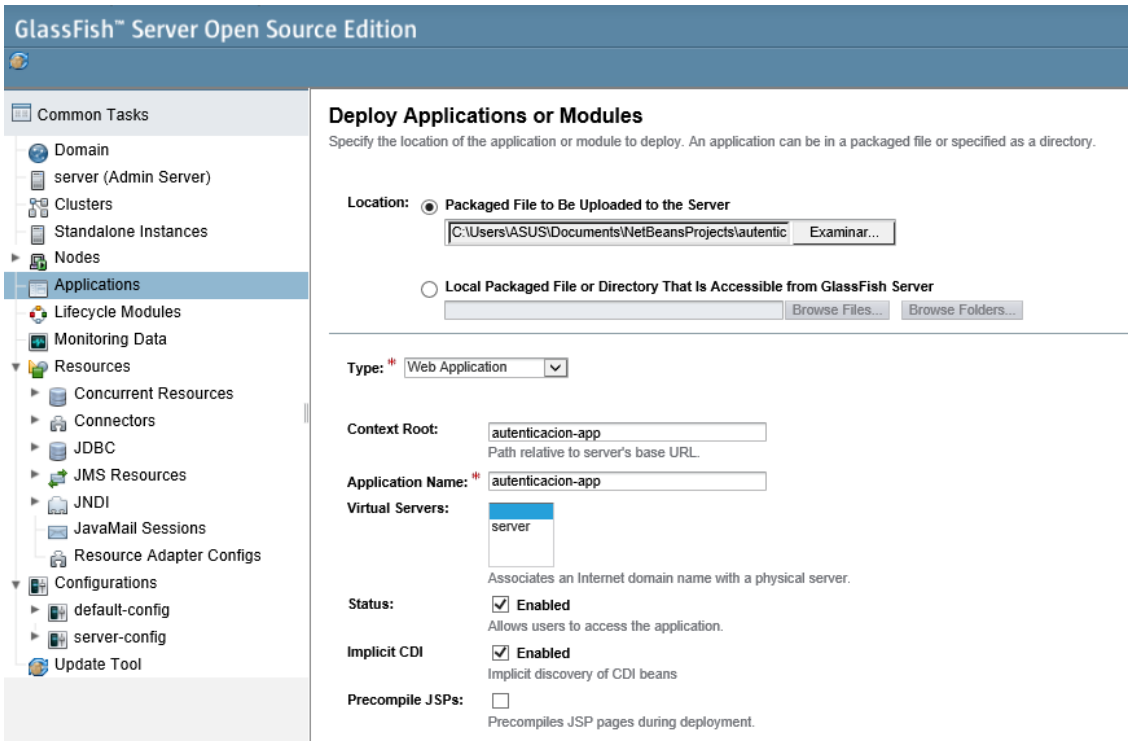


Gráfico 19 Despliegue de aplicación

El proyecto puede tardar un poco, pero al terminar ya se podrá acceder a este, a través de la IP del servidor, el puerto establecido y el nombre de la aplicación, de la siguiente manera: *(IP): (Puerto) / (Nombre de la aplicación)*.

De esta manera el proyecto ha sido desplegado correctamente y está listo para recibir las peticiones que se realicen de la plataforma y la aplicación móvil del módulo de autenticación.

www.unicundi.edu.co
unicundi@mail.unicundi.edu.co
Línea gratuita 018000 976000

Dirección de Sistemas y Tecnología
sistemasytecnologia@mail.unicundi.edu.co
PBX: 828 14 83 Ext. 110
Sede Fusagasugá

Anexo 3 Manual de Usuario

UDEC
UNIVERSIDAD DE CUNDINAMARCA

SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO AUTENTICACIÓN

MANUAL DE USUARIO
DESARROLLO DE SOFTWARE
UNIVERSIDAD DE CUNDINAMARCA

2020

www.unicundi.edu.co
unicundi@mail.unicundi.edu.co
Línea gratuita 018000 976000

Dirección de Sistemas y Tecnología
sistemasytecnologia@mail.unicundi.edu.co
PBX: 828 14 83 Ext. 110-170
Sede Fusagasugá

TABLA DE CONTENIDO

INDICE DE IMÁGENES

INDICE DE TABLAS

INTRODUCCIÓN

Este manual, tiene como finalidad poner en conocimiento de los usuarios, las funciones del módulo de autenticación que hace parte de la plataforma web de integración para el voto electrónico de los cuerpos colegiados de la Universidad de Cundinamarca. Por lo tanto, este presenta una descripción de las principales características del sistema y la forma en que interactúa el usuario con el software.

1.USUARIOS

El módulo de autenticación consta de dos roles de usuario que interactúan con el sistema; Usuario y administrador. Las funciones que pueden realizar cada uno se describen a continuación:

1.1 Administrador

El administrador es aquella persona que tiene el acceso a los recursos de la plataforma web para la parametrización de las opciones del módulo de autenticación. Este rol puede realizar las siguientes funciones:

- Ver y actualizar sus datos personales.
- Ver, agregar, eliminar usuarios con rol administrador. Cabe mencionar que mínimo debe existir un total de dos administradores.
- Ver, agregar, editar y eliminar tipos de documento visibles para el registro que se realiza desde la aplicación móvil, en el módulo de autenticación.
- Ver, agregar, editar y eliminar tipos de persona (ej. Estudiante, Docente).
- Ver, agregar, editar y eliminar programas académicos que ofrece la institución educativa.
- Ver, agregar, editar y eliminar sedes de la institución educativa, cual corresponda, además de relacionar cada sede con los programas que esta dispone.

- Establecer el dominio de correo institucional para el envió de emails de verificación.
- Consultar la información de usuarios registrados en el módulo de autenticación.

1.2 Usuario

El usuario es aquella persona que hace uso de la aplicación móvil para el proceso de autenticación y el acceso, en este caso, a los recursos de la plataforma de votación por internet de la Universidad de Cundinamarca. Este rol puede realizar las siguientes funciones:

- Registrarse con sus datos personales en el módulo de autenticación para obtener sus credenciales de acceso, esto mediante la aplicación móvil.
- Recuperar sus credenciales después de haber desinstalado la aplicación móvil o cambiado de dispositivo por alguna razón.
- Realizar el cambio de contraseña personal.
- Realizar la validación del correo electrónico institucional con el cual se registró.
- Completar el proceso de autenticación y acceder a la plataforma de votaciones.

2. REQUISITOS DE SOFTWARE

2.1 Dispositivo electrónico

Es necesario disponer de un computador de escritorio o portátil, y un dispositivo o teléfono móvil con sistema operativo Android.

2.2 Conexión a Internet

Se requiere estrictamente que los dispositivos tengan una conexión estable a internet.

2.3 Navegador

Para acceder a la plataforma web de administración del módulo de autenticación, se debe realizar desde un navegador con soporte Html5, CSS y JavaScript.

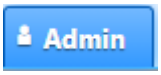
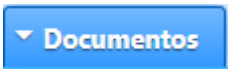
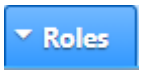
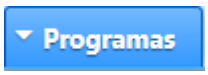
3. APLICATIVO

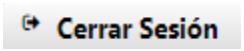
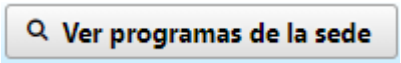
PLATAFORMA WEB DE INTEGRACIÓN PARA EL VOTO ELECTRÓNICO DE LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MODULO AUTENTICACIÓN

3.1 Iconos generales

3.1.1 Plataforma de administración.

Tabla 34 Iconos Generales Plataforma de Administración

Icono	Descripción
	Icono del botón de inicio para volver a la vista inicial donde se encuentra un instructivo de las funciones del módulo.
	Icono del botón para ir a la vista de administradores del módulo.
	Icono del botón para ir a la vista de Tipos de documento.
	Icono del botón para ir a la vista de Tipos de persona.
	Icono del botón para ir a la vista de sedes de la institución educativa.
	Icono del botón para ir a ir a la vista de programas que ofrece la institución educativa.
	Icono del botón para ir a la vista donde se establece el dominio de correo institucional.

	Icono del botón para ir a la vista donde se consultan los usuarios registrados.
	Icono del botón para cerrar sesión y salir de la plataforma
	Este icono se encuentra en las vistas que contienen tablas con registros, permite editar el registro seleccionado.
	Este icono se encuentra en las vistas que contienen tablas, permite eliminar los registros seleccionados.
	Este icono se encuentra en la vista de sedes. Este abre la tabla con los programas asignados para la sede seleccionada.
	Este icono se encuentra en la vista sedes, cuando se despliegan los programas de cada sede. Sirve para agregar un programa académico a la sede.
	Este icono se encuentra en la vista sedes, cuando se despliegan los programas de cada sede. Sirve para quitar los programas académicos seleccionados de la sede.

3.1.2 Aplicación Móvil.

Tabla 35 Iconos Generales Aplicación Móvil

Icono	Descripción
	Icono para desplegar menú lateral de la aplicación
	Icono para ir al inicio y ver los datos del usuario portador de credencial.

Cambiar Contraseña	Icono para ir a la vista donde se realiza la actualización de contraseña personal.
Validar Email	Icono para ir a la vista donde se realiza la validación de correo institucional.
Ayuda	Icono para ir a la vista donde se muestra la ayuda para el uso de la aplicación.

3.2 Ingreso al aplicativo

3.2.1 Plataforma de administración.

Para ingresar a la plataforma de administración del módulo de autenticación, desde su navegador debe dirigirse a la siguiente dirección http://ip-servidor:8080/autenticacion-app donde se le solicitara un usuario y contraseña para poder acceder como administrador, que previamente debió haber sido registrado.

Gráfico 20 Interfaz de inicio de sesión

3.2.2 Aplicación Móvil.

El usuario debe disponer de un dispositivo Android en donde instalar la aplicación. Posteriormente al ingresar por primera vez la aplicación móvil, el usuario debe seleccionar si desea registrarse para obtener sus credenciales de acceso o recuperarlas en caso de que ya se haya hecho un registro previamente. La descripción de las funciones mencionadas se realizará más adelante.

Gráfico 21 Interfaz Inicio de la Aplicación Móvil

3.3 Componente web administrador

A continuación, se describirán las funciones del componente web desde el cual se administra y parametriza el módulo de autenticación.

Gráfico 22 Interfaz Inicio Administrador

3.3.1 Sección Información de administrador

A la derecha de la ventana se presenta la sección que contiene la información del administrador que ha ingresado en la plataforma, además de los botones para realizar la actualización de datos y contraseña de ingreso al sistema.

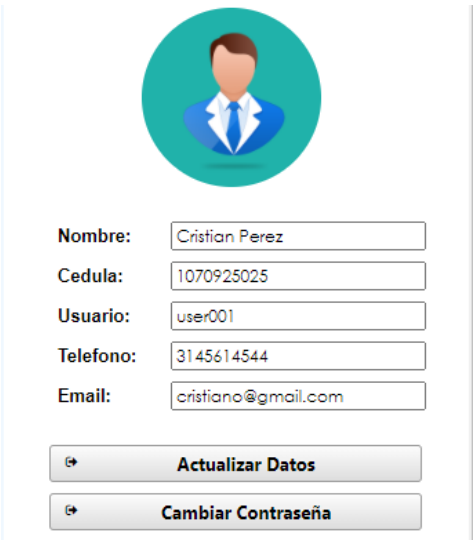


Gráfico 23 Sección Información de Administrador

Si selecciona la opción de actualizar datos, se despliega una ventana con el formulario que contiene la información que puede ser editada por el administrador. Al presionar el botón actualizar se guardan los cambios.

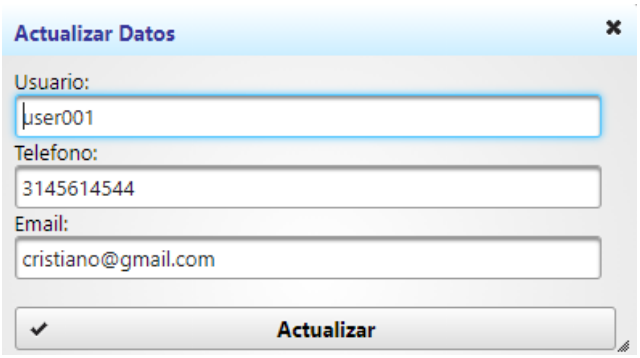


Gráfico 24 Actualizar Datos Administrador

Al presionar el botón de actualizar contraseña se despliega una ventana con el formulario para el cambio de contraseña, en donde el administrador debe ingresar su clave actual y la que nueva que desea establecer. Al presionar el botón aceptar, se guardan los cambios.

