Modelo de encriptación con llaves colegiadas

Aplicación para el voto electrónico en la Universidad Técnica Federico Santa María, Chile.

Cuarta Conferencia de Directores de Tecnología de Información y Comunicación en Instituciones de Educación Superior: Gestión de las TICs para la investigación y colaboración

Gustavo Anabalón

Gustavo.anabalon@usm.cl

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Universidad Técnica Federico Santa María

DIRECCION DE TECNOLOGIAS DE INFORMACION

Institución universitaria de más de 83 años de tradición, orientada a cultivar las ciencias y las tecnologías.

Uno de los principales objetivos legados por su fundador es: "*Poner al alcance del desvalido meritorio llegar al más alto grado del saber humano*".

Actualmente ya supera los 20.000 estudiantes.

Su casa central está ubicada en la ciudad de Valparaíso, Chile.

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

USM Gobierno Corporativo

DIRECCION DE TECNOLOGIAS DE INFORMACION

- **Consejo Superior**
  - **Representante del Presidente de la República**
  - **Representante de los Exalumnos**
  - **Seis Consejeros Académicos**
  - **Un Consejero, elegido por el Consejo Académico y los Directores de sedes**
  - **El Presidente, elegido por el Consejo Académico y los Directores de sedes**

    (*Entre los Exalumnos*)
- **Consejo Académico**
- **Consejo Normativo**

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Consejero representante de los Exalumnos

DIRECCION DE TECNOLOGIAS DE INFORMACION

- **Representa la visión desde el mundo profesional hacia el gobierno corporativo**
- **Entrega un testimonio claro de la importancia que da la institución a sus egresados**
- **Los egresados son la materialización del producto de la institución**

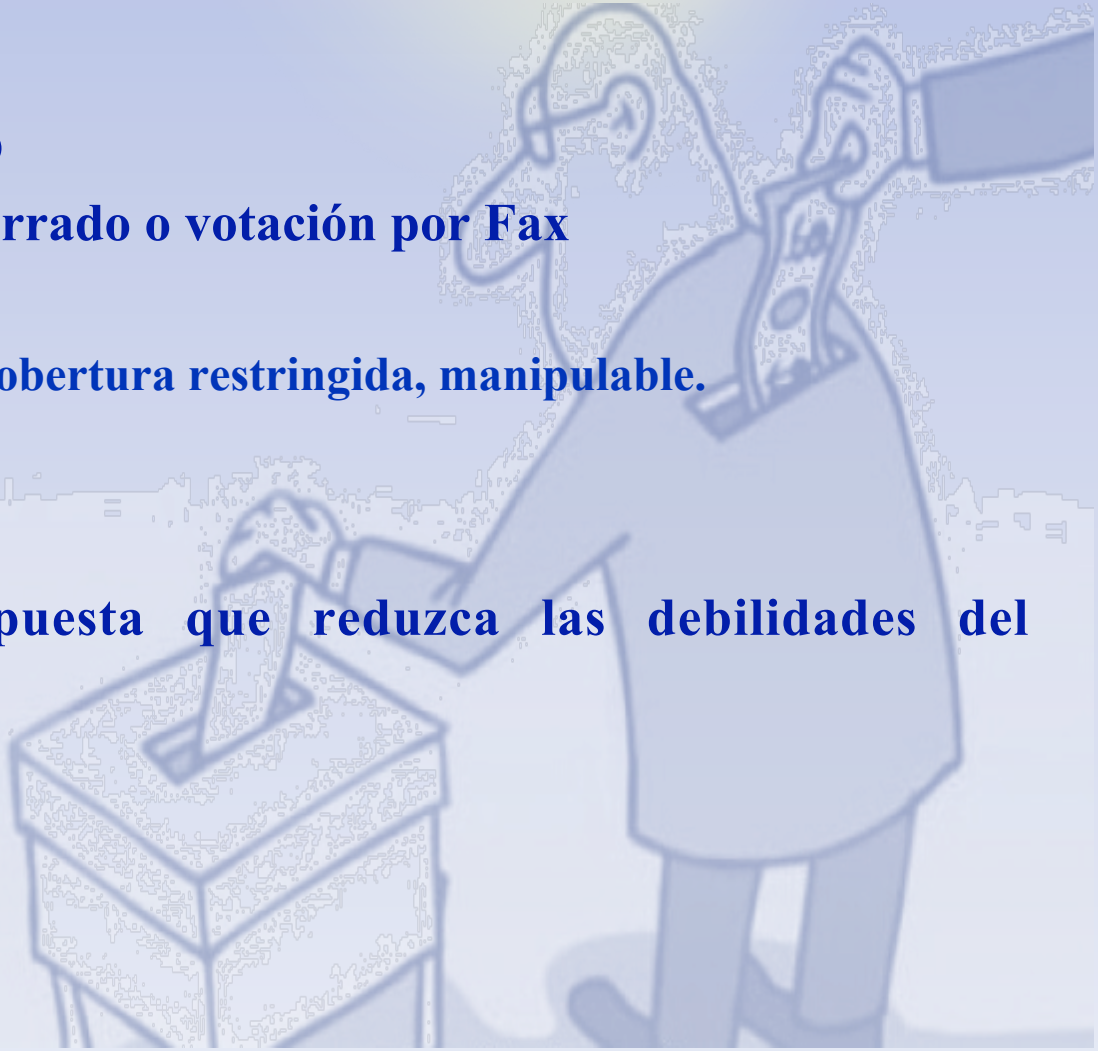
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Elección del Consejero Superior

