

# Propuesta de sistema de voto electrónico, utilizando esquemas de compartición de secretos.

## **Trabajo terminal No. 2021-A002**

*Alumnos: \*Jacinto Sánchez Alondra Jacqueline, Malvaez Landeros Kevin Uriel, Pérez Barajas Héctor Mauricio.*

*Directores: Gutiérrez Mejía Darwin, Vázquez González Leonor*

*\*email: [ajacintos1400@alumno.ipn.mx](mailto:ajacintos1400@alumno.ipn.mx)*

**Resumen:** Se desarrollará un sistema web para la realización de votaciones electrónicas en el proceso de elección de alumnos consejeros dentro de la ESCOM, automatizando así dicho proceso, tanto a votantes como a la mesa electoral, además de hacerlo más seguro y confiable. Para el desarrollo de las elecciones se hará uso de diversas herramientas criptográficas principalmente los esquemas de compartición de secretos (ECS).

**Palabras clave:** Criptografía, Compartición de secretos, Voto electrónico.

## **1.Introducción**

Dentro de la Escuela Superior de Cómputo (ESCOM), no se cuenta con un sistema propio para realizar votaciones, tomando en cuenta que cada año se realizan diversos tipos de votaciones dentro de la escuela, como elecciones a alumnos consejeros y consultas sobre prestatarios de servicios (cafetería, barra de café, papelería), el desarrollo de un sistema de voto electrónico facilitaría estos procesos de elecciones que usualmente llegan a ser tediosos y pesados para todos los involucrados en el desarrollo de estos.

Dentro de los procesos de votación electrónicos se debe de garantizar ciertas condiciones para validar estas mismas. Al igual que los procesos tradicionales, estas condiciones son: Democracia, transparencia, privacidad, entre otros [1]. En los procesos tradicionales son garantizados mediante transparencia en las urnas y escrutinio público en el conteo de los votos. Sin embargo, en un proceso electrónico se debe de utilizar protocolos criptográficos para poder garantizar que las elecciones sean confiables [2].

La criptografía es la ciencia que se encarga de estudiar distintas técnicas para cifrar información, de esta forma es posible de convertir un texto plano, a un texto cifrado que sea ilegible para cualquier persona que no sea el legítimo destinatario, el cual conocerá el proceso inverso para poder recuperar el texto plano. Haciendo uso de estas técnicas se garantiza la confidencialidad, integridad y autenticidad de la información enviada a través de un canal inseguro, como puede ser el internet.[3] Un protocolo es un proceso coordinado, donde dos o más partes hacen un intercambio de información. Por su parte, un protocolo criptográfico utiliza métodos y algoritmos criptográficos para cumplir esta función. Dentro de estos protocolos se encuentran los esquemas de compartición de secretos [4]. Haciendo uso de estos protocolos se da solución a distintos problemas de la vida real, por eso son especialmente usados en aquellos escenarios donde pueda existir desconfianza entre las partes involucradas en este proceso [5]. Un claro ejemplo de estos escenarios es una votación, ya que en ellas se involucran intereses políticos, económicos y sociales que pueden influir en los resultados de estas, además de que los votantes deberán de tener la certeza de que su voto contribuyo al resultado final, sin sufrir ningún tipo de alteración [6].

Un esquema de compartición de secretos (ECS) controla el acceso a la información distribuyendo la responsabilidad del acceso a esta, entre varios usuarios. El ECS divide la información en fragmentos que por sí solos son inteligibles, cada usuario recibe uno de estos fragmentos a los cuales se les conoce como secretos. De tal forma que una transacción sobre esta información solo pueda ser procesada si un conjunto de usuarios, establecido en el esquema, dan su autorización, es decir brindan su secreto, para la transacción. Bajo este esquema, si el conjunto de usuarios no está completo, aun si solo falta un usuario, es imposible acceder a la información inicial. [7 8].