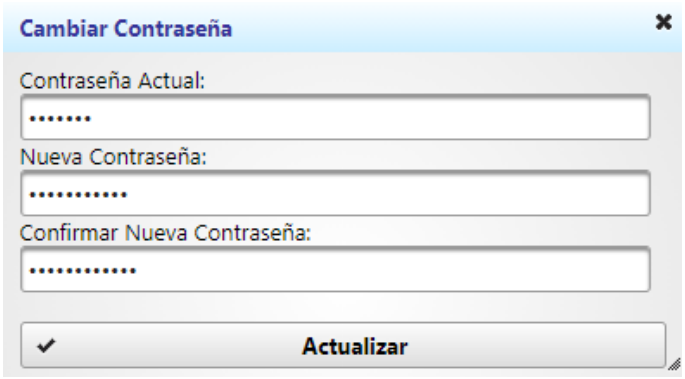


Gráfico 25 Cambiar Contraseña Administrador

3.3.2 Sección Admin

Al seleccionar la pestaña de admin, se muestra la vista que contiene la tabla con la información de los administradores del sistema, además de la opción para agregar un nuevo administrador al módulo de autenticación.

Gráfico 26 Interfaz Sección Admin

Al presionar el botón de Registrar administrador se despliega un formulario en donde se solicitan los datos para el registro de un nuevo administrador, entre ellos

se encuentran los datos personales, de contacto y la creación de un usuario y contraseña los cuales podrán ser alterados por el en su primer acceso a la plataforma. Al presionar el botón Registrar, se guardan los datos y se actualiza la tabla de administradores.

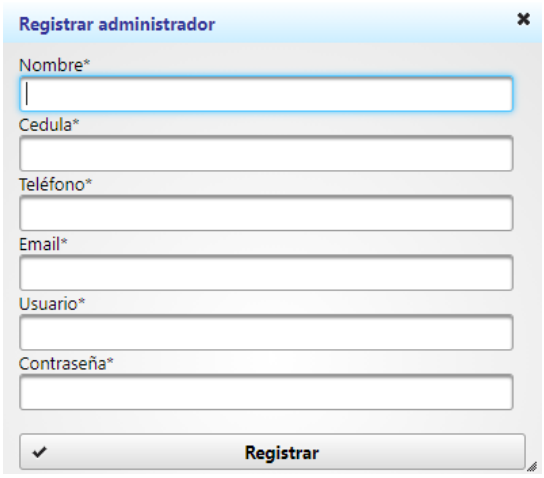


Gráfico 27 Registrar Nuevo Administrador

En los campos usuario y cedula hay un filtro en el caso de que se requiera buscar la información de algún administrador de manera más rápida.

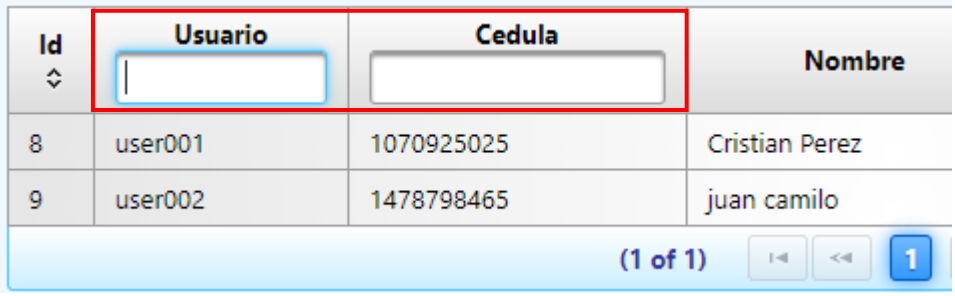


Gráfico 28 Filtro Tabla Administradores

En la ultima columna de la tabla se encuentran unos cuadros de selección, estos sirven para identificar los registros que desea borrar, posteriormente al presionar el

boton borrar, aparecera un cuadro de dialogo en donde se solicita una confirmacion para suprimir los registros seleccionados.

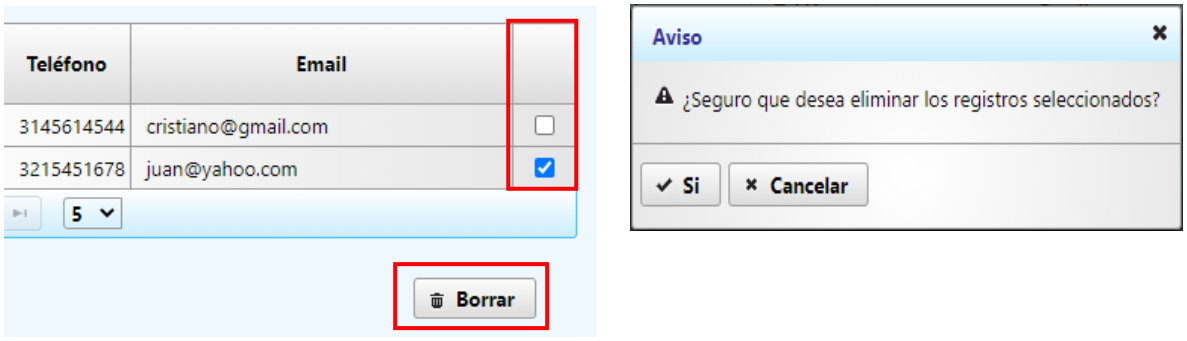


Gráfico 29 Borrar Registro Tabla

Cabe aclarar que en el sistema siempre deben existir minimo dos administradores, esta caracteristica se encuentra validada y en caso de intentar eliminar mas registros de los permitidos se mostrara una advertencia al administrador.

3.3.3 Sección Documentos

Al seleccionar la pestaña de Documentos, se muestra la vista que contiene la tabla con los tipos de documentos válidos para realizar un registro en el módulo de autenticación, estos son definidos por los administradores del sistema. En la parte superior se encuentra un campo en donde se ingresa el nombre del tipo de documento que se desea agregar, al presionar el botón agregar se guarda la información y se actualiza la tabla.

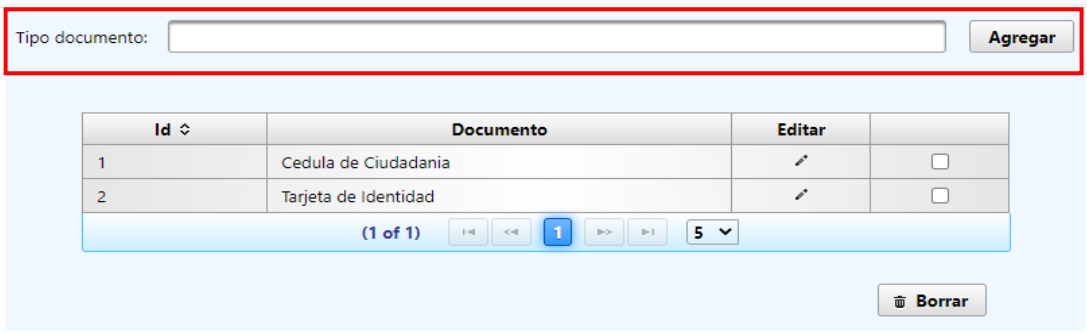


Gráfico 30 Interfaz Sección Documentos

El procedimiento para el proceso de editar y eliminar registros se realiza de la misma manera que en la tabla de administradores que se explicó en la sección anterior.

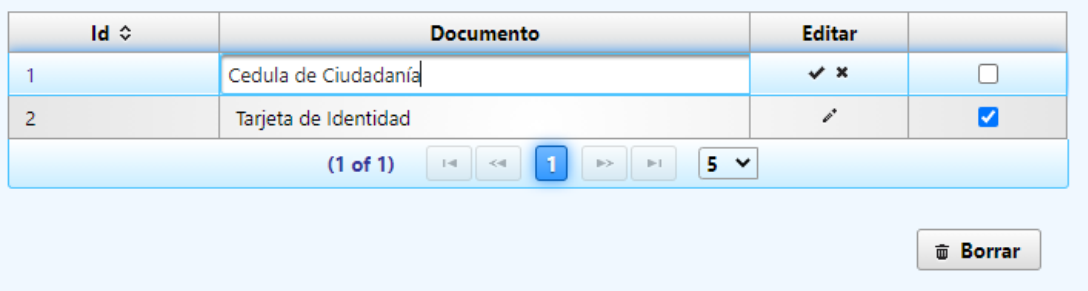


Gráfico 31 Editar Registro Tabla

3.3.4 Sección Roles

En la sección roles el administrador puede gestionar los tipos de persona que pueden registrarse en el módulo de autenticación. Al igual que en las secciones anteriores se muestra la tabla con los registros definidos por los administradores y el procedimiento para el registro, la edición y eliminación se realiza de la misma manera como se ha explicado anteriormente.

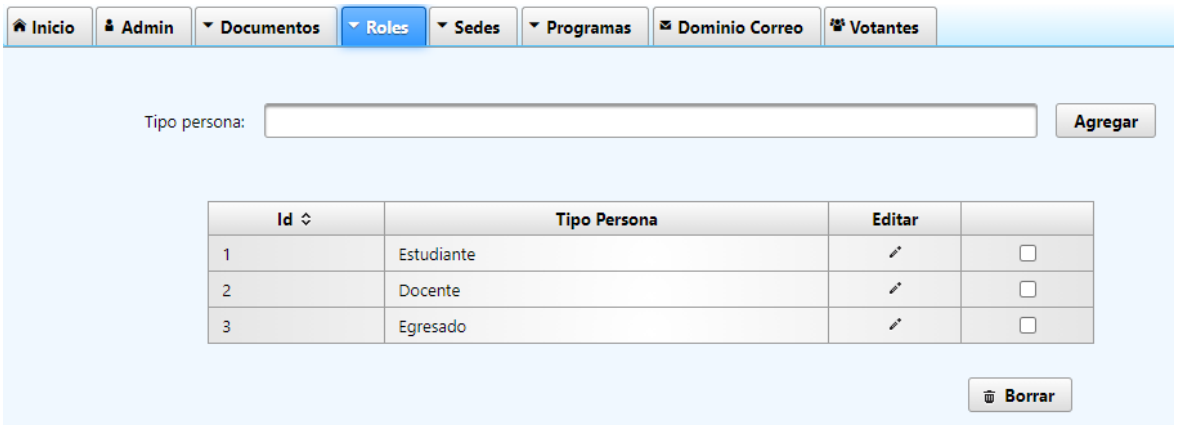


Gráfico 32 Interfaz Sección Roles

3.3.4 Sección Programas

En la sección programas el administrador puede gestionar los programas académicos que ofrece la institución educativa, los cuales se verán reflejados en el formulario de registro de la aplicación móvil, para saber a qué carrera pertenecen las personas que se registran en el módulo de autenticación. El procedimiento para el registro, la edición y eliminación se realiza de la misma manera como se ha explicado en las secciones anteriores.

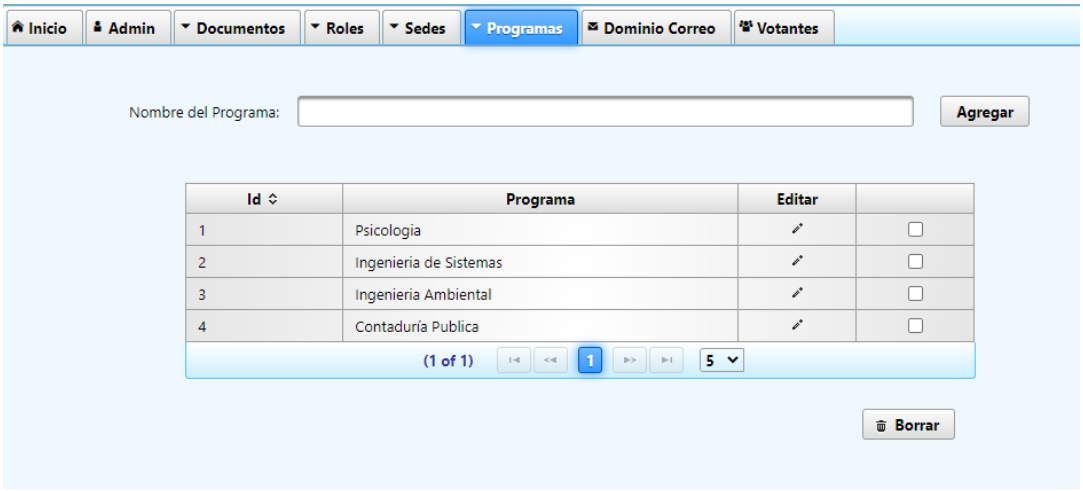


Gráfico 33 Interfaz Sección Programas

3.3.5 Sección Sedes

En esta sección se encuentran las sedes de tiene la institución educativa, además de poder gestionar los programas que se ofrecen por cada sede, según sea el caso. En primer lugar, se encuentra el campo para agregar el nombre de la sede. Al agregar una sede se actualiza la tabla.