DIRECCION DE TECNOLOGIAS DE INFORMACION

- **Procedimiento Clásico**
  - **Votación por sobre cerrado o votación por Fax**
  - **Debilidades**
    - **Inseguro, lento, de cobertura restringida, manipulable.**

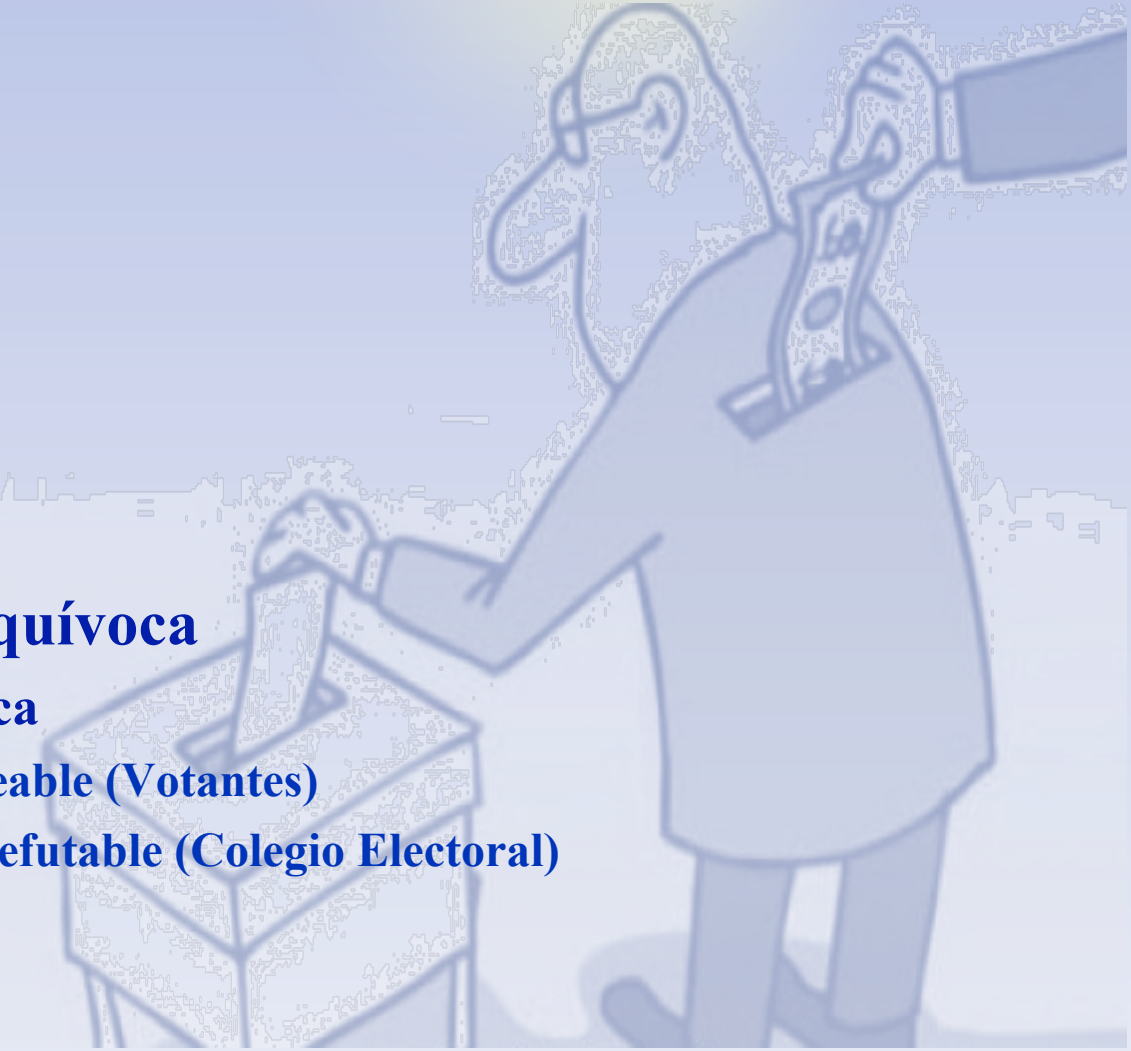
- **Desafío**
  - **Formular una propuesta que reduzca las debilidades del procedimiento clásico**