Haciendo uso combinado de estas herramientas, se puede establecer un sistema de voto electrónico en la ESCOM, donde al momento de que los alumnos generen el voto, se aplique un esquema de compartición de secretos, así el voto se divide en fragmentos de tal forma que solo las personas autorizadas en el proceso electoral, en este caso los actuales alumnos consejeros, puedan recuperar el voto, dando sus secretos para contabilizarse en los resultados finales.

Adicionalmente se garantizará un único voto por persona y verificará que solo los votantes autorizados introduzcan su voto, con total privacidad.

Existen algunos sistemas de votación electrónica, a continuación, se enlistan algunos de ellos

Software	Descripción	Características
Vote-Debian	Sistema basado en el uso de correo electrónico. Está orientado a decidir el funcionamiento interno del grupo de desarrolladores de Debian.	No se garantiza el secreto del voto. De hecho, el contenido y resultado de las votaciones es público La autenticación del votante se realiza vía “Pretty Good Privacy”. Existe un registro previo de usuarios
Sistema de Voto Electrónico por Internet (INE)	Sistema web en desarrollo, por parte del Instituto nacional electoral, se espera realizar las primeras votaciones en este durante las votaciones del 2021[9]	Sistema en la nube Garantiza la secrecía del voto Cuenta con una bitácora inmutable
Sistema institucional de voto (IPN)	Sistema web del IPN desarrollado para realizar votaciones académicas	Garantiza la secrecía del voto Hace uso del CURP y número de empleado, o boleta para generar el token de votación. El sistema genera un token único a cada usuario, es responsabilidad del usuario salvaguardar dicho token. El token es el elemento que da acceso al usuario para emitir su voto
Sistema de votación electrónica con autenticación biométrica para ESCOM	Sistema de votación capaz de crear una elección en la ESCOM.	Sistema de escritorio. Utilizar lector de huella digital para reconocer a los votantes. Utiliza AES, RSA y SHA1, para garantizar la autenticidad de los votos

*Tabla 1: Estado del arte de los sistemas de voto digital*

## 2.Objetivo

Diseñar e implementar un sistema web básico para automatizar los procesos electorales internos de elección de alumnos consejeros en la Escuela Superior de Cómputo, haciendo uso de un esquema de compartición de secretos para fragmentar la información del voto, así como algoritmos de cifrados modernos para realizar la autenticación de estos.

Objetivos particulares:

- Investigar, evaluar y elegir el esquema de compartición de secretos.
- Identificar e implementar algoritmos de cifrado moderno adecuados para la autenticación de los votos.
- Crear el sitio web donde se montará el sistema.
- Realizar una prueba de votación.

## 3. Justificación

Al no contar con un sistema propio para la realización de las votaciones electrónicas en la ESCOM, estas se realizan en urnas presenciales o a través del sistema institucional de votación electrónica (SIVE) del IPN, de ahí que la importancia de implementación de un sistema para realizar las votaciones de manera electrónica, que sea propio de la ESCOM. Especialmente en los tiempos actuales, donde no se puede realizar las votaciones de manera presencial en urnas.

La presente propuesta de proyecto nace de estas necesidades, ya que, si bien actualmente existen algunos sistemas, incluso en la propia escuela y el mencionado SIVE, no existe un sistema web que sea propio y brinde libertades y autonomía a los alumnos consejeros de la ESCOM para realizar los procesos electorales. A demás en esta propuesta utilizara esquemas de compartición de secretos para la distribución de los votos entre los alumnos consejeros actuales, haciendo así que las votaciones sean más seguras ya que para obtener los votos se requeriría de un numero definido de estos alumnos.

De igual manera el proyecto representa beneficios para los alumnos de la ESCOM, ya que si son votantes no deberán de desplazarse a otro lugar para poder ejercer su voto, podrán realizarlo desde una página web, desde cualquier computadora con internet. Para los alumnos consejeros, el sistema les ayudara a realizar el conteo, y la obtención de los votos, optimizando así los tiempos y recursos en la realización de las votaciones.

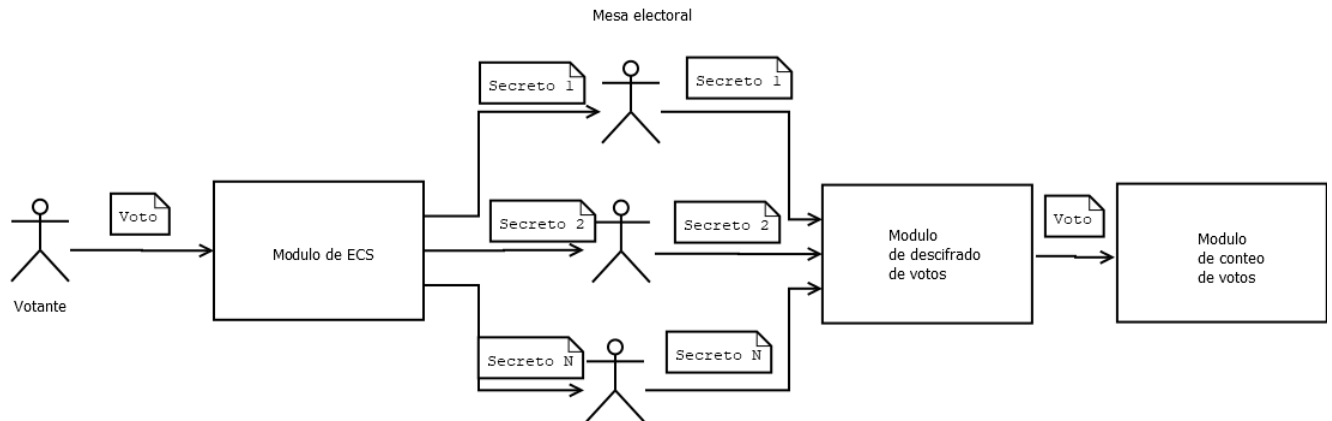
Para el desarrollo del sistema web haremos uso de diferentes tecnologías actuales y que son utilizadas en el mundo laboral, tecnologías como lo son React.js para la realización de las interfaces graficas del sistema, Node.js para realizar las operaciones del lado del servidor, y MySQL para el manejo de la base de datos del sistema.

El desarrollo de este proyecto implica tener conocimientos en seguridad informática, criptografía, probabilidad y algebra modular, esto para la creación de los algoritmos y protocolos criptográficos con los cuales garantizaremos la validez de las elecciones; De la misma forma se requieren conocimientos de desarrollo de sistemas y aplicaciones web, para generar el sitio donde se llevará a cabo el proceso. Por ello que generar la propuesta del sistema representa una complejidad que se espera para un trabajo terminal, en el cual invertiríamos aproximadamente 450 horas en el desarrollo, a lo largo de Trabajo terminal 1 y trabajo terminal 2.

#### **4. Productos o Resultados esperados**

Como resultado tendremos un sistema que, al recibir un voto, este será cifrado utilizando un esquema de compartición de secretos, de esta forma se distribuirá una parte del secreto por cada miembro de la mesa electoral, en este caso los alumnos consejeros, asegurando que cualquier persona no autorizada que recupere esos datos los encuentre cifrados e incompletos; para recuperar el voto se necesitara que las  $n$  personas autorizadas estén reunidas e introduzcan sus claves, así se recuperará el voto y se contabilizará automáticamente sin revelar la información del votante. De la misma forma se podrán utilizar algunos otros algoritmos de cifrado moderno, para garantizar la autenticidad de los votos.

1. Sistema web la cual permitirá que cada alumno que participe en el proceso de votación realice solo un voto, el cual será fragmentado para que únicamente los integrantes de la mesa electoral puedan recuperar el voto sin revelar la información del votante a estos mismos y de esta manera poder contabilizarlo.
2. Manual de usuario de la herramienta que describirá el funcionamiento completo del sistema para iniciar el proceso de votación y la finalización de este.
3. Código del sistema web para posibles actualizaciones y mantenimiento.
4. Reporte técnico del sistema.
5. Publicación de resultados de una prueba en un proceso de votación simulado del sistema.



*Imagen 1: Diagrama de bloques del sistema*

## 5. Metodología

La metodología a utilizar será Extreme Programming (XP), esta metodología puede ayudarnos a la conclusión satisfactoria del proyecto, esto debido a sus valores, principalmente el de comunicación, ya que con las condiciones actuales esta se puede volver un poco complicada y estar en constante contacto con el equipo ayudará a saber sobre el estado y las necesidades del proyecto. De la misma forma la capacidad de XP para adaptarse a los cambios de los requerimientos nos podrá servir, ya que, si bien no se prevén cambios significativos en la funcionalidad del proyecto, si pudiera tener cambios en la forma de utilización, como podría ser instalar centros de voto electrónico dentro de la escuela para efectuar las votaciones allí una vez que las condiciones sanitarias lo permitan. De la misma forma utilizar una metodología ágil nos ayudara a ajustarnos en los tiempos enfocándonos más sobre el software funcional y generando solo la documentación necesaria. Esta ventaja de tiempo viene sobre todo dada por el tiempo de desarrollo de un año a lo largo de TT1 y TT2. Las fases de XP son.

1. Planificación
2. Análisis
3. Desarrollo
4. Pruebas

Haciendo durante TT1 principalmente actividades de Planificación y Análisis y durante TT2 de Desarrollo y pruebas. Sin embargo, gracias a la flexibilidad de XP, los cronogramas podrían modificarse y realizar actividades que no estuvieran presupuestadas en los tiempos marcados al inicio del proyecto, esto claro tomando en cuenta siempre el desarrollo del proyecto y procurando la conclusión satisfactoria de este.

## 6. Cronograma

CRONOGRAMA Nombre de la alumna: Jacinto Sánchez Alondra Jacqueline

[illegible]

[illegible]

CRONOGRAMA Nombre del alumno: Pérez Barajas Héctor Mauricio

[illegible]

[illegible]





[illegible]

## 7. Referencias

- [1] E. Abu-shana, M. knight y H. Refai. "E-voting systems: a tool for e-democracy", *Management research and practice*, vol. 2, no. 3, pp. 264-274, septiembre 2010
- [2] D. Cabarcas. "Electronic voting and related cryptographic challenges", Revista *Facultad de Ciencias Universidad Nacional de Colombia*, vol. 4, no 2, pp. 83-102, diciembre 2015.
- [3] A. Gómez. *Enciclopedia de la seguridad informática*, 2nd ed, Ciudad de México: Alfaomega, 2014.
- [4] Corletti Estrada, A. *Ciberseguridad (una estrategia informática/militar)*. Madrid: Darfe, 2017
- [5] J. Aguirre. *Libro electrónico de seguridad informática y criptografía*, 6ta ed, España: universidad politécnica de Madrid.2006
- [6] S. Staak y P. Wolf, *Cybersecurity in Elections*, Strömsborg: International IDEA, 2019.
- [7] L. Vázquez Gonzales. "Métodos Computacionales para Esquemas de Compartición de Secretos ideales," Tesis de maestría, Departamento de ingeniería, sección computación, CINVESTAV, Ciudad de México, 2004
- [8] Y. Liu. y Q. Zhao (2017 enero). "E-Voting Scheme Using Secret Sharing and K-Anonymity". Available: [https://www.researchgate.net/publication/309369790\\_E-Voting\\_Scheme\\_Using\\_Secret\\_Sharing\\_and\\_K-Anonymity](https://www.researchgate.net/publication/309369790_E-Voting_Scheme_Using_Secret_Sharing_and_K-Anonymity)
- [9] INE. (2020 agosto 26). Implementará INE voto electrónico por internet para las y los mexicanos residentes en el exterior en elecciones 2021. Available <https://centralector.ine.mx/2020/08/26/implementara-ine-voto-electronico-internet-las-los-mexicanos-residentes-exterior-elecciones-2021/>

## 8. Alumnos y directores.

Héctor Mauricio Pérez Barajas. - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta:2015021002, Tel. 5532996639, email [hperezbl400@alumno.ipn.mx](mailto:hperezbl400@alumno.ipn.mx)



Firma: \_\_\_\_\_

Alondra Jacqueline Jacinto Sánchez. - Alumna de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta:2015090348, Tel. 5527584198, email [ajacintos1400@alumno.ipn.mx](mailto:ajacintos1400@alumno.ipn.mx)

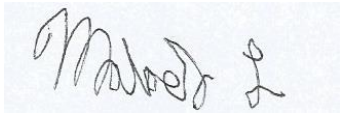


Firma: \_\_\_\_\_

Kevin Uriel Malvaez Landeros. Kevin Uriel. - Alumno de la carrera de Ing. en Sistemas

CARÁCTER: Confidencial  
FUNDAMENTO LEGAL: Artículo 11 Fracc. V y Artículos 108, 113 y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.  
PARTES CONFIDENCIALES: Número de boleta y teléfono.

Computacionales en ESCOM, Especialidad  
Sistemas, Boleta:2015020781, Tel. 5585833853,  
email [kmalvaez11400@alumno.ipn.mx](mailto:kmalvaez11400@alumno.ipn.mx)



Firma: \_\_\_\_\_

Darwin Gutiérrez Mejía. - Profesor Titular de la  
Escuela Superior de Cómputo del IPN, Estudios  
de posgrado en la Universidad Autónoma de  
Barcelona y doctorado en la Escuela Superior de  
Física y Matemáticas del IPN. Interesado en las  
aplicaciones de las matemáticas en diversos  
ámbitos del cómputo. Tel. 5513328307, Correo  
electrónico: [dargut@hotmail.com](mailto:dargut@hotmail.com)



Firma: \_\_\_\_\_

Leonor Vázquez González. - Profesora de  
Asignatura de la Escuela Superior de Física y  
Matemáticas. Maestría en Ciencias en la  
especialidad de Computación del CINVESTAV y  
Doctorado en Matemática Aplicada a la  
criptografía por la Universidad Politécnica de  
Cataluña, España. Experiencia como líder de  
desarrollo en aplicaciones y soluciones para la  
industria petrolera. Su interés se centra en el  
análisis y desarrollo de algoritmos, optimización  
y criptografía. Tel. 551915390 Correo  
electrónico: [leobaki@hotmail.com](mailto:leobaki@hotmail.com)



Firma: \_\_\_\_\_



Alondra Jacqueline Jacinto Sanchez

Jue 12/08/2021 15:17



Para: Darwin Gutierrez <dargut@hotmail.com>; leobaki@hotmail.com

CC: Hector Mauricio Perez Barajas; Kevin Uriel Malvaez Landeros



ProtocoloTT.pdf

397 KB



Buen día profesores,

Anexo el protocolo reestructurado final que será mandado a la CATT, solicitamos atentamente nos envíen el acuse de recibido.

Gracias.



Leonor Vázquez <leobaki@hotmail.com>

Jue 12/08/2021 15:21



Para: Darwin Gutierrez <dargut@hotmail.com>; Alondra Jacqueline Jacinto Sanchez

CC: Hector Mauricio Perez Barajas; Kevin Uriel Malvaez Landeros

Recibido, gracias.

Saludos cordiales,

Dra. Leonor Vázquez González  
Docente ESCOM IPN



Darwin Gutierrez <dargut@hotmail.com>

Vie 13/08/2021 11:49



Para: Hector Mauricio Perez Barajas; Alondra Jacqueline Jacinto Sanchez y 1 usuarios más

CC: Kevin Uriel Malvaez Landeros

Confirmando de recibido y acepto los cambios.  
Saludos

Enviado desde mi Huawei de Telcel.



Hector Mauricio Perez Barajas

Vie 13/08/2021 16:45



Para: Alondra Jacqueline Jacinto Sanchez

Recibido, de acuerdo con el documento. Saludos



Kevin Uriel Malvaez Landeros

Vie 13/08/2021 16:53



Para: Alondra Jacqueline Jacinto Sanchez

Recibido, gracias