Participa UChile:
Sistema de Votación Electrónica Remota de la U. de Chile

Alejandro Hevia

Director Proyecto LTP2, U. de Chile

Depto. Ciencias de la Computación & CLCERT, FCFM

Proyecto de la Prorrectoría U. de Chile

6 de Mayo 2022

clcert Universidad de Chile

Universidad de Chile

Votación Electrónica Remota Universitaria

Característica: Votación remota usando dispositivos móviles (teléfonos, tablets) y computadores vía Internet

Objetivo: elecciones de académicos (directores, consejeros), personal de colaboración, estudiantes, o similares.

Ej. de app de votación e. remota japonesa (CC-BY-SA 4.0)

Nivel de riesgo objetivo: bajo

Qué provee Participa UChile

- **Secreto del voto:** preservado ante un administrador curioso, incluso ante un hackeo al servidor, porque los votos son encriptados y la clave "repartida" entre 3 custodios
- **Certeza de voto contado**: provee mecanismo para asegurarme que mi voto fue contado
- **Integridad del resultado final**: provee un mecanismo para verificar que los resultados fueron calculados correctamente "desde fuera" sin ver los votos
- **Sufragar sin presiones:** Permite mitigar coerción (posibles presiones indebida al momento de votar) vía "votar de nuevo" y remplazar mi voto previamente emitido. Sólo el último voto emitido vale, siempre hay a lo más 1 voto por persona.

Características

- No requiere preparar papeletas de votación ni libro de registro de votantes para el día de la votación
  - Sí requiere definir y publicitar el padrón electoral con anterioridad
- Permite contabilizar blancos y nulos y votos ponderados.
- Todos en el padrón deben tener cuenta UChile.

Requerimientos

1. El marcar una preferencia debe realizarse en un computador o dispositivo móvil conectado a Internet. *Supone que todos los votantes tienen acceso regular a computadores o dispositivos móviles.*
2. Todo miembro del claustro elector debe tener cuenta institucional (cuenta “Mi UChile” o Pasaporte UChile)

Previo a la votación: Configuración y Difusión

- La Junta Electoral Local (JEL) debe:
  - (siguiendo la resolución que llama a votaciones) indicar el padrón electoral para la elección (nombre, RUT, correo) y lista de candidatos, comunicándolo a Participa UChile
  - difundir los detalles del sistema de votación Participa UChile en las unidades, usando Instructivo de votación, afiche y video provista por Participa UChile
  - recordar a los votantes que deben tener acceso a su cuenta y clave Pasaporte / Cuenta UChile
  - volver a recordar fecha y detalles en días previos

El día de la votación misma

- El día inicial de la votación, el equipo de Participa UChile abre la elección a la hora acordada.
- Desde ése momento, los votantes pueden enviar en forma remota sus votos encriptados, simplemente conectándose a https://participa.uchile.cl
- Luego de emitir el voto, todos los votantes pueden ver una "urna electrónica" que contiene lista de votos (encriptados) emitidos sin la identidad de quienes han votado
- Durante el periodo de votación, el equipo de Participa UChile envía reportes periódicos (c/2 hrs aprox.) indicando número de votos recibidos y cualquier evento
- Al concluir la elección, en un día/hora prefijada, el equipo de Participa UChile deshabilita la recepción de votos, cerrando el sistema.

Escrutinio y conclusión

- Cerrada la elección, se hace una "ceremonia de escrutinio":
  - Es una actividad pública (vía zoom, por ej.) con participación de los miembros relevantes de la comunidad
  - Se "abre la urna" publicando estadísticas de la concurrencia (votos recibidos, ponderaciones y ajustes si fueron necesarios),
  - Los custodios de claves se juntan a ejecutar el algoritmo de conteo utilizando sus "trozos" de claves privadas. Al hacerlo, se calcula el total o resultado de la votación, el cual es compartido y publicado.
- Durante el conteo valores públicos anexos de verificación se publican. *Ellos permiten que cualquier persona interna o externa pueda validar/confirmar/auditar el proceso de conteo, asegurándose que el total fue calculado correctamente.*

Resumen

- Sistema de votación moderno, seguro con diseño abierto y transparente
- Asegura privacidad del voto y/o anonimato del votante
- Requiere padrón con cuenta UChile y acceso a computador
- Requiere difusión previa (fecha, necesidad de cuenta, cómo votar)

¿Comentarios? ¿Preguntas?