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Premisas

- Secreto
- Simple
- Verificable
  - Auditable
- Confiable
  - Auditorias
- Identificación inequívoca
  - Firma Electrónica
    - Simple: Rastreable (Votantes)
    - Avanzada: Irrefutable (Colegio Electoral)



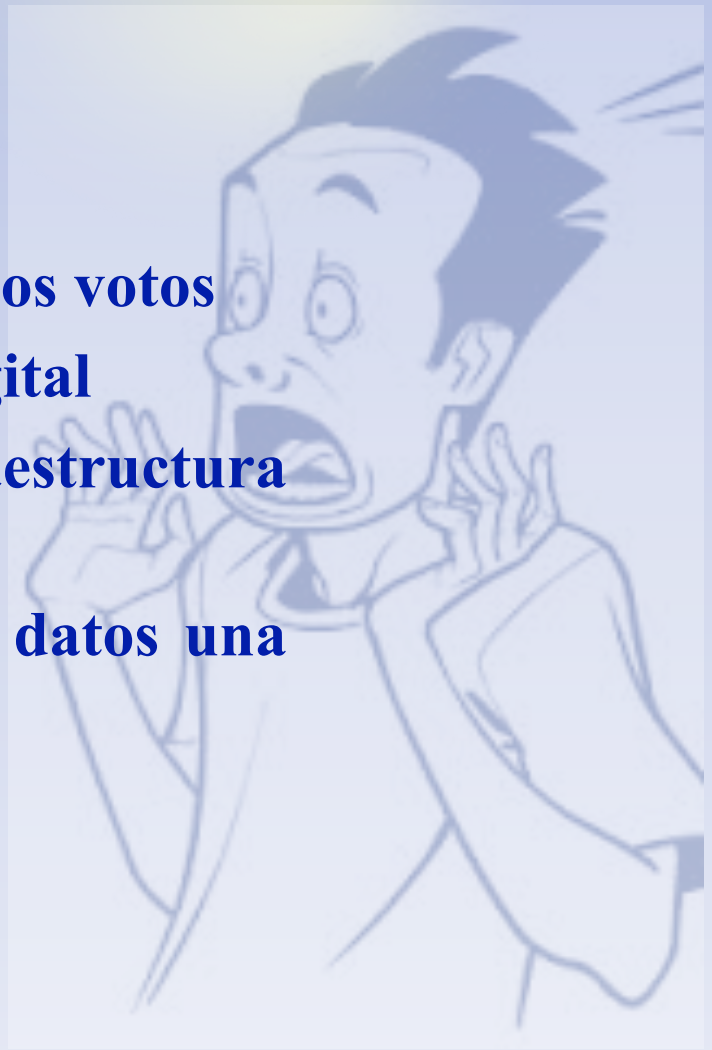
DIRECCION DE TECNOLOGIAS DE INFORMACION

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Aprehensiones

DIRECCION DE TECNOLOGIAS DE INFORMACION

- Riesgo de Suplantación
- Fraude en el registro y conteo de los votos
- Poca participación por brecha digital
- Pérdida ante desastre en la infraestructura tecnológica
- Temor a no poder recuperar los datos una vez cerrado el proceso



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Principales Componentes

DIRECCION DE TECNOLOGIAS DE INFORMACION

- Padrón electoral
- Incorporación de Firma Electrónica Avanzada
- Modelo de almacenamiento de sufragios seguro
- Procedimiento colegiado para abrir y cerrar la “urna electoral”
- Plataforma de Servidores Exclusiva y cerrada
- Acceso a plataforma transferido al CE
- Archivos del proceso respaldados y firmados electrónicamente

