

UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE INGENIERÍA
ANÁLISIS Y DISEÑO II
SECCIÓN 01 VESPERTINA
DRA. HILDA RUTH FLORES MUÑOZ

PROYECTO FINAL

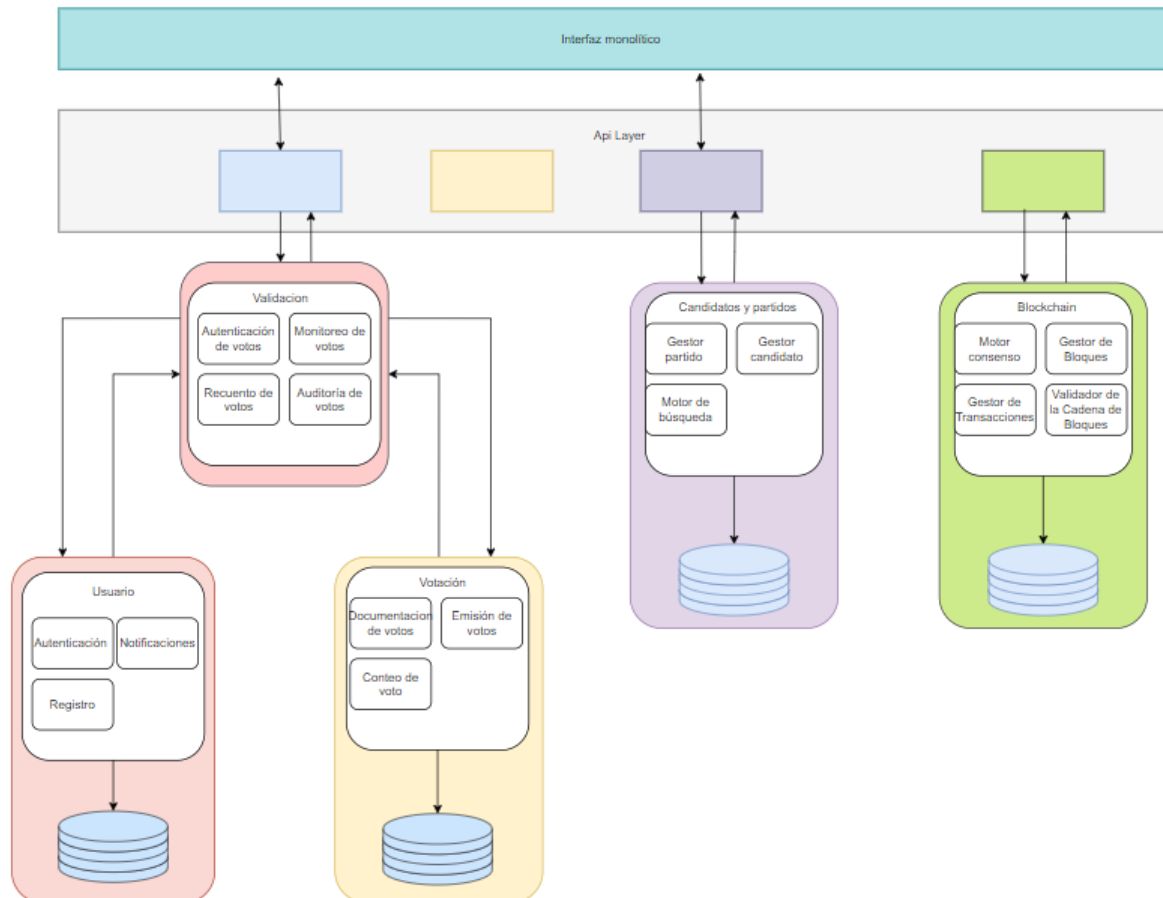
Eddie Alejandro Girón Carranza 1307419
Julio Anthony Engels Ruiz Coto 1284719
Oscar Josué Rivera Menendez 1203819
Diana Alejandra Aragón López 2530019