Para administrar los programas que se ofrecen por sede, debe seleccionar con un clic la fila de la sede que desea alterar y presionar el botón de ver programas de la sede. Esta acción despliega una tabla con los programas que ofrece esa sede, además de una lista desplegable con todos los programas que tiene la institución, esta última para ir agregando o quitando los programas académicos a la sede.

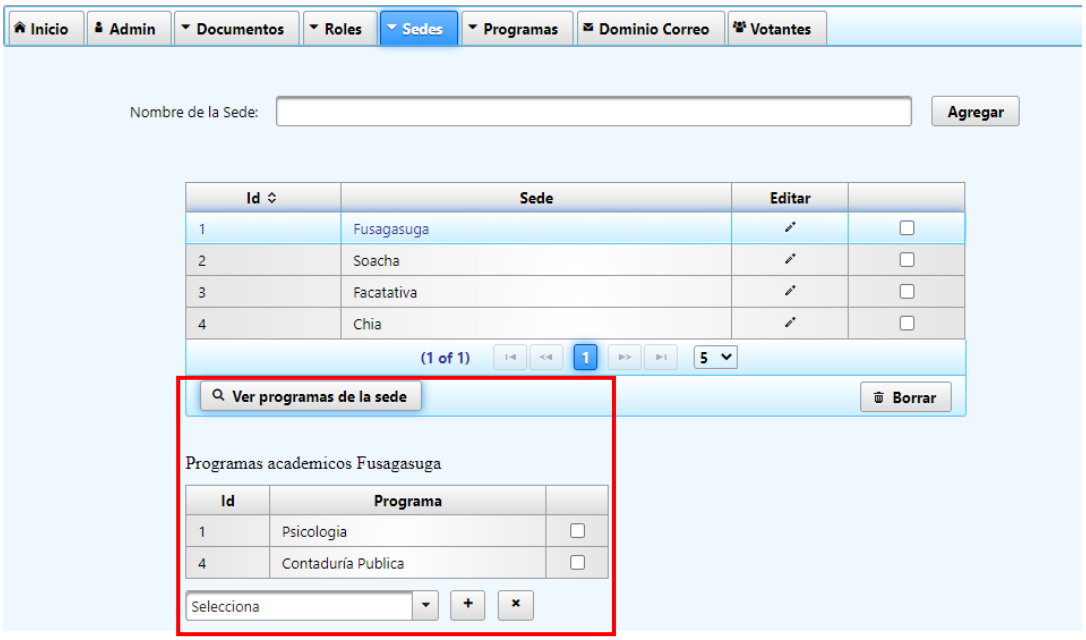


Gráfico 34 Interfaz Sección Sedes

Para agregar un programa a una sede se elige una carrera en la lista desplegables y se da clic a el botón con el icono (+), se ira actualizando la tabla a medida que se van agregando programas. Para quitar algún programa de una sede se selecciona en el cuadro de la derecha y se presiona el botón (×).

El procedimiento para la edición y eliminación de sedes se realiza de la misma manera como se ha explicado en las secciones anteriores.

3.3.5 Sección Dominio de Correo

En esta sección el administrador parametriza el dominio de correo electrónico institucional, el cual es parte importante dentro del proceso de registro de los usuarios, debido que, mediante este, se realiza la verificación de correo. Inicialmente hay un dominio por defecto, pero que puede ser modificado por el administrador de acuerdo con la institución.

En el campo se escribe el dominio de correo como se indica y al presionar el botón de actualizar dominio, se guardan los cambios en el sistema.

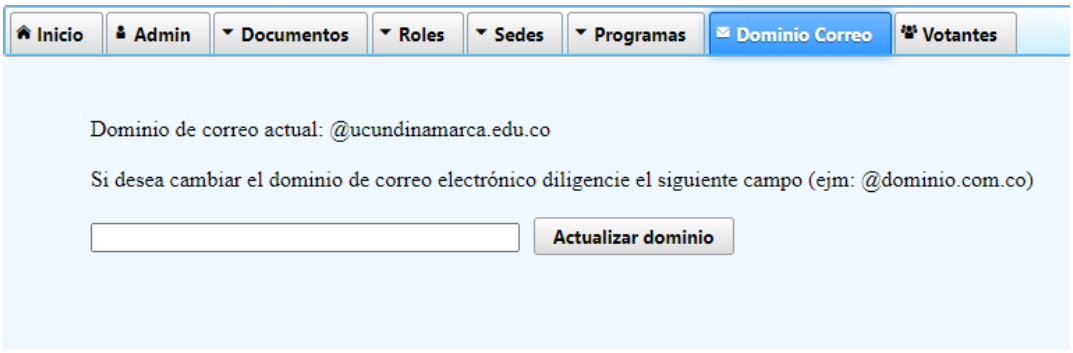


Gráfico 35 Interfaz Sección Dominio Correo

3.3.6 Sección Votantes

En esta sección el administrador puede consultar la información de un usuario registrado en el módulo de autenticación, con su número de identificación. Al diligenciar el campo solicitado y presionar el botón buscar, se mostrará una tabla con la información de ese usuario, si existe.

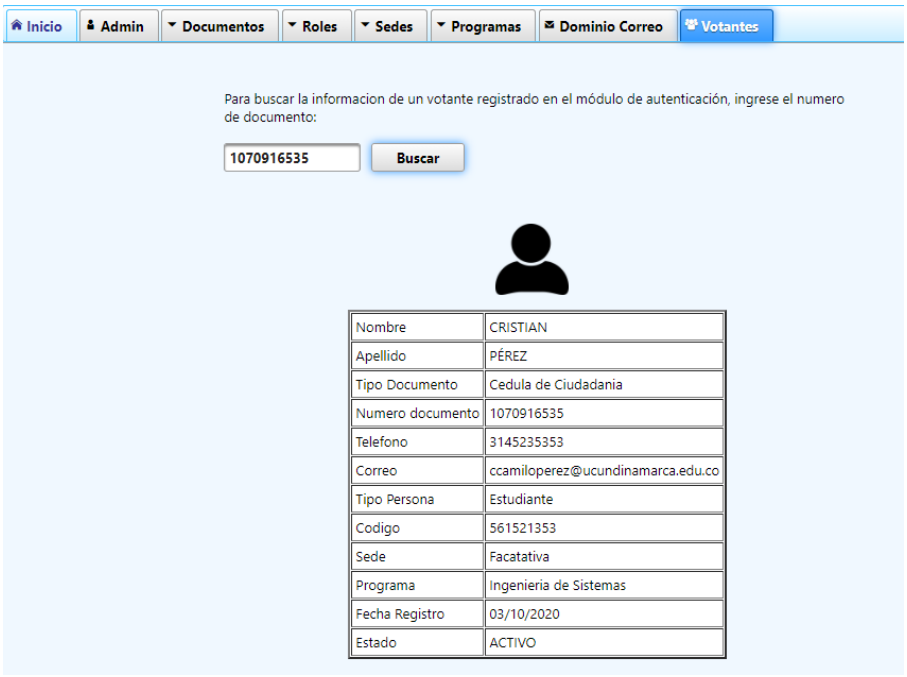


Gráfico 36 Interfaz Sección Votantes

3.4 Aplicación Móvil (ISVOTE)

A continuación, se describirán las funciones de la aplicación móvil destinada para el almacenamiento de credenciales y efectuar el proceso de autenticación de los usuarios a través de este módulo.

3.4.1 Registro de usuario

Cuando el usuario ingresa a la aplicación por primera vez y selecciona la opción de registrarse para obtener sus credenciales, se muestra el formulario de registro, el cual deberá diligenciar con sus datos personales, además de establecer una contraseña personal, factor importante en el proceso de autenticación.

Gráfico 37 Interfaz Registro de Usuario

3.4.2 Recuperación de credenciales

Cuando el usuario entra a la aplicación por primera vez y selecciona la opción de recuperación de credenciales, previamente tuvo que haber realizado el registro en el módulo de autenticación, pero por alguna razón perdió las llaves que se almacenaban, ya sea por desinstalar la aplicación o por cambio de dispositivo. Aquí

el usuario llena el formulario con los datos que se solicitan y si todo es correcto recupera sus credenciales.

Gráfico 38 Interfaz Recuperar Credenciales

3.4.3 Home

Cuando el usuario ya se ha registrado o ha recuperado sus credenciales de acceso, se ingresa directamente a la pantalla del home, donde se muestra algunos datos del usuario como evidencia de que ha obtenido las credenciales necesarias para el proceso de autenticación de forma correcta.

Gráfico 39 Interfaz Home

3.4.4 Cambiar contraseña

En esta sección el usuario puede realizar la actualización de su contraseña personal para el proceso de autenticación de identidad. En caso de que el usuario haya olvidado su contraseña, al presionar el botón de recuperar se enviara un correo con la clave.

Gráfico 40 Interfaz Cambiar Contraseña

3.4.5 Verificar Email

El usuario debe realizar la verificación de correo electrónico para confirmar que la información que ingreso es verídica y corroborar que se trata de una persona perteneciente a la institución. Esto por medio de un código que se envió al correo del usuario y el cual se ingresa en esta sección.

Gráfico 41 Interfaz Verificar Email

3.4.6 Sección ayuda

En esta sección se describe como se realiza el proceso de autenticación a través de la aplicación móvil y sirve como guía para el usuario.

Gráfico 42 Interfaz Ayuda

3.5 Proceso de autenticación

Inicialmente el usuario debe disponer de su dispositivo móvil con el que se registró, con una conexión a internet. Cuando el usuario ingresa con su número de identificación y su contraseña en la plataforma a la cual desea acceder (En este caso la plataforma de votación por internet institucional, de la Universidad de Cundinamarca), el sistema envía una notificación al teléfono móvil como la que se muestra a continuación.

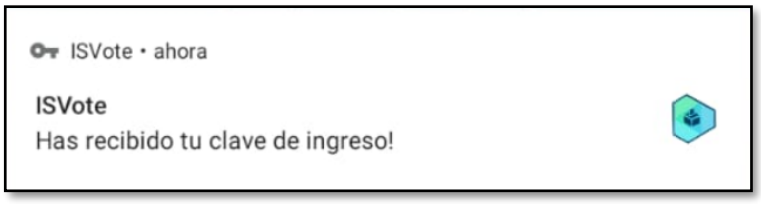


Gráfico 43 Notificación Aplicación

El usuario deberá abrir esta notificación antes del tiempo que tiene establecido para que se borre, si no deberá volver a intentarlo para recibir de nuevo la notificación. Al seleccionar la aplicación se despliega la aplicación solicitando ingresar de nuevo su contraseña personal.

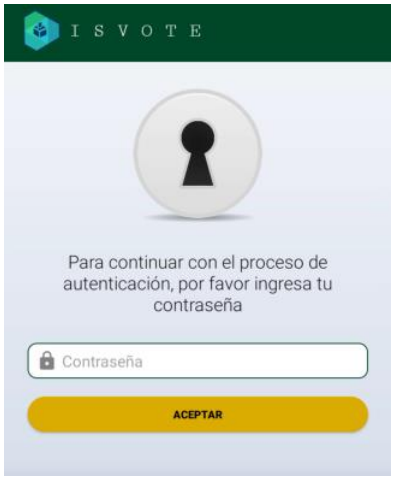


Gráfico 44 Solicitud Clave Autenticación

Cuando el usuario ingresa la contraseña y es correcta, la aplicación muestra al usuario el valor de una clave OTP, con la cual podrá acceder a la plataforma de votación de la institución.