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

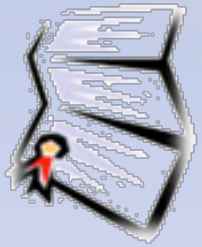
Proceso de Votación

DIRECCION DE TECNOLOGIAS DE INFORMACION

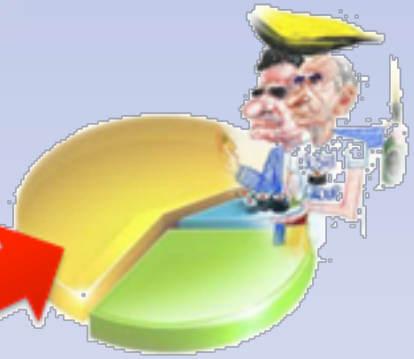
VOTANTES

Llamado

(a registro y a sufragar)



Resultados



Sufragios realizados

Escrutinio

VOTO

- X Pedro Candel
- X Voto en Blanco

AUDITORIA

- RUT votante
- Fecha
- Dirección ip
- Navegador

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Modelo de almacenamiento de sufragios seguro

DIRECCION DE TECNOLOGIAS DE INFORMACION

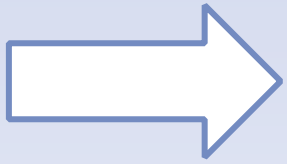
- **Proceso de Votaciones**

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Modelo de almacenamiento de sufragios seguro

DIRECCION DE TECNOLOGIAS DE INFORMACION

- **Apertura de Urna**



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

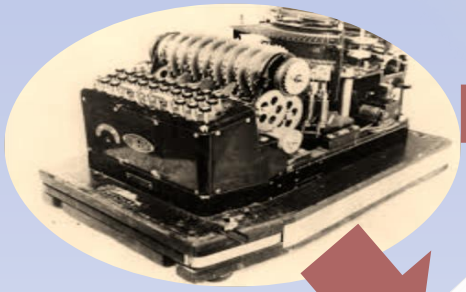
dti DIRECCION DE TECNOLOGIAS DE INFORMACION

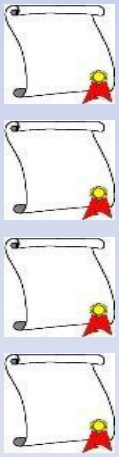
¿Qué pasa si alguien manipula la llave privada?

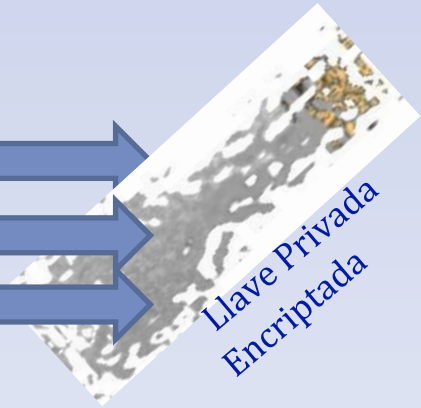
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Procedimiento colegiado para encriptar la llave privada