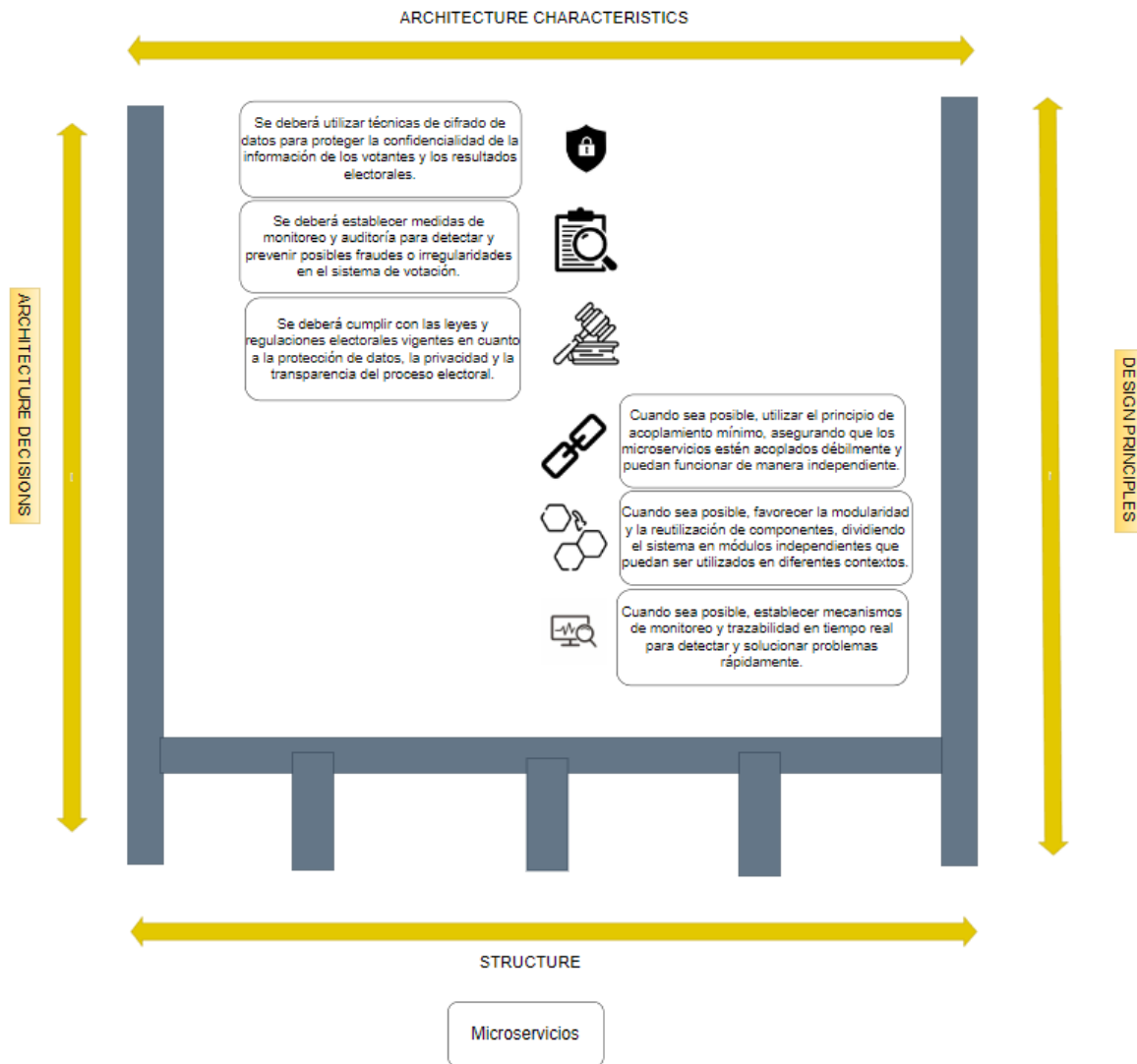
GUATEMALA DE LA ASUNCIÓN, JULIO 5 DE 2023
CAMPUS CENTRAL



Un sistema de votación debe ser capaz de manejar eficientemente un mayor número de votantes a medida que crece el electorado. La escalabilidad garantiza que el sistema pueda funcionar sin problemas y sin interrupciones, incluso durante períodos de alto volumen de votación. Un sistema escalable permite que los votantes accedan y emitan sus votos de manera eficiente y sin demoras significativas, debido a la población creciente la escalabilidad es una característica arquitectónica que se debe tomar en cuenta. La seguridad garantiza que el proceso de votación sea justo y que los resultados reflejen con precisión la voluntad de los electores. Un sistema de votación seguro protege contra amenazas como la manipulación de votos, el fraude electoral y

la interferencia externa. Un sistema de votación con una buena usabilidad garantiza que sea fácil de entender y utilizar para todos los votantes, incluyendo aquellos con habilidades tecnológicas limitadas o discapacidades. La usabilidad permite que el proceso de votación sea accesible para una amplia gama de personas, lo que promueve la participación inclusiva en el proceso democrático.





Otros decisiones de tecnologías

- **Lenguajes:** Java, JavaScript (Node.js para backend, React para frontend).
- **Base de Datos:** MySQL, Blockchain (Ethereum).
- **Infraestructura:** Docker para contenedores
- **Autenticación:** OAuth2, JWT.
- **Pruebas:** Junit, Mocha.
- **Servicios de nube:** Google Cloud

Patrones de diseño

Se utilizará el patrón observer para varios razones



El patrón Observer permite que los diferentes componentes del sistema estén informados y actualizados en tiempo real sobre los eventos y cambios relevantes en el sistema de votaciones. Por ejemplo, cuando se registra un nuevo voto, los observadores pueden recibir notificaciones instantáneas y actuar en consecuencia. Esto es especialmente útil para mantener un recuento de votos en tiempo real y mostrar resultados actualizados a medida que se emiten los votos.

También se tiene la idea de utilizar el patrón de “Proxy” para ayudar a la validación de votos. El patrón Proxy puede permitir que un auditor tenga acceso a la información relevante utilizando un Proxy específico para ese propósito. El Proxy puede actuar como una capa adicional que permite al auditor acceder a los datos y registros necesarios para realizar su función de auditoría, mientras mantiene el resto del sistema aislado y seguro. El Proxy puede implementar mecanismos de autenticación y autorización para verificar la identidad y los permisos del auditor antes de permitirles acceder a los datos confidenciales.



ADR

Title:

ADR-1.1: Uso de técnicas de cifrado de datos para proteger la confidencialidad de la información de los votantes y los resultados electorales.

Status: Proposed

Context:

Es fundamental garantizar la confidencialidad de la información de los votantes y los resultados electorales para poder ofrecer total transparencia para un evento de esta importancia a nivel nacional y mundial. Para lograr esto, se requiere el uso de técnicas de cifrado de datos que protejan la información sensible contra accesos no autorizados.

Decision:

Se deberá implementar el uso de técnicas de cifrado de datos para proteger la confidencialidad de la información de los votantes y los resultados electorales. Se recomienda un cifrado de extremo a extremo para garantizar la comunicación en dos puntos, por este medio se garantiza que solo las personas autorizadas puedan acceder a este. Además, se deberán establecer medidas de seguridad para la gestión de claves y certificados, garantizando su protección y autenticidad.

Consequences:

- Con esta decisión se mejoraría la confidencialidad ya que esto contribuye a la seguridad de nuestro sistema, de igual manera se atribuye mayor confianza en los resultados electorales.
- Se debe tomar en cuenta que en aspectos negativos el cifrado aumenta los recursos necesarios lo que puede afectar el rendimiento.

Compliance:

Se alinea con los requisitos de estándares de seguridad y con las leyes de protección de datos.

Notes:

Realizar evaluaciones para identificar vulnerabilidades por lo tanto se necesitan expertos en el área de cifrado. Además esta propuesta será revisada por los stakeholders para obtener su retroalimentación y aprobación.

Title:

ADR-1.2: Establecimiento de medidas de monitoreo y auditoría para detectar y prevenir posibles fraudes o irregularidades en el sistema de votación.

Status: Proposed

Context:

Es esencial garantizar la integridad y confiabilidad del proceso electoral, como es posible observar actualmente a nivel nacional las elecciones se encuentran en pausa debido al mal proceso de datos. Por lo tanto, para lograrlo, se deben establecer medidas de monitoreo y auditoría que permitan detectar y prevenir posibles fraudes o irregularidades en el sistema de votación.

Decision:

Las medidas que se pueden tomar es registrar todas las actividades relevantes del sistema de votación, como el registro de acceso, cambios en la configuración, entre otras. Esto permite rastrear y analizar cualquier actividad sospechosa o inusual, por lo tanto implementar una bitácora. También implementar medidas de control de acceso y autenticación para garantizar que solo las personas autorizadas tengan acceso al sistema de votación, basado en roles.

Consequences:

- En aspectos positivos el monitoreo continuo y el análisis de datos permiten identificar de manera temprana posibles fraudes o comportamientos inusuales, lo que facilita las acciones preventivas y correctivas, por lo tanto se crea un ambiente de control y supervisión.

Compliance:

Se cumple con la transparencia que un sistema electoral requiere, además se cumple con las leyes electorales y protección de datos. Como guatemaltecos se cumpliría con nuestro deber como ciudadanos de brindar un sistema seguro y honesto para un proceso electoral.

Notes:

Esta propuesta será revisada por los stakeholders para obtener su retroalimentación y aprobación. Además se recomienda que las actividades de monitoreo y auditoría deben ser realizadas por personas o entidades independientes y neutrales, que no tengan conflictos de interés en el proceso electoral.

Title:

ADR-1.3: Cumplimiento de leyes y regulaciones electorales en cuanto a la protección de datos, la privacidad y la transparencia del proceso electoral.

Status:Proposed

Context:

Estas normativas buscan garantizar la integridad y confianza en el proceso electoral, así como salvaguardar los derechos de los votantes y la integridad de los datos electorales. En un entorno electoral cada vez más digitalizado, donde se utilizan sistemas electrónicos y tecnologías avanzadas para la realización de votaciones, es crucial tener en cuenta las leyes y regulaciones electorales deben adaptarse a estos avances.

Decision:

Garantizar que el voto de cada elector sea anónimo y confidencial, evitando cualquier forma de identificación del votante a través de los datos electorales. Implementar mecanismos de transparencia y auditoría como la publicación de resultados por mesa, municipio y departamento, la apertura a la observación por parte de terceros independientes. Existen varias medidas contra ciberataques que se pueden implementar para proteger un sistema electoral, en este caso implementar firewalls y sistemas de IDS/IPS para monitorear y controlar el tráfico de red, detectando y bloqueando posibles intentos de intrusión o ataques maliciosos.

Consequences:

- En los aspectos positivos se tiene un fortalecimiento de la confianza en el proceso electoral por parte de los ciudadanos y los usuarios que utilizaran la plataforma. También se reducen los riesgos de ciberataques y manipulación de datos.

Compliance:

Se cumple con la transparencia que un sistema electoral requiere, además se cumple con las leyes electorales y protección de datos.

Notes:

Esta propuesta será revisada por los stakeholders para obtener su retroalimentación y aprobación. Además realizar pruebas de penetración periódicas por parte de expertos en seguridad informática para identificar vulnerabilidades y evaluar la resistencia del sistema frente a posibles ataques.

Prototipo