ahevia@dcc.uchile.cl

clcert
Universidad de Chile

Universidad de Chile

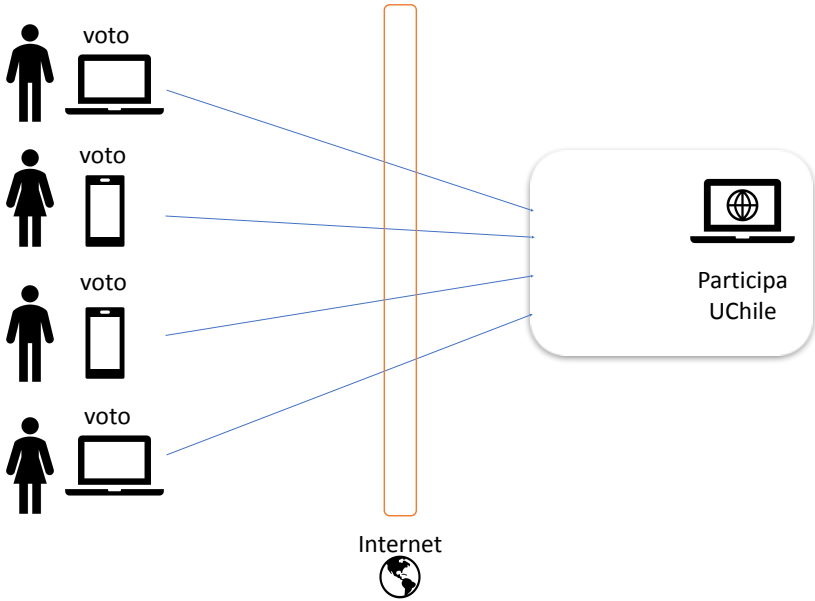
Créditos Íconos e imágenes

Freepik, Pixel Perfect (flaticon.com)