DIRECCION DE TECNOLOGIAS DE INFORMACION



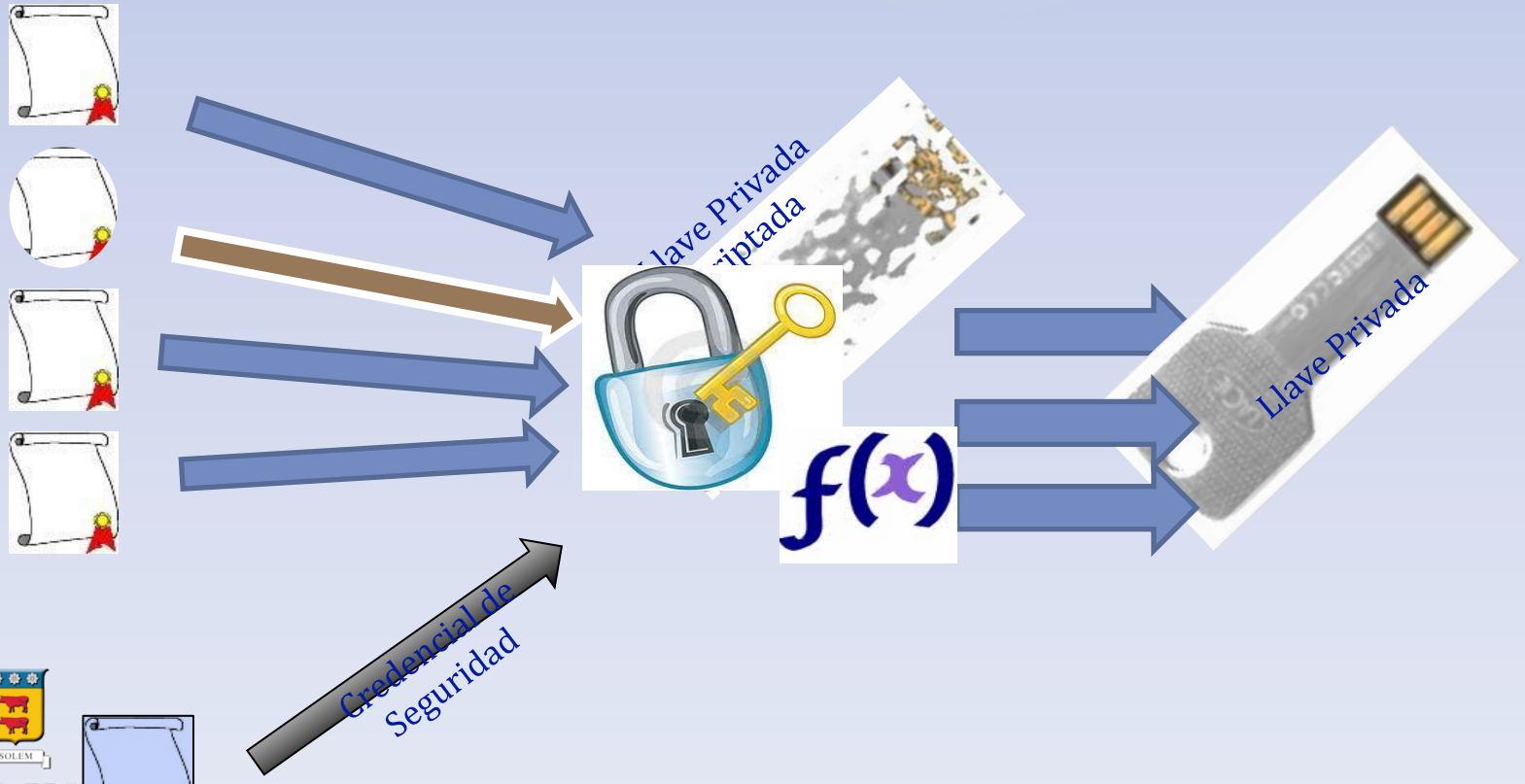




Credencial de Seguridad

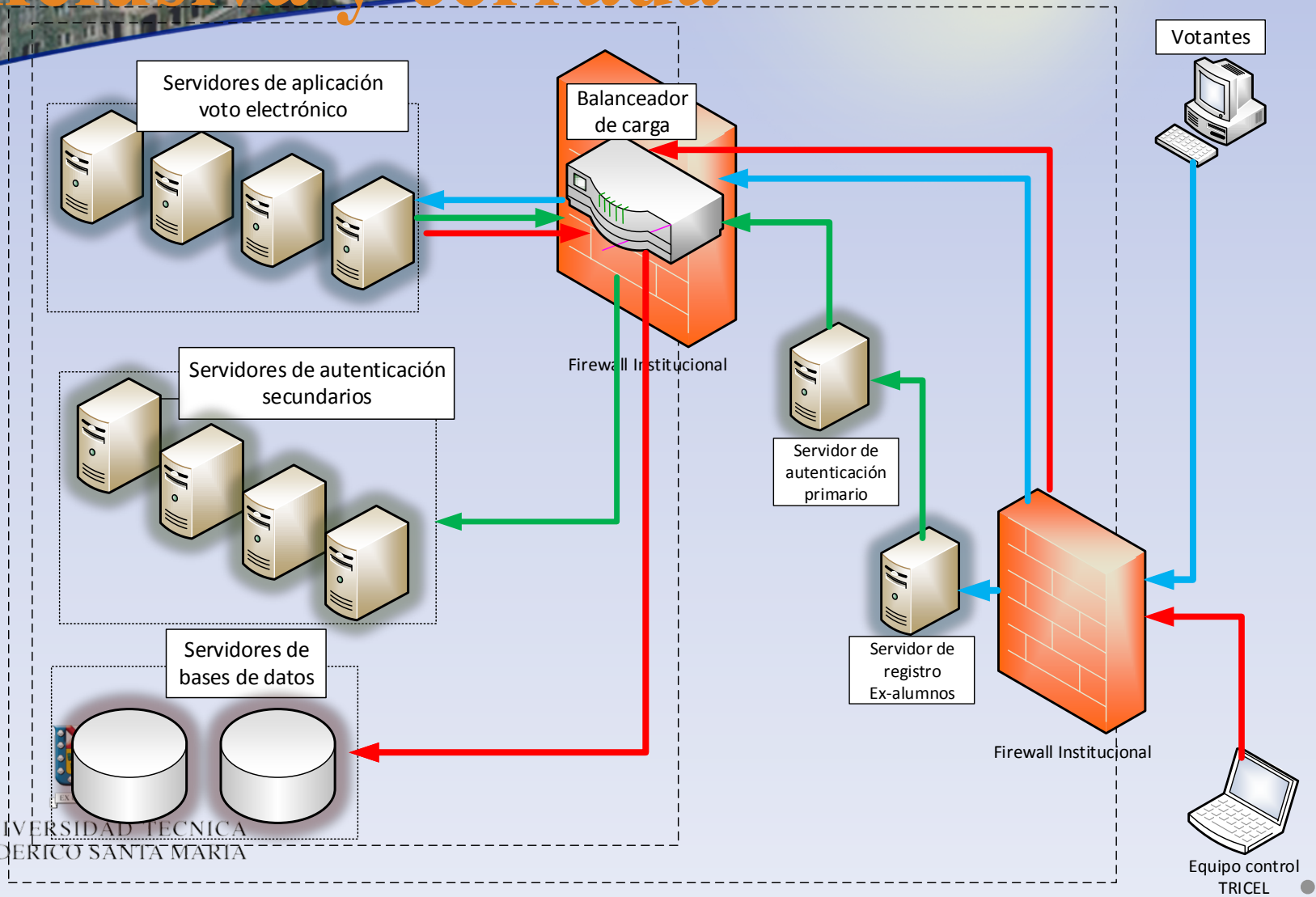
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Procedimiento colegiado para desencriptar la llave privada



Plataforma de Servidores exclusiva y cerrada

DIRECCION DE TECNOLOGIAS DE INFORMACION



El Proceso

- Conformación del Padrón
- Certificación de las Aplicaciones y de la Plataforma
- Apertura del Proceso
- Proceso de Votación Electrónica
- Cierre y Publicación de Resultados