Gráfico 45 Clave OTP de Autenticación

Así concluye el proceso de autenticación. Cada vez que se vaya a ingresar a la plataforma se realiza de la misma manera.

4. Control de cambios del manual

Tabla 36 Control de cambios

Actualización Nro.	Descripción del cambio	Versión del aplicativo	Fecha de cambio

www.unicundi.edu.co
unicundi@mail.unicundi.edu.co
Línea gratuita 018000 976000

Dirección de Sistemas y Tecnología
sistemasytecnologia@mail.unicundi.edu.co
PBX: 828 14 83 Ext. 110
Sede Fusagasugá

Anexo 4 Articulo CIETA 2020

ANALYSIS FOR THE DEVELOPMENT OF A MULTIFACTOR AUTHENTICATION SYSTEM BASED ON ASYMMETRIC KEY ENCRYPTION, FOR E-VOTING

ANÁLISIS PARA EL DESARROLLO DE UN SISTEMA DE AUTENTICACIÓN MULTIFACTOR BASADO EN CIFRADO DE CLAVE ASIMÉTRICA, PARA VOTO ELECTRÓNICO

Cristian Camilo Pérez Bohórquez, Gina Maribel Valenzuela Sabogal

Universidad de Cundinamarca
Extensión Facatativá, Cundinamarca, Colombia.
Tel.: 57-1-8920706 | 892 0707
E-mail: {ccamiloperez, gvalenzuela}@ucundinamarca.edu.co

Abstract: The authentication process constitutes an indispensable factor for the operations carried out through the internet, due to the increasing progress that the development of new e-learning platforms, electronic government and the economy of the current world has represented in the last decade, for what a digital, verifiable and trustworthy identity is of vital importance to avoid fraud, corruption and data loss in an information system. The methods based on multi-factor authentication, widely used in different sectors of the current web industry and public key encryption algorithms are the basis for the study and development of a multi-factor authentication module for an internet voting platform. The current project starts from the generation of asymmetric keys for platform users, a repository of credentials and the implementation of a challenge response protocol linked to the authentication process, being the basis for the establishment of an institutional digital environment and electronic government.

Keywords: Authentication, Informatic security, Cryptography, Asymmetric Key.

Resumen: El proceso de autenticación constituye un factor indispensable para las operaciones que se realizan a través de internet, debido al creciente avance que ha representado en la última década el desarrollo de nuevas plataformas de e-learning, gobierno electrónico y la economía del mundo actual, por lo que una identidad digital, verificable y de confianza es de vital importancia para evitar el fraude, la corrupción y la perdida de datos en un sistema de información. Los métodos basados en la autenticación multifactor, ampliamente usados en diferentes sectores de la industria web actual y los algoritmos de cifrado de clave pública son la base para el estudio y desarrollo de un módulo de autenticación multifactor a fin de una plataforma de voto por internet. El proyecto en curso parte de la generación de claves asimétricas para los usuarios de la plataforma, un repositorio de credenciales y la implementación de un protocolo de desafío respuesta vinculado al proceso de autenticación, siendo la base para el establecimiento de un entorno digital institucional y gobierno electrónico.

Palabras Clave: Autenticación, Seguridad Informática, Criptografía, Clave Asimétrica.

I. INTRODUCCIÓN

En la actualidad, con el uso masivo de dispositivos electrónicos, sumado al creciente desarrollo y aplicación de nuevas tecnologías de la información, el tratamiento de datos y el pleno auge del internet, se ha generado un aumento en la necesidad de implementar procesos de autenticación que permitan determinar la identidad de los usuarios que interactúan con un sistema, sobre todo en sectores como la industria, la economía y el gobierno electrónico, en los que es indispensable minimizar el riesgo de fraude en las partes involucradas en una transacción web. Para ello existen múltiples estándares y alternativas que ofrecen diferentes niveles de seguridad que van desde métodos de autenticación simple como la implementación de usuario y contraseña, hasta validación de la identidad por medio de análisis biométrico.

Actualmente se destaca el uso de métodos de autenticación multifactor y de identidad basados en criptosistemas y esquemas de firma digital. La infraestructura de clave pública (PKI) se postula como la base para dichos procesos, debido al éxito de su implementación en países como Estonia (Vinkel, 2014), en donde los avances en materia de gobierno electrónico y voto por internet han demostrado el potencial de dicha tecnología, que se basa en un conjunto de protocolos y estándares de seguridad por los cuales se realiza un proceso de generación y distribución de claves relacionadas a través de un algoritmo o función matemática y almacenadas en un DNI electrónico o el teléfono móvil del titular, además de que permite la administración de certificados digitales, autenticación de identidad y firma digital. Principios en los que el proyecto está basado, tomando algunos de los elementos característicos de dicha infraestructura y que se mencionan en este artículo.

II. PROBLEMA

La influencia de los sistemas en el mundo actual, ha llevado a la automatización de diferentes procesos que se realizaban de forma presencial, trámites para los que era inevitable tener que desplazarse a una entidad y hacer filas interminables, sin mencionar el desperdicio de papel que supone un impacto sobre el desarrollo sostenible de una sociedad a la que la sobreexplotación de recursos está llevando a un punto sin retorno. Muchos países y sectores de la industria han considerado nuevas alternativas como brindar a sus usuarios la posibilidad de realizar diferentes tipos de transacciones a través de internet, una solución viable, necesaria. Sin embargo, aún tiene muchos retos que enfrentar, sobre todo en materia de seguridad, debido a que dichas transacciones que se realizan a través de un dispositivo electrónico, desde un ambiente no controlado carecen de supervisión, suponiendo un incremento en el riesgo de suplantación de identidad y la necesidad de determinar si una persona que intenta acceder a una información es quien dice ser en realidad, a esto se suma la desconfianza que genera la implementación de dichos sistemas en algunos sectores de la población, adicionalmente la brecha digital existente entre las generaciones más adultas y los más jóvenes. Lo anterior lleva al planteamiento de las siguientes preguntas; ¿Cómo asegurar la identidad de una persona o entidad a través de un entorno web? ¿cuáles son las alternativas que existen actualmente en materia de autenticación e identidad digital?

III. IDENTIFICACIÓN, AUTENTICACIÓN Y AUTORIZACIÓN EN PLATAFORMAS DIGITALES

Cuando se hace referencia a las medidas de seguridad dentro de una infraestructura digital; la identificación de usuarios, el proceso de autenticación y la autorización son conceptos clave.

Fig. 1. Identificación, Autenticación y autorización. Fuente: (Andress & Winterfeld, 2014).

3.1. Identificación

La identificación, es simplemente una afirmación de quiénes somos, como persona o a través de un sistema informático.

3.2. Autenticación

> La autenticación es, en un sentido de seguridad de la información, el conjunto de métodos que utilizamos para establecer un reclamo de identidad como verdadero. Es importante tener en cuenta que la autenticación solo establece si el reclamo de identidad realizado es correcto (Andress & Winterfeld, 2014).

La autenticación a través de dispositivos electrónicos constituye la base del futuro de las operaciones transaccionales y los trámites a distancia, por lo que una identidad digital de confianza es el punto de partida para un sistema o plataforma que requiera ofrecer garantías de seguridad a sus usuarios.

> Además, se define como un elemento que hace parte de un sistema más amplio de prácticas, procedimientos e implementaciones técnicas, que trabajan juntas para proteger los sistemas de información, las redes y las comunicaciones electrónicas (OECD, 2007).
>
> Es primordial entender que la identidad digital es la representación única de un sujeto involucrado en una transacción en línea, esta siempre es única en el contexto de un servicio digital, pero no necesariamente necesita identificar de forma única al sujeto en todos los contextos. (Grassi, Garcia, & Fenton, 2017).

La directriz de autenticación electrónica establecida por el Instituto Nacional de Estándares y Tecnología NIST (Burr et al., 2013), señala tres factores básicos que caracterizan a los sistemas de autenticación estándar:

- El primero de ellos es aquel basado en el conocimiento, más conocido KBA (Knowledge Based Authentication), que hace referencia a cosas que únicamente conoce cada persona, por ejemplo, el uso de usuarios y contraseñas privadas.
- El segundo a partir de la posesión, se caracteriza por la obtención de un documento o elemento único por parte de cada usuario, ya sea un documento de identidad ID-Card, un token o un certificado digital.
- Por último, se encuentra la autenticación basada en todo aquello inherente a cada persona, recurriendo a datos biométricos como la huella dactilar, las facciones del rostro o la voz.

"Las buenas prácticas señalan que, para operaciones de riesgo alto, se debe utilizar una combinación de al menos dos de estos elementos" (Pareja, Pedak, Gómez, & Barros, 2017) lo que se denomina autenticación multifactor.

3.2.1. Autenticación Multifactor (MFA)

La autenticación multifactor, hace referencia a la implementación de las fortalezas de los métodos anteriormente mencionados, para un mayor nivel de seguridad, teniendo en cuenta que la combinación de múltiples fuentes de datos garantiza mayor precisión y confianza a la hora de realizar la identificación de un usuario.

> La multiplicación del número de factores de autenticación aumenta el nivel de seguridad general, pero supone algunos retos como la administración del ciclo de vida de cada factor, la usabilidad del sistema, los costes de elementos electrónicos como tarjetas, lectores o sensores biométricos y la carga del servicio de ayuda al usuario (Evidian, 2015) .

Teniendo en cuenta los principios mencionados anteriormente, el objetivo de implementar un MFA es dificultar la intrusión de usuarios no autenticados a un sistema, dispositivo o red; debido a que este constituye un sistema de defensa por niveles.

Tabla 1: Niveles de garantía para autentificación de entidades

Nivel	Descripción
1-Bajo	Poca o ninguna confianza en la entidad declarada.
2-Medio	Cierta Confianza en la entidad declarada.
3-Alto	Mucha confianza en la entidad declarada.
4-Muy alto	Muchísima confianza en la entidad declarada.

Fuente: Marco de garantía de autenticación de entidad (UIT, 2013).

1) Nivel de garantía 1: Existe cierta confianza en la identidad de la persona que se ha autenticado en diferentes eventos. Generalmente se emplea cuando el nivel de riesgo que representa una autenticación errónea es bajo.

2) Nivel de garantía 2: Se emplea cuando el riesgo que representa la autenticación errónea de un usuario es moderado, por lo que se puede recurrir a la autenticación de doble factor.

3) Nivel de garantía 3: En este nivel de garantía se emplean los sistemas de autenticación multifactor, debido al nivel de riesgo considerable que representa la autenticación errónea de una entidad.

4) Nivel de garantía 4: Cuando los riesgos que representa una autenticación errónea son muy altos, se recurre a la utilización de medios físicos inalterables además del uso de certificados digitales que permitan identificar idóneamente a su portador.

3.3. Autorización

"La autorización nos permite determinar, una vez que hemos autenticado a la parte en cuestión, exactamente qué se les permite hacer" (Andress & Winterfeld, 2014). Uno de los mecanismos de autorización más utilizados es el control de acceso basado en roles.

IV. CRIPTOGRAFÍA

La palabra criptografía proviene en un sentido etimológico del griego Kriptos, "Ocultar", y Graphos, "escritura", lo que significaría ocultar la escritura, o en un sentido más amplio sería aplicar alguna técnica para hacer ininteligible un mensaje.

> Es la ciencia encargada de diseñar funciones o dispositivos, capaces de transformar mensajes legibles o en claro a mensajes cifrados de tal manera que esta transformación (cifrar) y su transformación inversa (descifrar) sólo pueden ser factibles con el conocimiento de una o más llaves (Paredes, 2006).

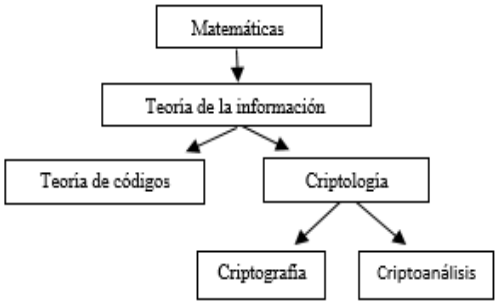


Fig. 2. Origen de la Criptografía. Fuente: (Paredes, 2006).

El uso de técnicas criptográficas tiene como propósito prevenir algunas faltas de seguridad en un sistema computarizado. Otros autores plantean que la Criptografía se ocupa del problema de enviar información confidencial por un medio inseguro.

> Para garantizar la confidencialidad, podría asegurarse el medio de transmisión o bien la información; la Criptografía utiliza este último enfoque, encripta la información de manera que, aun cuando se encuentre disponible para cualquiera, no pueda utilizarla, a menos que alguien autorizado la descifre (Marrero Travieso, 2003).

4.1 Clasificación de la criptografía moderna

La criptografía se divide en dos grandes ramas, la de clave privada o simétrica y la de clave pública o asimétrica.

4.1.1 Criptografía Simétrica

La criptografía de clave simétrica, también conocida como criptografía de clave privada, utiliza una sola clave tanto para el cifrado del texto sin formato como para el descifrado del texto cifrado.

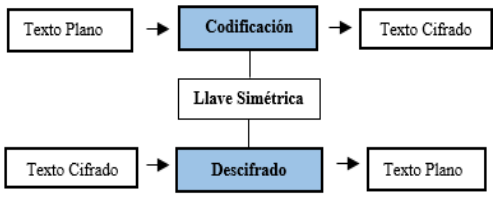


Fig. 3. Proceso de clave para criptografía simétrica. Fuente: (Medina & Miranda, 2015).

4.1.2 Criptografía Asimétrica

La criptografía de clave asimétrica, también conocida como criptografía de clave pública, utiliza dos claves: una clave pública y una clave privada.

> La clave pública se usa para cifrar los datos enviados desde el remitente al receptor. la clave privada se utiliza para descifrar los datos que llegan al extremo receptor (Andress & Winterfeld, 2014).

"Si encripta datos utilizando la clave pública de alguien, solo su clave privada correspondiente puede descifrarla" (Ristić, 2015). Principio empleado en el módulo de autenticación para voto electrónico, por medio de la aplicación de un protocolo de desafío- respuesta.

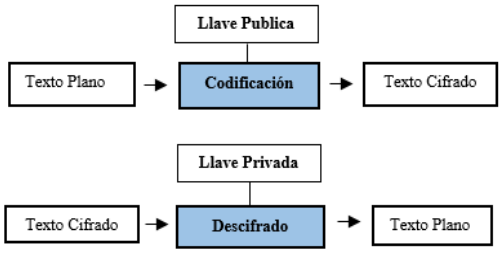


Fig. 4. Proceso de clave para criptografía asimétrica. Fuente: (Medina & Miranda, 2015).

4.2. Algoritmos de clave Asimétrica

> El algoritmo RSA, llamado así por sus creadores Ron Rivest, Adi Shamir y Leonard Adleman, es un algoritmo asimétrico utilizado en todo el mundo, incluso en el protocolo Secure Sockets Layer (SSL), que se utiliza para asegurar muchas transacciones comunes como Web y tráfico de correo. RSA se creó en 1977 y sigue siendo uno de los algoritmos más utilizados en el mundo hasta el día de hoy (Andress & Winterfeld, 2014).

"Se basan en la dificultad de factorizar números enteros de gran tamaño" (Franchi, 2012).

- Cifrado de pequeñas cantidades de datos, por ejemplo, claves.
- El sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits.
- Algoritmo más sencillo de entender para su aplicación.
- Firmas digitales.

ECC, la criptografía de curva elíptica (ECC) lleva el nombre del tipo de problema matemático en el que se basan sus funciones criptográficas. ECC tiene varias ventajas sobre otros tipos de algoritmos (Andress & Winterfeld, 2014).

- Mayor fuerza criptográfica.
- Claves más cortas que muchos otros tipos de algoritmos.
- Rápido y eficiente.

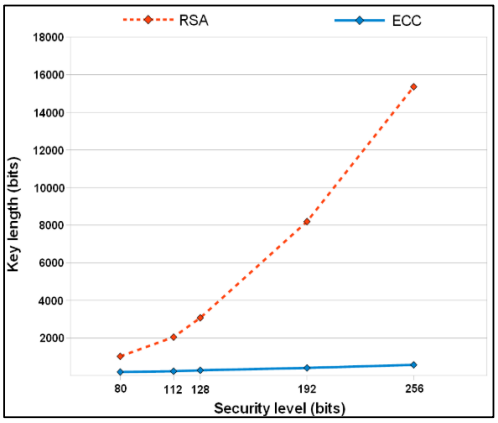


Fig. 5. Comparación de longitud de clave para criptosistemas RSA y ECC. Fuente: (Gayoso, Hernandez, & Sanchez, 2010).

Por lo anterior se ha elegido la implementación de llaves ECC en el desarrollo del proyecto.

V. HERRAMIENTAS DE DESARROLLO

El desarrollo del proyecto se basa fundamentalmente en el lenguaje de programación Java.

Desde su aparición en la década de 1990, este lenguaje ha experimentado un crecimiento constante con respecto al número de programadores y despliegues comerciales, siendo utilizado de forma masiva en aplicaciones web y corporativas (Martínez, Ávila, García, & Encinas, 2005).

En la arquitectura Java, la API de seguridad (construida alrededor el paquete java.security) es una de las principales interfaces del lenguaje. La implementación de la biblioteca Java Cryptography Architecture (JCA) que "es una especificación del lenguaje que precisa interfaces y clases que sirven de base para las implementaciones concretas de algoritmos criptográficos" (Maiorano, 2010), en conjunto con Java Cryptography Extension (JCE) que más exactamente proporciona implementaciones para cifrado, algoritmos de encriptación, generación y concordancia de claves de acuerdo a los lineamientos definidos por la JCA.

5.1. Proveedor Bouncy Castle

Es un kit de herramientas criptográficas de terceros.

Las API criptográficas de este proveedor son atendidas por una organización benéfica australiana, la Legión de Bouncy Castle Inc., que se ocupa del mantenimiento de dichas API (Ganesh Adhagale, 2014).

- Bouncy Castle tiene soporte para muchos algoritmos
- Es libre en términos de licencia.
- Ofrece soporte matemático para criptografía de curvas elípticas. Las clases de utilidad se pueden usar para producir y leer cadenas BASE64 y hexadecimales.

VI. METODOLOGIA

Para el diseño y desarrollo del módulo de autenticación se establece el uso de elementos de la metodología ágil basada en SCRUM, debido a que este "es un marco dentro del cual puede emplear diversos procesos y técnicas" (Schwaber & Sutherland, 2011) . La forma en que se adapta esta metodología al desarrollo del módulo, se basa en el establecimiento de objetivos claros y alcanzables en un tiempo determinado por el equipo de trabajo, que permitan evidenciar avances en el desarrollo del proyecto además de generar un plan estratégico basado en dicho progreso, con una respuesta al cambio y a los problemas que se puedan presentar, además de la retroalimentación en cada uno de los procesos presentes en la ejecución e incremento del software.

La organización y jerarquización de las tareas está fundamentado en el modelo en cascada para el proceso de desarrollo del software, como se muestra en el siguiente esquema:

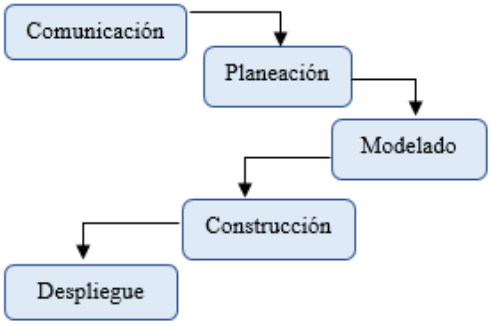


Fig. 6. Modelo cascada desarrollo de software. Fuente: (Pressman, 2010).

VII. RESULTADOS

7.1 Problema de almacenamiento de clave

Durante el estudio de los requerimientos y el diseño del módulo se estableció que posterior al proceso de registro, cada usuario es el responsable de almacenar la llave privada. Por lo que se concluyó en la necesidad del desarrollo de una aplicación móvil complementaria al sistema de registro y generación de claves, cuya función sería el almacenamiento de dicha llave privada y ser un elemento primordial e indispensable para el proceso de autenticación y acceso a la plataforma de voto por internet.

7.2 Problema de distribución de clave

Consiste en la problemática que se genera en el momento del envió de la clave privada a cada usuario por un canal "inseguro" de comunicación y constituye un riesgo de seguridad, debido a la posible interceptación de la llave privada. Para implementar una solución se establecieron los siguientes puntos:

1. Para evitar una posible suplantación de identidad, las llaves privadas están asociadas única y exclusivamente a un número de teléfono móvil. Por lo que, si un intento de acceso al sistema se realiza con una clave privada valida, desde un móvil diferente al asociado inicialmente, se denegara la solicitud.

2. Para realizar el envío de la clave privada a cada usuario, se implementará un método de cifrado adicional, por lo que, si alguna clave privada es interceptada durante el envío, no podría ser descifrada y por lo tanto seria invalida.

VIII. CONCLUSIONES

En la actualidad, el proceso de autenticación en entornos digitales, es uno de los factores fundamentales de la seguridad dentro de un sistema de información y constituye una herramienta para conservar la integridad, confidencialidad y veracidad de los datos allí almacenados, además de minimizar el riesgo de fraude y suplantación de identidad.

Existen diferentes métodos o técnicas de autenticación que se implementan actualmente en plataformas y servicios en la red. Estos se dividen en tres grandes grupos; a) aquellos basados en el conocimiento (usuario y contraseña), b) Por medio de la posesión de un elemento o clave única y C) a través de todo aquello inherente a la persona o datos biométricos.

Con respecto a los niveles de garantía que existen en los sistemas de autenticación, cabe resaltar que dependen de los requisitos y el nivel de confidencialidad de la información que se pretende resguardar, teniendo en cuenta el impacto que genere un acceso malintencionado, en la integridad de los datos y el sistema en sí.

Es recomendable la implementación de más de un factor de autenticación que asegure un nivel de confianza más alto en la identificación de entidades que intentan acceder a un sistema, además del uso de técnicas de cifrado de datos y envió seguro de información.

Las llaves asimétricas son una herramienta de cifrado, que representan un avance para el proceso de autenticación en entornos no controlados y son la base para la implementación de la firma digital en transacciones electrónicas.

VIII. REFERENCIAS

Andress, J. y Winterfeld, S. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, Elsevier, Second Edition, USA.

Burr, W., Dodson, D., Newton, E., Perlner, R., Polk, T., Gupta, S. y Nabbus, E. (2013). *Electronic Authentication Guideline*, Archived NIST Technical Series Publication Superseding Publication(s), USA.

Evidian. (2015). “Los 7 métodos de Autentificación más utilizados”. Evidian a Group Bull Company.

Franchi, M. R. (2012). “Algoritmos De Encriptación De Clave Asimétrica”. Universidad Nacional de la Plata.

Adhagale, G., y Vishnu, S. S. (2014). “A Comparative Study of Various Cryptographic Algorithm Used in Bouncy Castle Toolkit", International Journal of Emerging Technology and Advanced Engineering, **Vol. 4**, No. 11.

Gayoso, V., Hernandez, L. y Sanchez, C. (2010). “A survey of the elliptic curve integrated encryption scheme”, Journal Of Computer Science And Engineering, **Vol. 2**, No. 2.

Grassi, P. A., Garcia, M. E. y Fenton, J. L. (2017). *Digital identity guidelines*, National Institute of Standards and Technology, U.S Departament of Commerce, USA.

Maiorano, A. (2010). *Criptografía para desarrolladores*,Segu–Info. http://www.cuspide.com/detalle_libro.php/9872311382 (23 Enero 2020)

Marrero Travieso, Y. (2003). “La Criptografía como elemento de la seguridad informática”, ACIMED, **Vol. 11**, No. 6.

Martínez, V. G., Ávila, C. S., García, J. E. y Encinas, L. H. (2005). “Elliptic Curve Cryptography: Java implementation issues”, International Carnahan Conference on Security Technology.

Medina, T. y Miranda, A. (2015). *Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES*, Revista Mundo Fesc, **Vol. 9**.

OECD. (2007). OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication. www.oecd.org/sti/security-privacy

Paredes, G. (2006). "Introducción A La Criptografía", DGSCA-UNAM, **Vol. 7**, No. 7. http://www.revista.unam.mx/vol.7/num7/art55/int55.htm

Pareja, A., Pedak, M., Gómez, C. y Barros, A. (2017). *La gestion de la identidad y su impacto en la economia digital*, Banco Interamericano de Desarrollo. https://doi.org/10.18235/0000786

Pressman, R. S. (2010). *Ingenieria del Software - Un Enfoque Practico*, Editorial McGRAW-HILL, Septima Edicion, Mexico D. F.

Ristić, I. (2015). Bulletproof SSL And TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, Editorial Feisty Duck, United Kingdom.

Schwaber, K., y Sutherland, J. (2011). The Scrum Guide - The Definitive Guide to Scrum: The Rules of the Game, Srum Org, **Vol. 2.** https://doi.org/10.1053/j.jrn.2009.08.012

Unión Internacional de Telecomunicaciones. (2013). X.1254 : Marco de garantía de autenticación de entidad, UIT.

Vinkel, P., Madisse, U. y Maaten, E. (2014). "Voto por Internet en Estonia", Instituto de Investigaciones Juridicas, Universidad Nacional Autonoma de Mexico UNAM.

Anexo 5 Articulo Encuentro de Semilleros UDEC 2020

PLATAFORMA WEB DE INTEGRACIÓN PARA EL VOTO ELECTRÓNICO DE LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MODULO AUTENTICACIÓN

Cristian Camilo Pérez Bohórquez Autor 1[1]
Gina Maribel Valenzuela Sabogal Autor 2[2]

RESUMEN

El proyecto en curso pretende dar solución a la problemática que se genera debido a la ausencia de un sistema de información que permita la administración y gestión de las jornadas electorales que se llevan a cabo dentro de la Universidad de Cundinamarca, mediante el desarrollo de una plataforma institucional de voto por internet, en la cual, el proceso de autenticación constituye un factor fundamental, debido a la necesidad de asegurar de manera efectiva y confiable la identidad del individuo que accede para emitir un voto. Por tal razón se estableció el desarrollo de un módulo de autenticación multifactor, conformado por una aplicación móvil dedicada al almacenamiento de las credenciales del votante y el proceso de autenticación, además de la implementación de infraestructura de servicios web mediante la cual se establece la comunicación e integración con la plataforma de voto. Cabe mencionar que el módulo autenticación consta de un componente web propio para la administración y parametrización de las características del registro de votante, siendo totalmente independiente haciendo viable la posibilidad de integrarlo con proyectos que se desarrollen en un futuro.

ABSTRACT

The current project aims to solve the problem that is generated due to the absence of an information system that allows the administration and management of the electoral days that are carried out within the University of Cundinamarca, through the development of a platform institutional voting system over the internet, in which the authentication process is a fundamental factor, due to the need to effectively and reliably ensure the identity of the individual who accesses to cast a vote. For this reason, the development of a multifactor authentication module was established, consisting of a mobile application dedicated to storing the voter's credentials and the authentication process, in addition to the implementation of web services infrastructure through which communication and communication are established. integration with the voting platform. It is

[1] Estudiante Pregrado, Ingeniería de sistemas, Universidad de Cundinamarca, ccamiloperez@ucundinamarca.edu.co, ORCID # 0000-0002-3189-4524.
[2] Magister en Administración y Planificación Educativa, Docente Investigador, Universidad de Cundinamarca, gvalenzuela@ucundinamarca.edu.co, ORCID # 0000-0002-2833-1579.

worth mentioning that the authentication module consists of its own web component for the administration and parameterization of the characteristics of the voter registry, being totally independent, making it possible to integrate it with projects that are developed in the future.

Palabras claves: Autenticación, Clave asimétrica, Voto electrónico, Servicios Web.

Keywords: Authentication, Asymmetric password, Electronic voting, Web services.

INTRODUCCIÓN

"La identidad digital es la representación única de un sujeto involucrado en una transacción en línea" (Grassi, Garcia, & Fenton, 2017) y permite un control sobre el acceso a los recursos o la manipulación de datos almacenados en un sistema de información. Conforme al incremento en el uso de plataformas de e-learning, aplicaciones que vinculan las transacciones bancarias en línea y de gobierno electrónico, se ha vuelto indispensable corroborar la identidad de un usuario de manera precisa y confiable. Para ello se han establecido tres grupos de métodos de autenticación de usuarios; aquellos basados en el conocimiento, las características biométricas inherentes al usuario y por último la posesión de una clave u objeto único (Burr et al., 2013). A la combinación de dos o más de estos métodos se le conoce como autenticación multifactor, esta garantiza un nivel mayor de seguridad en operaciones de alto riesgo (Pareja, Pedak, Gómez, & Barros, 2017) como puede ser la ejecución de una jornada electoral a través de internet debido a que una de las dificultades presentes en la implementación de dicho sistema, es la correcta identificación y autenticación de los votantes, asimilando que "el proceso individual de votación por Internet no puede ser supervisado por las autoridades u observado de la manera tradicional" (Madise & Martens, 2006).Como ejemplo a seguir de la implementación exitosa de un modelo de votación a distancia y autenticación a través de medios digitales esta Estonia, un país reconocido mundialmente por ser pionero en materia de gobierno electrónico (e-Governement), debido a que fue el primer país en implementar el voto por internet a nivel nacional desde el 2005 y a los avances que ha presentado en este campo a través de los años. Uno de los factores que han influido en su éxito, es la implementación de la tarjeta nacional de identidad electrónica y una infraestructura de clave asimétrica (PKI), permitiendo a los estonios autenticarse en sitios web, realizar firmas legalmente vinculantes en los documentos y emitir su voto sin la necesidad de desplazarse a una mesa electoral, únicamente requiere de un lector de tarjetas y conexión a internet (Springall et al., 2014). "La experiencia de Estonia ha demostrado que el uso de la biometría no es necesario para crear un ecosistema seguro en un país con alfabetización digital avanzada" (Pareja et al., 2017). Ahora bien, teniendo en cuenta lo anteriormente mencionado se define la arquitectura de un módulo de autenticación basado en el conocimiento del usuario y la posesión de una llave privada almacenada mediante una aplicación móvil, permitiendo efectuar el proceso de autenticación por medio de un protocolo de desafío respuesta con el que se corrobora la identidad de cada votante, representando un avance hacia la modernización y agilización de los diferentes procesos electorales que se llevan a cabo en la institución, destacando la alternativa que se brinda a las personas de poder ejercer el

voto desde cualquier lugar que tenga una conexión a internet e incentivando la participación de la comunidad educativa en los temas relevantes en el marco de la gestión y el plan de desarrollo de la universidad, planteando las bases para lo que se denomina “gobierno electrónico” institucional.

DESARROLLO

La metodología de investigación propuesta es mixta, vinculando los enfoques cuantitativo y cualitativo, permitiendo abordar el problema desde distintos puntos de vista a partir del análisis e interpretación de los principios teóricos y pruebas experimentales mediante herramientas informáticas.

La fase de desarrollo del proyecto se realiza bajo la implementación de elementos de la metodología ágil SCRUM que se destaca por la flexibilidad, adaptación y organización de las tareas, para este caso establecidas conforme a las fases del ciclo de vida clásico o modelo en cascada, uno de los más antiguos y ampliamente usados en la ingeniería de software, dividido en las etapas de comunicación, planeación, modelado, desarrollo, despliegue y retroalimentación.

A partir del análisis del problema, el estudio de requerimientos y el modelado UML se define la estructura y funciones del módulo de autenticación como se describe a continuación:

1. Diseño y desarrollo de una aplicación móvil Android, para el almacenamiento de llave privada de cada usuario y realizar el proceso de autenticación.

2. Implementación de una arquitectura de servicios web tipo REST, para la comunicación e integración a la plataforma de voto por internet y la aplicación móvil como se muestra a continuación.

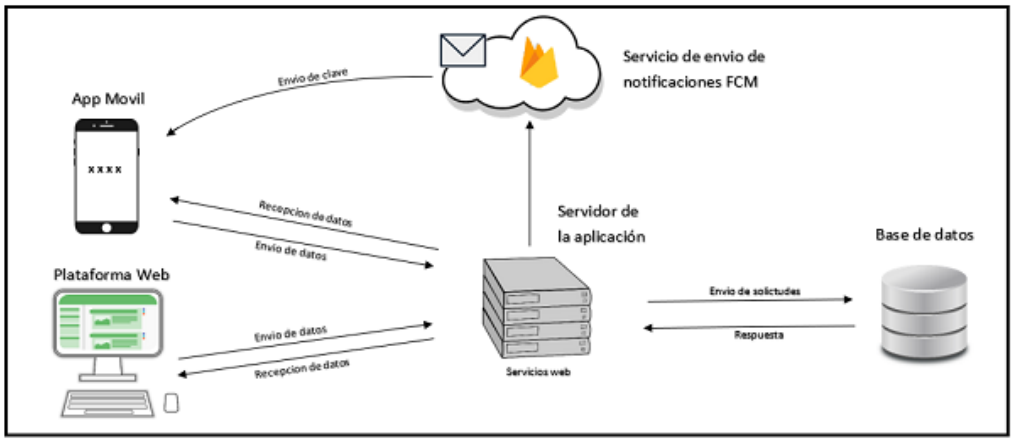


Fig. 1 Diagrama de la estructura del módulo de autenticación

3. Componente web para el rol administrador, que permita gestionar y parametrizar los datos de registro de usuarios del módulo de autenticación.

1. Implementación del cifrado de clave asimétrica para el proceso de autenticación, efectuando un protocolo de desafío respuesta en el que el usuario con la llave privada almacenada en su dispositivo móvil es capaz de descifrar y conocer el contenido de un mensaje cifrado el cual contiene una clave de acceso OTP.

2. Ruta del proceso de autenticación para confirmar la identidad de quien accede a emitir un voto a partir de dos factores, el conocimiento de una clave establecida por el usuario y la posesión de una llave única generada por el sistema.

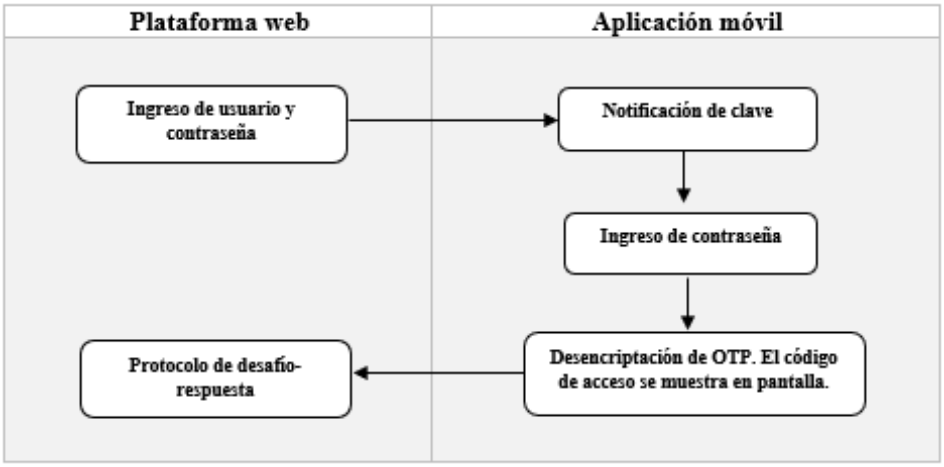


Figura 1 Proceso de autenticación del usuario

CONCLUSIONES

La incursión de la tecnología dentro de las jornadas electorales representa un reto, principalmente por las brechas digitales que existen actualmente, sumado a la desconfianza que genera en gran parte de la sociedad la vinculación de herramientas informáticas en los comicios, siendo la seguridad y la veracidad de los resultados dos de los aspectos más cuestionados, además del riesgo de fraude o acceso malintencionado para favorecer a un candidato durante unas elecciones.

El desarrollo del módulo de autenticación de manera independiente, mediante la implementación de la arquitectura de servicios web, permitió de manera más sencilla la integración y comunicación con la aplicación móvil y la plataforma web de voto por internet.

Los sistemas de información ofrecen diferentes alternativas innovadoras para la ejecución de tramites que se realizaban de forma tradicional, pero exige que de manera paulatina vayan migrando muchos de los procesos, no solo de gobierno institucional, sino también la modernización de la actividad administrativa de la universidad.

REFERENCIAS BIBLIOGRAFICAS

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines: revision 3. https://doi.org/10.6028/NIST.SP.800-63-37

Burr, William E, Dodson, Donna F, Newton, Elaine M, … Emad A. (2013). Archived NIST Technical Series Publication Superseding Publication(s) Electronic Authentication Guideline. 54. https://doi.org/10.6028/NIST.SP.800-63-2

Pareja, A., Pedak, M., Gómez, C., & Barros, A. (2017). La gestión de la identidad y su impacto en la economía digital. https://doi.org/10.18235/0000786

Madise, Ü., & Martens, T. (2006). E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. Electronic Voting 2006 - 2nd International Workshop, 15–26. Retrieved from http://www.id.ee/pages.php/030301

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security analysis of the estonian internet voting system. Proceedings of the ACM Conference on Computer and Communications Security, 703–715. https://doi.org/10.1145/2660267.2660315

Mohamed, M. A. (2014). A survey on elliptic curve cryptography. Applied Mathematical Sciences, 8(153–156), 7665–7691. https://doi.org/10.12988/ams.2014.49752

Anexo 6 Articulo CICI 2020

Desarrollo del Módulo de Autenticación Multifactor para Plataforma de Voto Electrónico de la Universidad de Cundinamarca

Cristian Camilo Pérez Bohórquez[1][0000-0002-3189-4524], Gina Maribel Valenzuela Sabogal [2][0000-0002-2833-1579] y Francisco Alfonso Lanza Rodríguez [3][0000-0003-0006-9430]

Universidad de Cundinamarca, Extensión Facatativá, Colombia
[1]ccamiloperez@ucundinamarca.edu.co
[2]gvalenzuela@ucundinamarca.edu.co
[3]flanza@ucundinamarca.edu.co

Resumen. El proyecto en curso pretende dar solución a la problemática que se genera debido a la ausencia de un sistema de información que permita la administración y gestión de las jornadas electorales que se llevan a cabo dentro de la Universidad de Cundinamarca, mediante el desarrollo de una plataforma institucional de voto por internet, en la cual, el proceso de autenticación constituye un factor fundamental, debido a la necesidad de asegurar de manera efectiva y confiable la identidad del individuo que accede para emitir un voto, con el fin de salvaguardar los principios de integridad, confidencialidad y universalidad. Se espera entonces que la mediación de la tecnología en las jornadas electorales que se lleven a cabo dentro de la institución proporcione no solo una mayor celeridad en el reporte de resultados sino exactitud en el conteo al garantizar que los votos contabilizados responden a la voluntad de los votantes, permitiendo la modernización de la actividad electoral y el establecimiento de una identidad digital verificable y de confianza, sentando las bases para la instauración de un entorno denominado gobierno electrónico.

Palabras clave: Autenticación, Criptografía, Clave Asimétrica.

1 Introducción

"La identidad digital es la representación única de un sujeto involucrado en una transacción en línea"[1] y permite mantener un control sobre el acceso a los recursos o la manipulación de datos almacenados en un sistema de información, por lo que hasta la actualidad, se han adelantado investigaciones en el área de la seguridad informática y el proceso de autenticación a través de medios digitales, conforme al crecimiento en el uso plataformas de aprendizaje en línea, aplicaciones que vinculan transacciones bancarias y de gobierno electrónico, en las que es indispensable corroborar la identidad de un usuario de manera precisa y confiable, estableciendo tres grupos diferentes de

grupos diferentes de métodos de autenticación de usuarios; aquellos basados en el conocimiento, las características biométricas inherentes al usuario y por último la posesión de una clave u objeto único [2]. A la combinación de dos o más de estos métodos se le conoce como autenticación multifactor, esta garantiza un nivel mayor de seguridad en operaciones de alto riesgo [3] como puede ser la ejecución de una jornada electoral a través de internet, siendo una de sus principales ventajas que cada ciudadano puede emitir su voto a través de medios electrónicos "aun cuando este se encuentre distante de su lugar de residencia"[4]. Como ejemplo a seguir de la implementación exitosa de un modelo de votación a distancia y autenticación a través de medios digitales esta Estonia, un país reconocido mundialmente por ser precursor en materia de gobierno electrónico (e-Governement). A partir del uso de lectores de tarjetas y una infraestructura de clave asimétrica (PKI) los estonios pueden autenticarse en sitios web, realizar firmas legalmente vinculantes en los documentos y votar sin dirigirse a una sede electoral "demostrando que el uso de la biometría no es necesario para crear un ecosistema seguro en un país con alfabetización digital avanzada"[3].

1 Metodología

El proyecto se realiza bajo la implementación de elementos de la metodología ágil SCRUM que proporciona un marco de trabajo adaptable en el cual se puede emplear diversos procesos y técnicas [5] destacándose por la flexibilidad, adaptación, organización de las tareas de desarrollo del software.

Las fases del desarrollo del software están establecidas bajo el ciclo de vida clásico o modelo en cascada, uno de los más antiguos y ampliamente usados en la ingeniería de software, dividido en las etapas de comunicación, planeación, modelado, desarrollo, despliegue y retroalimentación.

También se vincula el uso de técnicas criptográficas tienen como propósito prevenir algunas faltas de seguridad, a partir de la combinación del cifrado simétrico y asimétrico. En el uso de la criptografía simétrica, la misma clave se usa tanto para el cifrado como para el descifrado, mientras en la criptografía asimétrica se realiza la operación a partir de dos claves diferentes, una es para cifrado y la otra se usa para descifrar. Es así como se garantiza la integridad y autenticidad de las llaves, además de ser el principio por el cual se realiza el proceso de autenticación a partir del protocolo de desafío-respuesta.

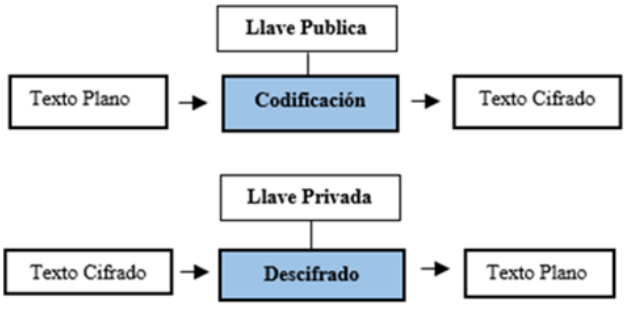


Fig. 1. Proceso de clave para criptografía asimétrica [6]

Ahora bien, para la generación del par de llaves relacionadas matemáticamente por una función, se opta por la criptografía de curva elíptica (ECC), fundamentada en la estructura matemática de las curvas elípticas sobre un campo finito. Este, requiere longitudes de clave más cortas para garantizar el mismo nivel de seguridad como se muestra en la siguiente tabla con información tomada del artículo "A Survey of the Elliptic Curve Integrated Encryption Scheme" [7] en la que se evidencia que por ejemplo una clave ECC de 160 bits, es equivalente a una clave RSA de 1024 bits.

Tabla 1. Longitud de claves ECC y RSA

Criptografía de curvas elípticas ECC (bits)	RSA (bits)
160	1024
224	2048
256	3072
384	7680
512	15360

1 Resultados

Se establece el diseño de un módulo de autenticación multifactor basado en arquitectura de servicios web que facilite su integración, conformado por un componente dedicado a la plataforma web y otro a la aplicación móvil, como se muestra en la siguiente figura.

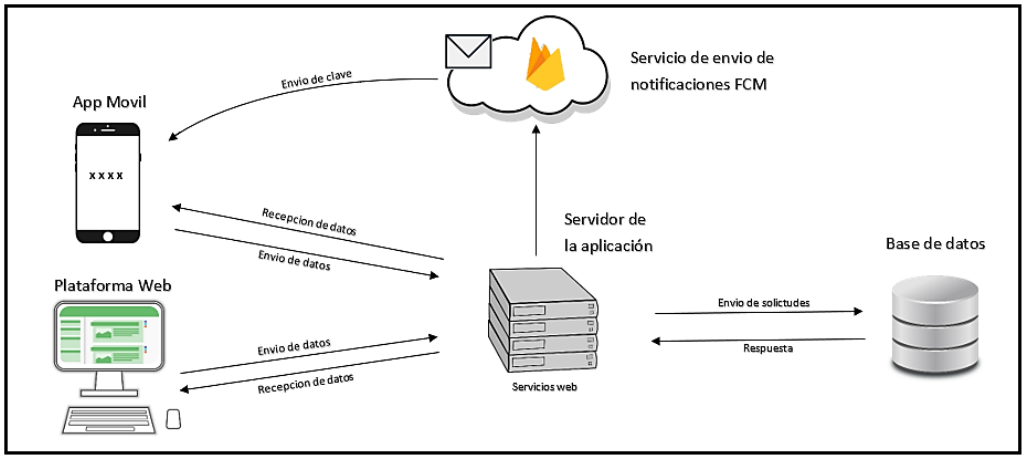


Fig. 2. Estructura módulo de autenticación

Además del registro de las personas habilitadas para emitir un voto, refiriéndose única y exclusivamente a personas pertenecientes a la Universidad de Cundinamarca, realizando una validación a través del correo institucional, obteniendo así las credenciales para el acceso a la plataforma de voto electrónico.

El proceso de autenticación para confirmar la identidad de quien accede a emitir un voto, mediante técnicas basadas en conocimiento del votante y la posesión de la llave almacenada en su dispositivo móvil como se ilustra en la siguiente figura.

Fig. 3.

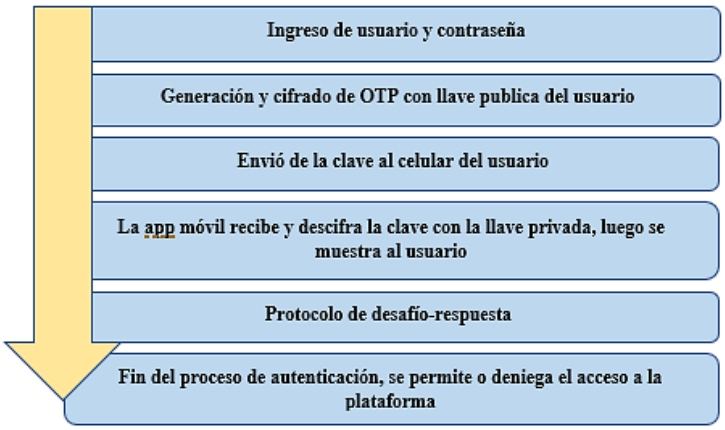


Diagrama del proceso de autenticación establecido.

1 Conclusiones

El voto constituye un instrumento indispensable en el contexto de una democracia, debido a que este influye en la toma de decisiones y se ve reflejado en poder político, por lo que garantizar la transparencia, integridad y veracidad de los resultados del proceso electoral supone un reto para la implementación de la tecnología, principalmente por las brechas digitales que existen actualmente, sumado a la desconfianza que se genera en gran parte de la sociedad la vinculación de herramientas informáticas en los comicios.

Actualmente, el proceso de autenticación en entornos digitales es uno de los factores fundamentales de la seguridad dentro de un sistema de información y constituye una herramienta para conservar la integridad, confidencialidad y veracidad de los datos allí almacenados.

Existen diferentes métodos o técnicas de autenticación que se implementan actualmente en plataformas y servicios en la red, en primer lugar, aquellos basados en el conocimiento, en segundo lugar, por medio de la posesión de un elemento o clave única y por último aquello inherente a la persona o datos biométricos, siendo este el más fiel a la hora de validar la identidad de un individuo.

Referencias

1. P. A. Grassi, M. E. Garcia, and J. L. Fenton, “Digital identity guidelines: revision 3,” 2017.
2. Burr *et al.*, “Archived NIST Technical Series Publication Superseding Publication(s) Electronic Authentication Guideline,” p. 54, 2013.
3. A. Pareja, M. Pedak, C. Gómez, and A. Barros, “La gestión de la identidad y su impacto en la economía digital,” 2017.
4. P. Pesado *et al.*, “E-Government: El voto electrónico sobre Internet,” in *XIV Congreso Argentino de Ciencias de la Computación*, 2008, p. 11.
5. K. Schwaber and J. Sutherland, “The Scrum Guide - The Definitive Guide to Scrum: The Rules of the Game,” *Scrum. org, October*, vol. 2, no. October. p. 17, 2011.
6. T. Medina and A. Miranda, “Comparison of Algorithms Based Cryptography Symmetric DES, AES and 3DES,” *Rev. Mundo Fesc*, vol. 9, pp. 14–21, 2015.
7. V. Gayoso, L. Hernandez, and C. Sanchez, “A survey of the elliptic curve integrated encryption scheme,” *J. Comput. Sci. Eng.*, vol. 2, no. 2, pp. 7–13, 2010.

Anexo 7 Certificado Ponencia CIETA

La República de Colombia, y en su nombre

UNIVERSIDAD DE **PAMPLONA**

FACULTAD DE INGENIERÍAS Y ARQUITECTURA

CERTIFICA QUE

CRISTIAN CAMILO PEREZ BOHORQUEZ

CC. 1070926072

PONENTE

XIV CONGRESO INTERNACIONAL DE INGENIERÍA ELECTRÓNICA Y TECNOLOGÍAS AVANZADAS. X CONGRESO INTERNACIONAL EN SISTEMAS, INFORMÁTICA E INGENIERÍA DEL CONOCIMIENTO . X CONGRESO EN TELECOMUNICACIONES. IX CONGRESO EN INGENIERÍA ELÉCTRICA. V CONGRESO INTERNACIONAL DE INGENIERÍA MECATRÓNICA. II CONGRESO INTERNACIONAL DE INGENIERIA INDUSTRIAL

Realizado los días 28,29 y 30 de octubre de 2020

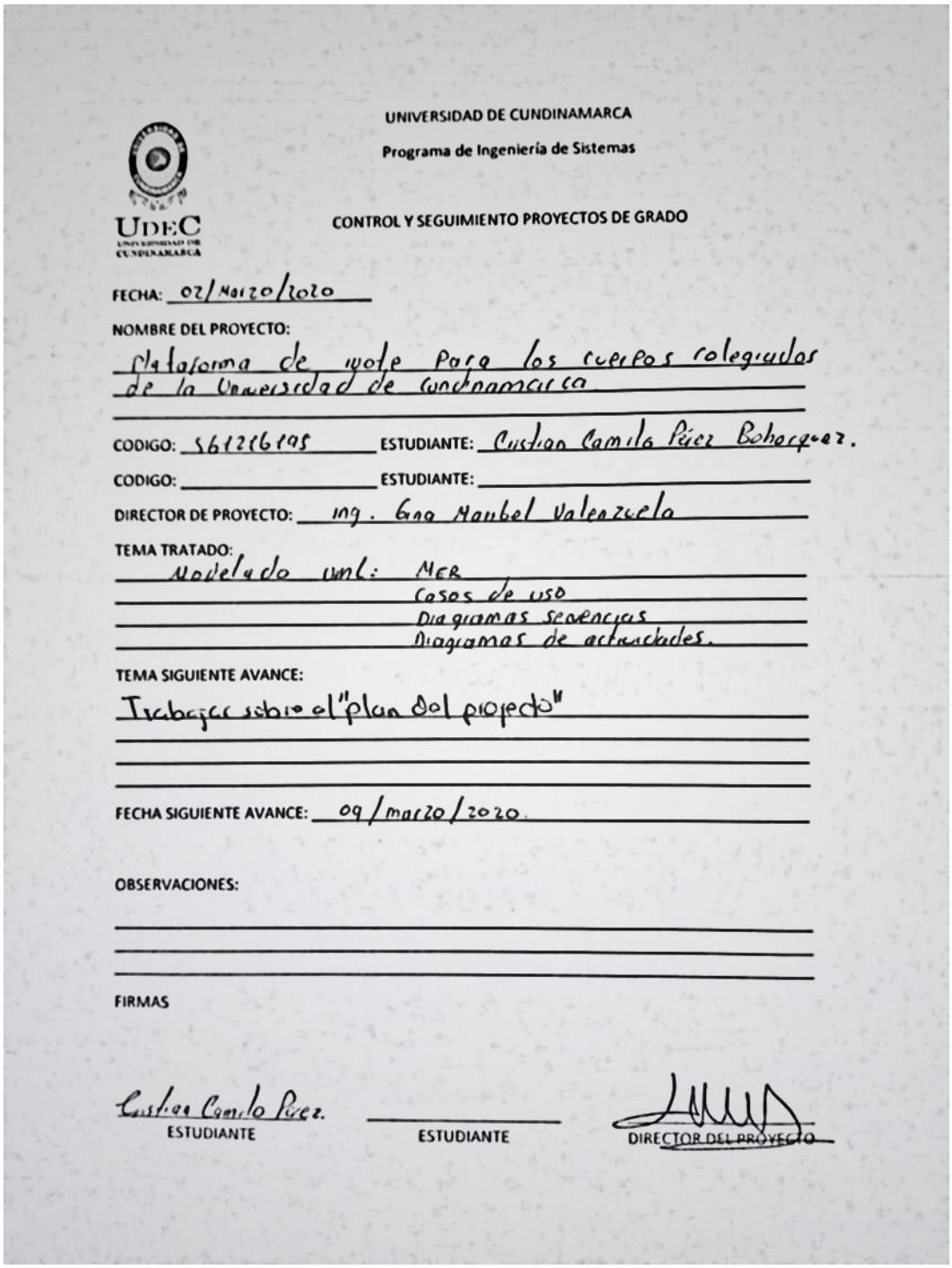
Con una intensidad de 24 horas

JORGE LUIS DÍAZ RODRÍGUEZ
Decano Facultad de Ingenierías y Arquitectura

ALDO PARDO GARCÍA
Coordinador

55003

Anexo 8 Formatos de Seguimiento



UNIVERSIDAD DE CUNDINAMARCA

Programa de Ingeniería de Sistemas

UDEC

CONTROL Y SEGUIMIENTO PROYECTOS DE GRADO

FECHA: 02/Marzo/2020

NOMBRE DEL PROYECTO:
Plataforma de voto para los cuerpos colegiados de la Universidad de Cundinamarca

CODIGO: 561216195 ESTUDIANTE: Cristian Camilo Páez Bohorquez.

CODIGO: ESTUDIANTE:

DIRECTOR DE PROYECTO: Ing. Gna Maribel Valenzuela

TEMA TRATADO:
Modelado uml: MER
Casos de uso
Diagramas secuencias
Diagramas de actividades.

TEMA SIGUIENTE AVANCE:
Trabajar sobre el "plan del proyecto"

FECHA SIGUIENTE AVANCE: 09/marzo/2020.

OBSERVACIONES:

FIRMAS

Cristian Camilo Páez. ESTUDIANTE

ESTUDIANTE

DIRECTOR DEL PROYECTO

UNIVERSIDAD DE CUNDINAMARCA

Programa de Ingeniería de Sistemas

UDEC
UNIVERSIDAD DE CUNDINAMARCA

CONTROL Y SEGUIMIENTO PROYECTOS DE GRADO

FECHA: 24 / Febrero / 2020

NOMBRE DEL PROYECTO:

Plataforma de Voto Para los cuerpos colegiados de la universidad de Cundinamarca.

CODIGO: 561216195 ESTUDIANTE: Cristian Camilo Pérez Bohorquez

CODIGO: _____ ESTUDIANTE: _____

DIRECTOR DE PROYECTO: Ing. Gina Maribel Valenzuela

TEMA TRATADO:

Articulo de investigación para congreso CIETA

TEMA SIGUIENTE AVANCE:

Modelado : MER
casos de uso
diagramas secuencia
diagramas actividades.

FECHA SIGUIENTE AVANCE: 02 / Marzo / 2020

OBSERVACIONES:

Se amplia el plazo de envio de articulo para CIETA

FIRMAS

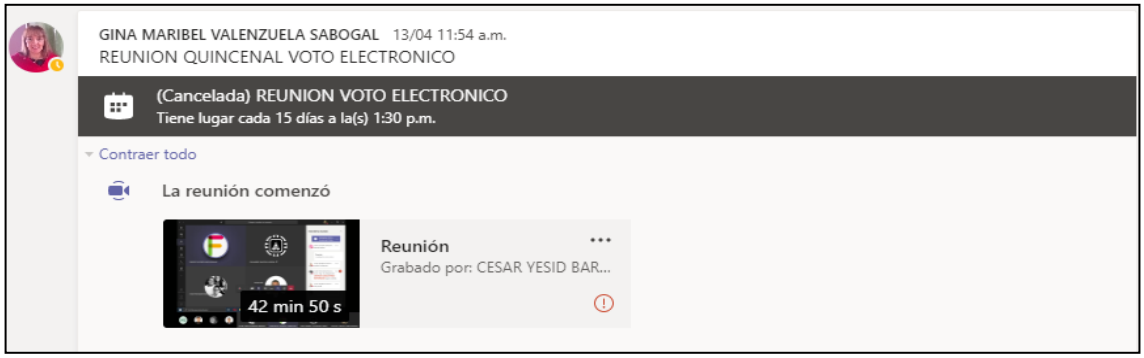
Cristian Camilo Perez
ESTUDIANTE

_____
ESTUDIANTE

DIRECTOR DEL PROYECTO

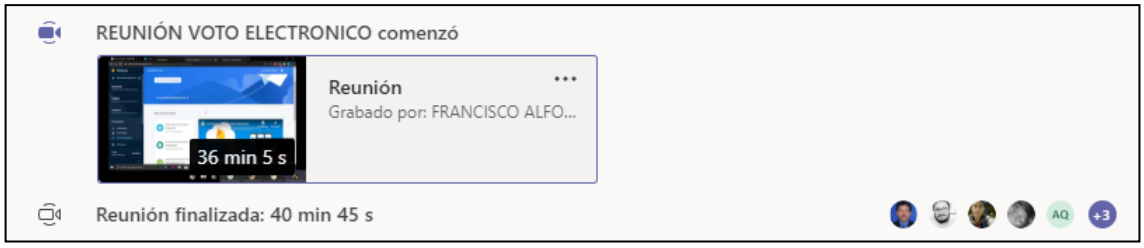
Los seguimientos se realizaron de manera virtual mediante la plataforma Teams.

Seguimiento Microsoft Teams 13 mayo de 2020



Seguimiento Microsoft Teams 08 junio de 2020

Seguimiento Microsoft Teams 17 junio de 2020

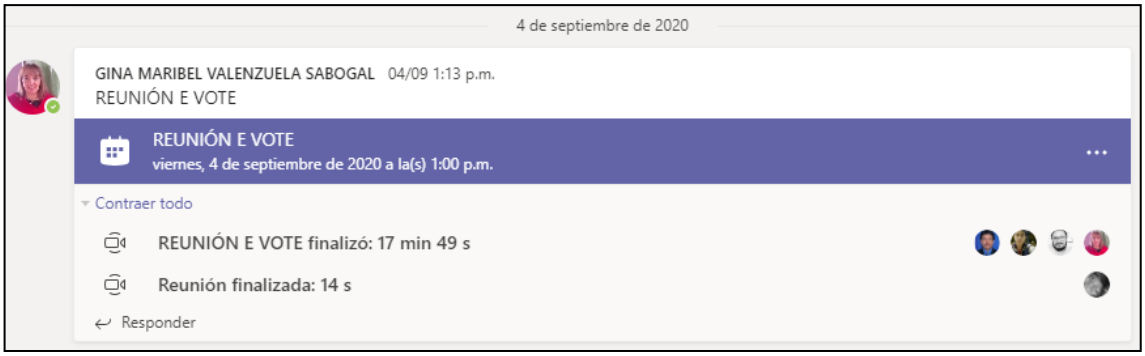


Seguimiento Microsoft Teams 15 julio de 2020

Seguimiento Microsoft Teams 29 julio de 2020

Seguimiento Microsoft Teams 12 agosto de 2020

Seguimiento Microsoft Teams 04 septiembre de 2020



Seguimiento Microsoft Teams 16 octubre de 2020

Seguimiento Microsoft Teams 23 octubre de 2020

Seguimiento Microsoft Teams 30 octubre de 2020