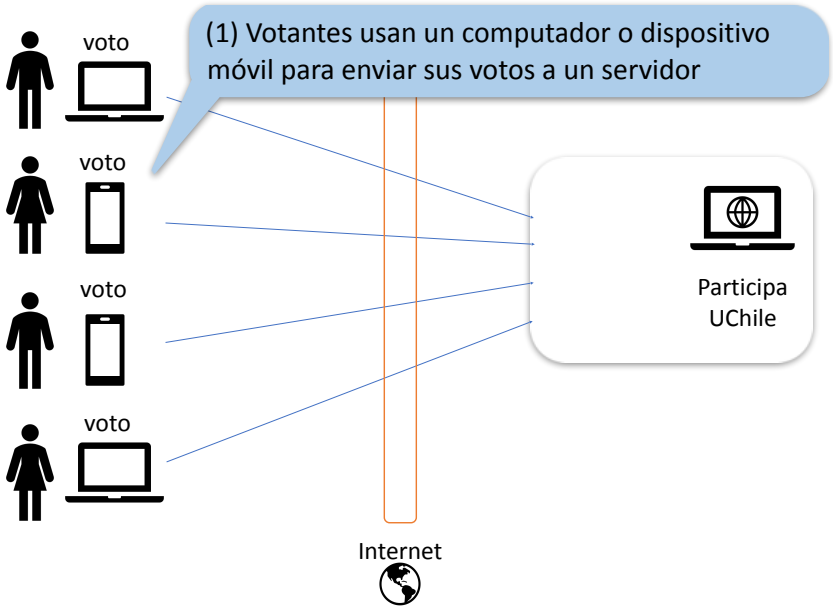
Apéndices

Propiedades del sistema

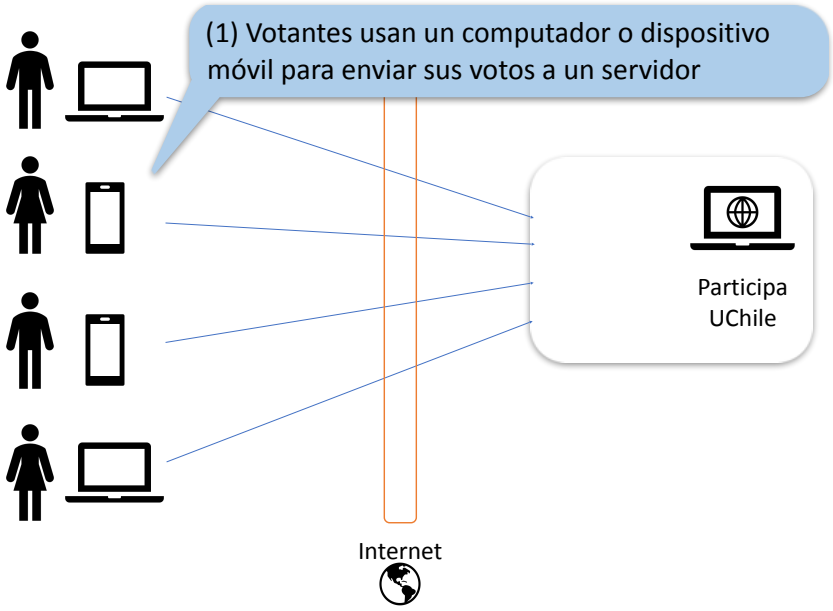
La idea de votación electrónica



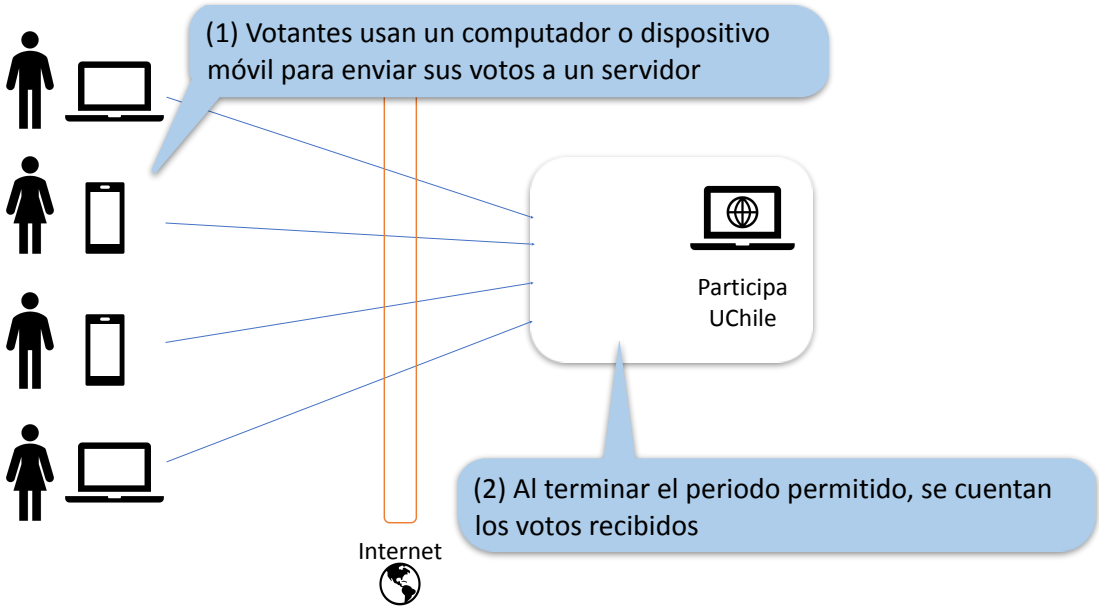
La idea de votación electrónica



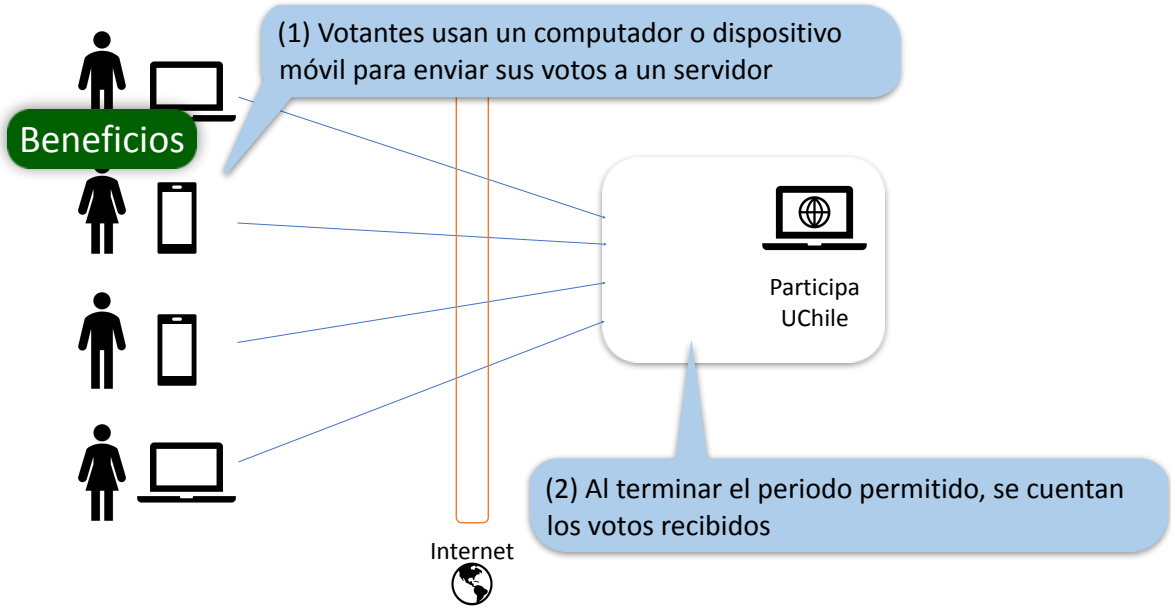
La idea de votación electrónica



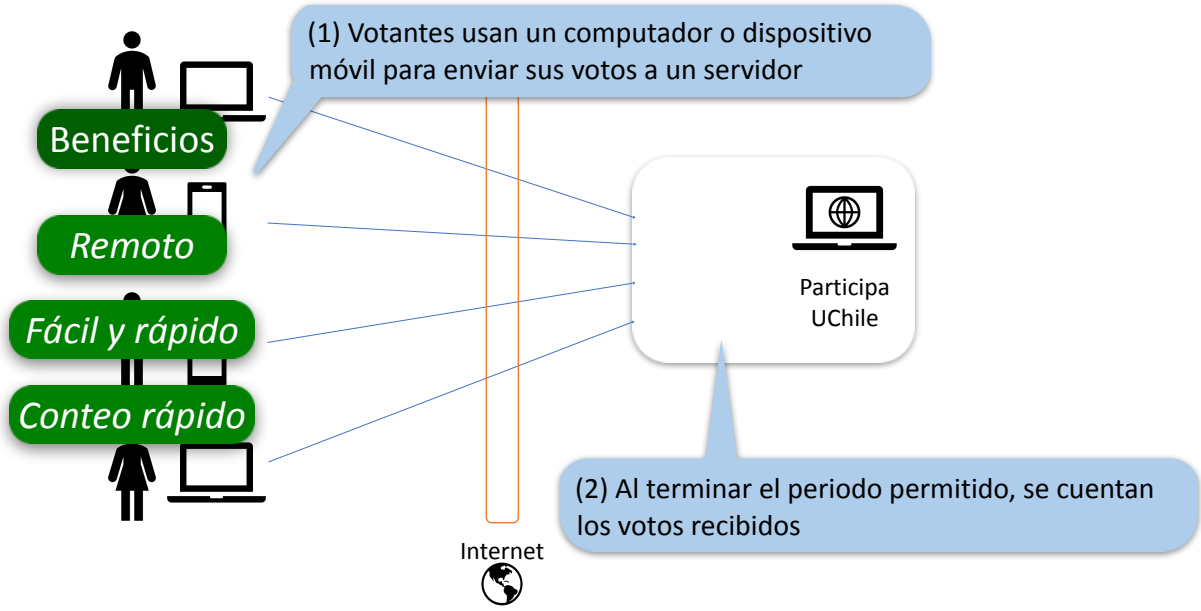
La idea de votación electrónica



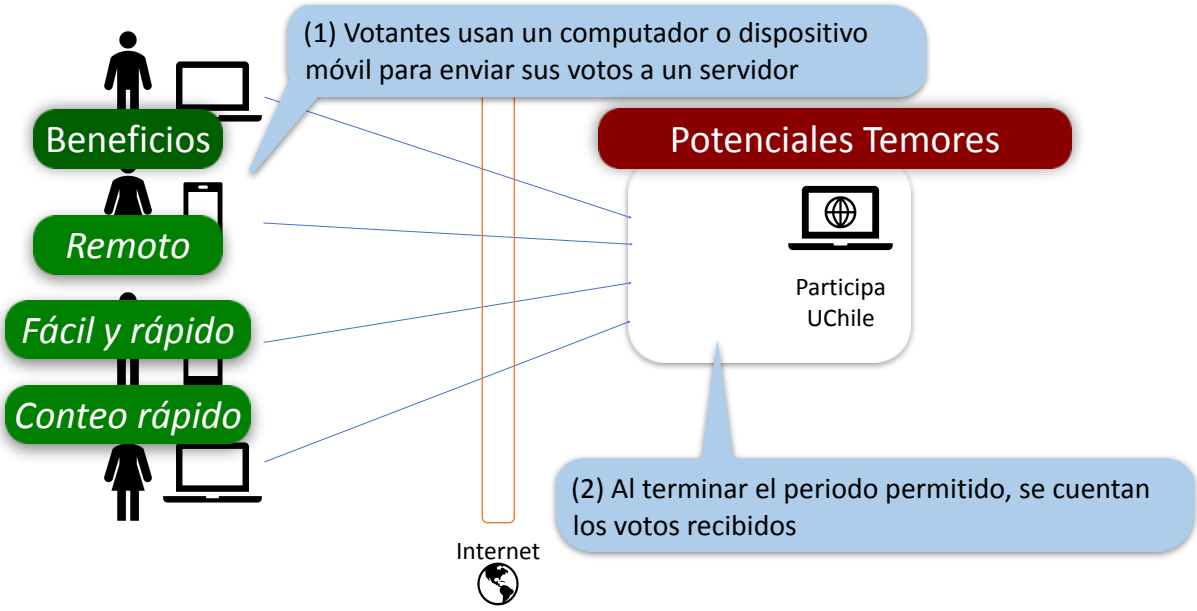
La idea de votación electrónica



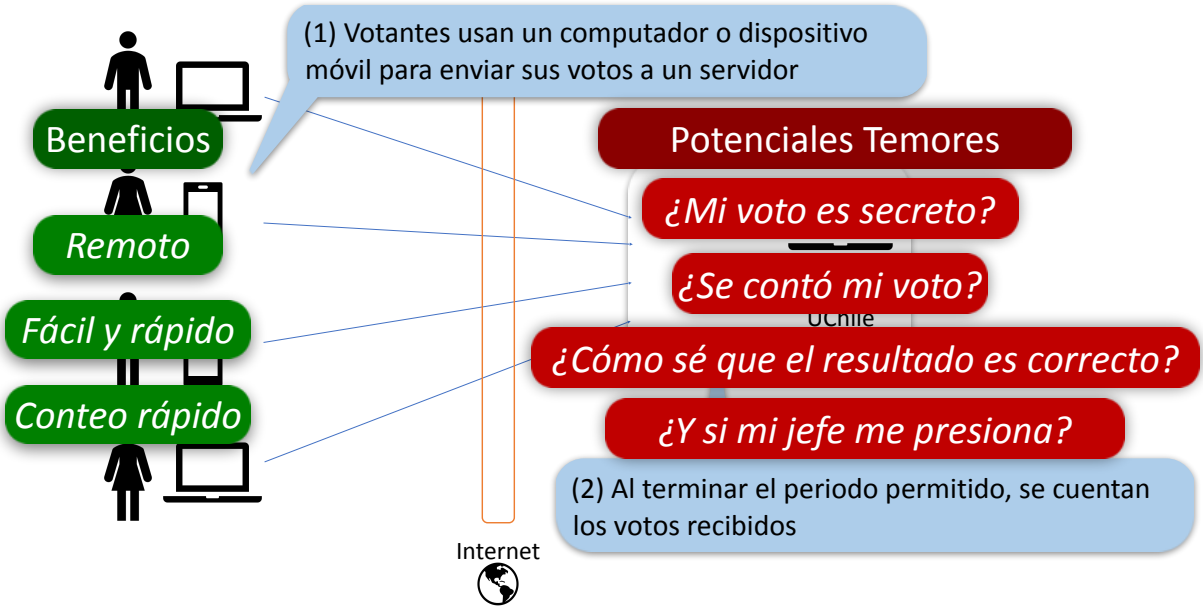
La idea de votación electrónica



La idea de votación electrónica

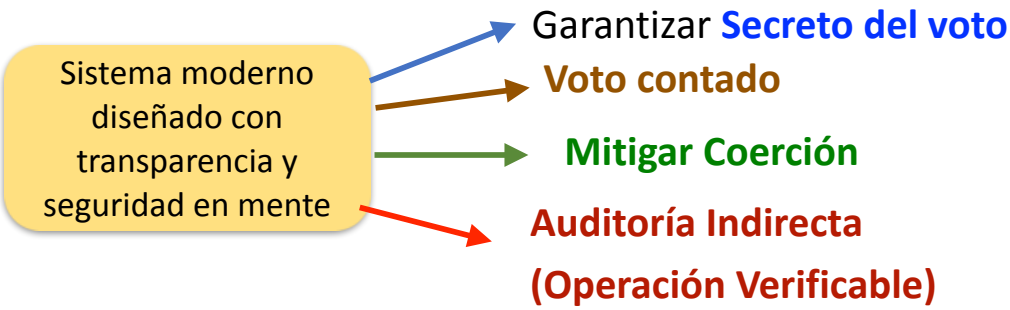


La idea de votación electrónica



Participa UChile: Historia y Diseño

- No **reinventa** la rueda
  - Basado en HeliosVoting.org (Ben Adida, 2008; usado por la *Asociación Internacional de Investigación Criptográfica, U.C.Louvain,* entre otros)
  - Mejorado y adaptado para la U. de Chile
- Diseño **transparente** y código **abierto**
  - Usa Criptografía (garantías matemáticas) y será de código abierto



Participa UChile: Historia y Diseño

- No **reinventa** la rueda
  - Basado en HeliosVoting.org (Ben Adida, 200
    Internacional de Investigación Criptográfica,
  - Mejorado y adaptado para la U. de Chile
- Diseño **transparente** y código **abierto**
  - Usa Criptografía (garantías matemáticas) y será de cód go abierto

- Votos **encriptados**
- Clave "dividida" **entre 2 ó 3 custodios,** para conteo se necesitan sólo 2
- Custodios por ahora administradores pero en el futuro no tienen que serlo

Sistema moderno diseñado con transparencia y seguridad en mente

Garantizar **Secreto del voto**

Voto contado

Mitigar Coerción

Auditoría Indirecta

(Operación Verificable)

Participa UChile: Historia y Diseño

- No **reinventa** la rueda
  - Basado en HeliosVoting.org (Ben Adida, 200
    Internacional de Investigación Criptográfica,
  - Mejorado y adaptado para la U. de Chile
- Diseño **transparente** y código **abierto**
  - Usa Criptografía (garantías matemáticas) y será de cód go ab

- Votos **encriptados**
- Clave "dividida" **entre 2 ó 3 custodios,** para conteo se necesitan sólo 2
- Custodios por ahora administradores pero en el futuro no tienen que serlo

Hay urna virtual donde confirmar está el voto emitido

Sistema moderno diseñado con transparencia y seguridad en mente

Garantizar **Secreto del voto**

Voto contado

Mitigar Coerción

Auditoría Indirecta

(Operación Verificable)

Participa UChile: Historia y Diseño

- No **reinventa** la rueda
  - Basado en HeliosVoting.org (Ben Adida, 200
    Internacional de Investigación Criptográfica,
  - Mejorado y adaptado para la U. de Chile
- Diseño **transparente** y código **abierto**
  - Usa Criptografía (garantías matemáticas) y será de cód go ab

- Votos **encriptados**
- Clave "dividida" **entre 2 ó 3 custodios,** para conteo se necesitan sólo 2
- Custodios por ahora administradores pero en el futuro no tienen que serlo

Hay urna virtual donde confirmar está el voto emitido

Sistema moderno diseñado con transparencia y seguridad en mente

Garantizar **Secreto del voto**

Voto contado

Mitigar Coerción

Permite "reemplazar" voto emitido si se necesita

Auditoría Indirecta

(Operación Verificable)

Participa UChile: Historia y Diseño

- No **reinventa** la rueda
  - Basado en HeliosVoting.org (Ben Adida, 200
    Internacional de Investigación Criptográfica,
  - Mejorado y adaptado para la U. de Chile
- Diseño **transparente** y código **abierto**
  - Usa Criptografía (garantías matemáticas) y será de có go ab

- Votos **encriptados**
- Clave "dividida" **entre 2 ó 3 custodios,** para conteo se necesitan sólo 2
- Custodios por ahora administradores pero en el futuro no tienen que serlo

Hay urna virtual donde confirmar está el voto emitido

Sistema moderno diseñado con transparencia y seguridad en mente

Garantizar **Secreto del voto**

Voto contado

Mitigar Coerción

Auditoría Indirecta

(Operación Verificable)

Permite "reemplazar" voto emitido si se necesita

Observador externo puede "recalcular" y verificar conteo

Riesgos inherentes en votación remota

- Ningún sistema de votación electrónico remoto es 100% seguro
  - **Virus**, **falla Internet**, o ataques (DoS) para **botar el servidor**
- Pero son inusuales en elecciones universitarias
  - ataques caros/difíciles de llevar a cabo
  - menos interés vs. elecciones nacionales, por ej.

Aviso de caída por cáscara de plátano (dominio público)

- NO busca reemplazar mecanismos existentes, sólo agrega uno nuevo