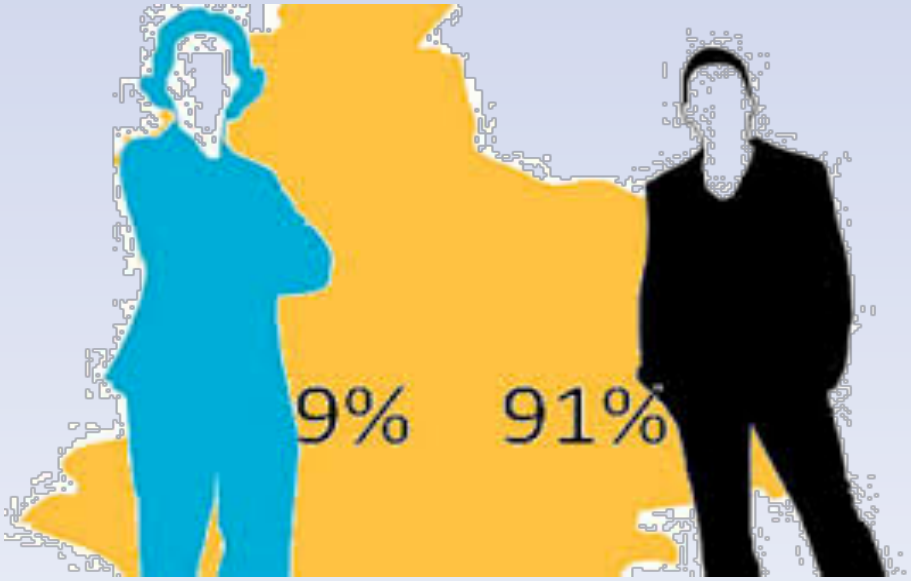
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

La Experiencia

DIRECCION DE TECNOLOGIAS DE INFORMACION

- **Conformación del Padrón**
  - **Más de 20 invitaciones y recordatorios enviados a 34.000 direcciones de correos electrónicos.**
  - **783 electores registrados**
  - **585 electores validados**

- **Candidatos**
  - **Pedro Candel**



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Resultados

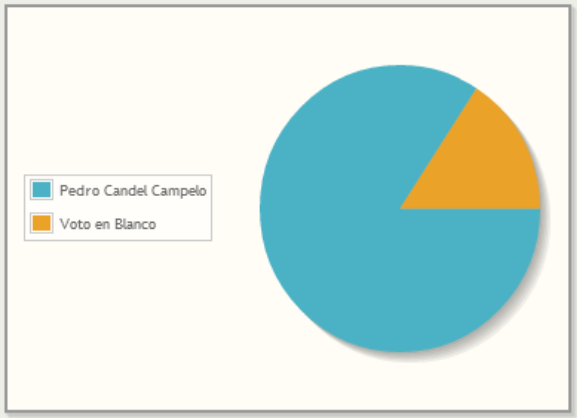
- 367 Sufragios (63% del padrón)
- 309 Votos por don Pedro Candel (84,2%)
- 58 Votos en blanco (15,8%)

RESULTADOS

Universo de Votantes:	585	100.0%
Votos válidamente emitidos:	367	62.74%

Opción	Cantidad de Votos	% Votos Emitidos	% Universo de Votantes
Pedro Candel Campelo	309	84.2	52.82
Voto en Blanco	58	15.8	9.91
TOTAL	367	100.0	62.74

GRÁFICO DE VOTACIÓN



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Comentarios Finales

- ***El modelo de encriptación basado en llaves colegiadas, permite guardar información segura, que sólo puede ser accedida con la concurrencia simultánea del quórum definido por el grupo que le dio origen.***

- ***Las aplicaciones que se pueden construir a partir de este modelo son todas aquellas que requieran mantener custodiada información confidencial, tanto para procesos eleccionarios, como para documentos de carácter notarial, valores, herencias, etcétera.***

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

DIRECCION DE TECNOLOGIAS DE INFORMACION

Muchas Gracias

Gustavo Anabalón

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA