

# Consideraciones sobre el Voto Electrónico

M. Montes, D. Penazzi, N. Wolovick

Universidad Nacional de Córdoba

12 de Abril de 2016

# Contenidos

Introducción

Problemas con el Voto Electrónico

Requerimientos mínimos de un sistema de VE

Algunos ejemplos

## DREs y EBPs (IREs)

- En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en **una sola máquina**.

## DREs y EBPs (IREs)

- En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas suelen llamarse **Direct-Recording Electronic** voting machines (DRE).

## DREs y EBPs (IREs)

- En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas suelen llamarse **Direct-Recording Electronic** voting machines (DRE).
- Algunos tienen un registro en papel que es guardado para auditorías, otros no.

## DREs y EBPs (IREs)

- En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas suelen llamarse **Direct-Recording Electronic** voting machines (DRE).
- Algunos tienen un registro en papel que es guardado para auditorías, otros no.
- Otros sistemas separan físicamente la generación del voto del conteo del voto, permitiendo que el elector realice una **creación de un objeto físico** que representa su voto (un “token” o “boleta”), la cual es depositada en una urna para ser contada posteriormente, ya sea manual o electrónicamente.

## DREs y EBPs (IREs)

- En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en **una sola máquina**.
- Estos sistemas suelen llamarse **Direct-Recording Electronic** voting machines (DRE).
- Algunos tienen un registro en papel que es guardado para auditorías, otros no.
- Otros sistemas separan físicamente la generación del voto del conteo del voto, permitiendo que el elector realice una **creación de un objeto físico** que representa su voto (un “token” o “boleta”), la cual es depositada en una urna para ser contada posteriormente, ya sea manual o electrónicamente.
- Suelen ser llamados **Electronic Ballot Printers** (EBP) o **Indirect-Recording Electronic** voting machines (IRE).

## Voto Electrónico vs Boleta Electrónica

- La característica técnica que distingue los DREs de los EBPs es que los EBPs no guardan ningún dato sobre el voto que generó (al menos, no deberían guardarlo) mientras que los DRE necesariamente deben hacerlo.

## Voto Electrónico vs Boleta Electrónica

- La característica técnica que distingue los DREs de los EBPs es que los EBPs no guardan ningún dato sobre el voto que generó (al menos, no deberían guardarlo) mientras que los DRE necesariamente deben hacerlo.
- EBPs son mas seguros que los DRE, aunque los costos pueden ser mayores.

## Voto Eléctronico vs Boleta Electrónica

- La característica técnica que distingue los DREs de los EBPs es que los EBPs no guardan ningún dato sobre el voto que generó (al menos, no deberían guardarlo) mientras que los DRE necesariamente deben hacerlo.
- EBPs son mas seguros que los DRE, aunque los costos pueden ser mayores.
- Algunas personas cualifican la expresión “voto electrónico” sólo para determinados sistemas.

## Voto Electrónico vs Boleta Electrónica

- La característica técnica que distingue los DREs de los EBPs es que los EBPs no guardan ningún dato sobre el voto que generó (al menos, no deberían guardarlo) mientras que los DRE necesariamente deben hacerlo.
- EBPs son mas seguros que los DRE, aunque los costos pueden ser mayores.
- Algunas personas cualifican la expresión “voto electrónico” sólo para determinados sistemas.
- Por ejemplo, a veces se usa “voto electrónico” sólo si la emisión del voto es electrónica, y “conteo electrónico” si sólo se usa en la parte del conteo.

## Voto Electrónico vs Boleta Electrónica

- La característica técnica que distingue los DREs de los EBPs es que los EBPs no guardan ningún dato sobre el voto que generó (al menos, no deberían guardarlo) mientras que los DRE necesariamente deben hacerlo.
- EBPs son mas seguros que los DRE, aunque los costos pueden ser mayores.
- Algunas personas cualifican la expresión “voto electrónico” sólo para determinados sistemas.
- Por ejemplo, a veces se usa “voto electrónico” sólo si la emisión del voto es electrónica, y “conteo electrónico” si sólo se usa en la parte del conteo.
- Algunas personas llaman “Voto Electrónico” sólo a los DREs y a los EBPs los llaman “Boleta Electrónica”.

## Voto Electrónico vs Boleta Electrónica

- La característica técnica que distingue los DREs de los EBPs es que los EBPs no guardan ningún dato sobre el voto que generó (al menos, no deberían guardarlo) mientras que los DRE necesariamente deben hacerlo.
- EBPs son mas seguros que los DRE, aunque los costos pueden ser mayores.
- Algunas personas cualifican la expresión “voto electrónico” sólo para determinados sistemas.
- Por ejemplo, a veces se usa “voto electrónico” sólo si la emisión del voto es electrónica, y “conteo electrónico” si sólo se usa en la parte del conteo.
- Algunas personas llaman “Voto Electrónico” sólo a los DREs y a los EBPs los llaman “Boleta Electrónica”.
- Es un detalle que no vale la pena discutir mucho ahora, pero en una ley de voto electrónico debería quedar claro cual definición se usa.

# Requerimientos Básicos de un sistema de votación

- En cualquier sistema de votación debe garantizarse, entre otras cosas:

# Requerimientos Básicos de un sistema de votación

- En cualquier sistema de votación debe garantizarse, entre otras cosas:
  - El **secreto** del voto.

# Requerimientos Básicos de un sistema de votación

- En cualquier sistema de votación debe garantizarse, entre otras cosas:
  - El **secreto** del voto.
  - La **fidelidad** del voto (el resultado final debe reflejar la voluntad de los electores)

# Requerimientos Básicos de un sistema de votación

- En cualquier sistema de votación debe garantizarse, entre otras cosas:
  - El **secreto** del voto.
  - La **fidelidad** del voto (el resultado final debe reflejar la voluntad de los electores)
  - Que sólo **electores autorizados** voten y que cada elector emita **un y sólo un voto**

# Requerimientos Básicos de un sistema de votación

- En cualquier sistema de votación debe garantizarse, entre otras cosas:
  - El **secreto** del voto.
  - La **fidelidad** del voto (el resultado final debe reflejar la voluntad de los electores)
  - Que sólo **electores autorizados** voten y que cada elector emita **un y sólo un voto**
- El primer requerimiento incluye un subrequerimiento:

# Requerimientos Básicos de un sistema de votación

- En cualquier sistema de votación debe garantizarse, entre otras cosas:
  - El **secreto** del voto.
  - La **fidelidad** del voto (el resultado final debe reflejar la voluntad de los electores)
  - Que sólo **electores autorizados** voten y que cada elector emita **un y sólo un voto**
- El primer requerimiento incluye un subrequerimiento: **La no coercibilidad del voto.**

## Tres principios básicos

Respetar la **fidelidad** del voto se plasma en tres principios básicos, que son conocidos (en inglés) como:

## Tres principios básicos

Respetar la **fidelidad** del voto se plasma en tres principios básicos, que son conocidos (en inglés) como:

**Cast-As-Intended** el voto se “crea” en la forma que el votante realmente planea votar.

## Tres principios básicos

Respetar la **fidelidad** del voto se plasma en tres principios básicos, que son conocidos (en inglés) como:

**Cast-As-Intended** el voto se “crea” en la forma que el votante realmente planea votar.

**Store-As-Cast** el voto se resguarda de la forma en que fue creado, sin alteraciones.

## Tres principios básicos

Respetar la **fidelidad** del voto se plasma en tres principios básicos, que son conocidos (en inglés) como:

**Cast-As-Intended** el voto se “crea” en la forma que el votante realmente planea votar.

**Store-As-Cast** el voto se resguarda de la forma en que fue creado, sin alteraciones.

**Tallied-As-Stored** el voto se cuenta en la forma en que fue resguardado, sin alteraciones.

# Problemas Teóricos

El VE tiene problemas a **nivel teórico** y a **nivel práctico**.

## Problemas Teóricos

El VE tiene problemas a **nivel teórico** y a **nivel práctico**.

- A nivel teórico es un problema de difícil solución pues los requerimientos de mantener el **secreto** pero al mismo tiempo poder corroborar la **fidelidad** del voto son **contradictorios**.

## Problemas Teóricos

El VE tiene problemas a **nivel teórico** y a **nivel práctico**.

- A nivel teórico es un problema de difícil solución pues los requerimientos de mantener el **secreto** pero al mismo tiempo poder corroborar la **fidelidad** del voto son **contradictorios**.
- A diferencia de un cajero automático, donde la identidad del extractor de dinero es conocida, y las transacciones quedan registradas, aquí la identidad del votante debe ser oculta, para garantizar el secreto del voto.

## Problemas Teóricos

El VE tiene problemas a **nivel teórico** y a **nivel práctico**.

- A nivel teórico es un problema de difícil solución pues los requerimientos de mantener el **secreto** pero al mismo tiempo poder corroborar la **fidelidad** del voto son **contradictorios**.
- A diferencia de un cajero automático, donde la identidad del extractor de dinero es conocida, y las transacciones quedan registradas, aquí la identidad del votante debe ser oculta, para garantizar el secreto del voto.
- Entonces debido a que no es deseable guardar mucha información sobre el voto en si, **no es fácil hacer un sistema que permita ser auditado** para comprobar si hubo o no algún problema.

# ¿Democrático?

- Otro problema a nivel teórico tiene que ver con la esencia del proceso democrático.

## ¿Democrático?

- Otro problema a nivel teórico tiene que ver con la esencia del proceso democrático.
- No sirve de nada un sistema seguro, rápido, fidedigno, etc., si **los únicos que lo pueden entender son miembros de una elite técnica.**

## ¿Democrático?

- Otro problema a nivel teórico tiene que ver con la esencia del proceso democrático.
- No sirve de nada un sistema seguro, rápido, fidedigno, etc., si **los únicos que lo pueden entender son miembros de una elite técnica.**
- Pero por su naturaleza misma, eso es lo que suele pasar con el VE.

## ¿Democrático?

- Otro problema a nivel teórico tiene que ver con la esencia del proceso democrático.
- No sirve de nada un sistema seguro, rápido, fidedigno, etc., si **los únicos que lo pueden entender son miembros de una elite técnica.**
- Pero por su naturaleza misma, eso es lo que suele pasar con el VE.
- Por lo tanto hay que agregar elementos que permitan al votante, aún sin entender todos los detalles, estar razonablemente seguro que las partes fundamentales del acto de votar se cumplen.

## ¿Democrático?

- Otro problema a nivel teórico tiene que ver con la esencia del proceso democrático.
- No sirve de nada un sistema seguro, rápido, fidedigno, etc., si **los únicos que lo pueden entender son miembros de una elite técnica.**
- Pero por su naturaleza misma, eso es lo que suele pasar con el VE.
- Por lo tanto hay que agregar elementos que permitan al votante, aún sin entender todos los detalles, estar razonablemente seguro que las partes fundamentales del acto de votar se cumplen.
- Y esto no es fácil de hacer.

# Problemas Prácticos

- A nivel práctico está el problema de la **escalabilidad de las amenazas**:

## Problemas Prácticos

- A nivel práctico está el problema de la **escalabilidad de las amenazas**: en un sistema tradicional, para crear cambios a una escala suficiente para cambiar una elección deben estar involucrados muchos individuos.

## Problemas Prácticos

- A nivel práctico está el problema de la **escalabilidad de las amenazas**: en un sistema tradicional, para crear cambios a una escala suficiente para cambiar una elección deben estar involucrados muchos individuos. En el VE, los individuos necesarios son mucho menos, y un par de líneas de código hábilmente ocultas pueden cambiar cientos de miles de votos.

## Problemas Prácticos

- A nivel práctico está el problema de la **escalabilidad de las amenazas**: en un sistema tradicional, para crear cambios a una escala suficiente para cambiar una elección deben estar involucrados muchos individuos. En el VE, los individuos necesarios son mucho menos, y un par de líneas de código hábilmente ocultas pueden cambiar cientos de miles de votos.
- Además las implementaciones del VE suelen tener fallas tanto evitables (errores en la programación) como estructurales (concepción equivocada).

## Problemas Prácticos

- A nivel práctico está el problema de la **escalabilidad de las amenazas**: en un sistema tradicional, para crear cambios a una escala suficiente para cambiar una elección deben estar involucrados muchos individuos. En el VE, los individuos necesarios son mucho menos, y un par de líneas de código hábilmente ocultas pueden cambiar cientos de miles de votos.
- Además las implementaciones del VE suelen tener fallas tanto evitables (errores en la programación) como estructurales (concepción equivocada).
- Una GARANTÍA de que un sistema propuesto no es seguro es:

## Problemas Prácticos

- A nivel práctico está el problema de la **escalabilidad de las amenazas**: en un sistema tradicional, para crear cambios a una escala suficiente para cambiar una elección deben estar involucrados muchos individuos. En el VE, los individuos necesarios son mucho menos, y un par de líneas de código hábilmente ocultas pueden cambiar cientos de miles de votos.
- Además las implementaciones del VE suelen tener fallas tanto evitables (errores en la programación) como estructurales (concepción equivocada).
- Una GARANTÍA de que un sistema propuesto no es seguro es: que los responsables del mismo digan que es 100% seguro.

# Transparencia

- Cualquier sistema de VE que use “**Seguridad por obscuridad**” debe ser **evitado**.

# Transparencia

- Cualquier sistema de VE que use “**Seguridad por obscuridad**” debe ser **evitado**.
- Se debe disponer de **amplio tiempo** (semanas, como mínimo) para que expertos de todo tipo (y no solo los “expertos designados por los partidos políticos”) puedan **estudiar el sistema**.

# Transparencia

- Cualquier sistema de VE que use “**Seguridad por obscuridad**” debe ser **evitado**.
- Se debe disponer de **amplio tiempo** (semanas, como mínimo) para que expertos de todo tipo (y no solo los “expertos designados por los partidos políticos”) puedan **estudiar el sistema**.
- El **acceso al código** debe ser lo mas **abierto** posible. Muchos expertos consideran que es necesario que sea “open source software” o al menos “disclosed source software”. Si esto no es posible, los *non-disclosure agreements* deben ser tales que los expertos puedan reportar las fallas que encontraron.

# Transparencia

- Cualquier sistema de VE que use “**Seguridad por obscuridad**” debe ser **evitado**.
- Se debe disponer de **amplio tiempo** (semanas, como mínimo) para que expertos de todo tipo (y no solo los “expertos designados por los partidos políticos”) puedan **estudiar el sistema**.
- El **acceso al código** debe ser lo mas **abierto** posible. Muchos expertos consideran que es necesario que sea “open source software” o al menos “disclosed source software”. Si esto no es posible, los *non-disclosure agreements* deben ser tales que los expertos puedan reportar las fallas que encontraron.
- No significa que automáticamente va a ser seguro por ser de código abierto.

# Requerimiento Fundamental

## Requerimiento Fundamental

El votante debe poder estar seguro de que la máquina que crea el voto, no lo revela individualizándolo de alguna forma.

# Requerimiento Fundamental

## Requerimiento Fundamental

El votante debe poder estar seguro de que la máquina que crea el voto, no lo revela individualizándolo de alguna forma.

Ejemplos de individualización de voto:

- Guardar el voto.

# Requerimiento Fundamental

## Requerimiento Fundamental

El votante debe poder estar seguro de que la máquina que crea el voto, no lo revela individualizándolo de alguna forma.

Ejemplos de individualización de voto:

- Guardar el voto.
- Transmitirlo por red.

# Requerimiento Fundamental

## Requerimiento Fundamental

El votante debe poder estar seguro de que la máquina que crea el voto, no lo revela individualizándolo de alguna forma.

Ejemplos de individualización de voto:

- Guardar el voto.
- Transmitirlo por red.
- Correlacionar con alguna secuencia.

# Requerimiento Fundamental

## Requerimiento Fundamental

El votante debe poder estar seguro de que la máquina que crea el voto, no lo revela individualizándolo de alguna forma.

Ejemplos de individualización de voto:

- Guardar el voto.
- Transmitirlo por red.
- Correlacionar con alguna secuencia.

# Requerimiento Fundamental

## Requerimiento Fundamental

El votante debe poder estar seguro de que la máquina que crea el voto, no lo revela individualizándolo de alguna forma.

Ejemplos de individualización de voto:

- Guardar el voto.
- Transmitirlo por red.
- Correlacionar con alguna secuencia.

Esta seguridad debe ser una seguridad **DEL VOTANTE** en el momento de emisión del voto y no que *“los expertos dijeron”, “la auditoría fue buena”, “el presidente de la compañía asegura”, etc.*

## Requerimientos: Protección del Secreto

- La máquina que emite el voto **no debe guardar ningún tipo de información** sobre el voto o el votante. Por lo tanto sistemas de voto electrónico sin boleta (DREs) no deben ser permitidos.

## Requerimientos: Protección del Secreto

- La máquina que emite el voto **no debe guardar ningún tipo de información** sobre el voto o el votante. Por lo tanto sistemas de voto electrónico sin boleta (DREs) no deben ser permitidos.
- La **identificación** del votante debe realizarse en forma **independiente del sistema de emisión de voto**. Sistemas que requieran la lectura de la huella digital o introducir algún código individual para permitir usar la máquina de emisión de votos deben estar prohibidos.

## Requerimientos: Protección del Secreto

- La máquina que emite el voto **no debe guardar ningún tipo de información** sobre el voto o el votante. Por lo tanto sistemas de voto electrónico sin boleta (DREs) no deben ser permitidos.
- La **identificación** del votante debe realizarse en forma **independiente del sistema de emisión de voto**. Sistemas que requieran la lectura de la huella digital o introducir algún código individual para permitir usar la máquina de emisión de votos deben estar prohibidos.
- El sistema debe contar con una protección adecuada contra el *Van Eck Phreaking*. (lectura a distancia del monitor captando las radiaciones electromagnéticas de la pantalla).

## Requerimientos: Emisión del Voto

- El votante debe poder estar razonablemente seguro de que el voto creado por la computadora es el mismo que el quiere crear, o que al menos alguien contará el voto que el quiso crear correctamente. Como en el requerimiento fundamental, esta seguridad debe ser una seguridad DEL VOTANTE y no de los expertos.

## Requerimientos: Emisión del Voto

- El votante debe poder estar razonablemente seguro de que el voto creado por la computadora es el mismo que el quiere crear, o que al menos alguien contará el voto que el quiso crear correctamente. Como en el requerimiento fundamental, esta seguridad debe ser una seguridad DEL VOTANTE y no de los expertos.
- Si bien esto no es posible lograr con un 100% de certeza, sistemas en los cuales el votante pueda verificar lo grabado en el voto con una máquina independiente (y que sea incapaz de sobrescribir los votos) parecen ser mejores que sistemas donde esto no es posible.

## Requerimientos: Conteo de los Votos

- El conteo electrónico debe ser realizado por una máquina físicamente distinta de la máquina que emitió los votos e incapaz de sobrescribir electrónicamente los votos.

## Requerimientos: Conteo de los Votos

- El conteo electrónico debe ser realizado por una máquina físicamente distinta de la máquina que emitió los votos e incapaz de sobrescribir electrónicamente los votos.
- Sistemas en los cuales se imprime en la boleta el voto en forma legible por humanos son mas confiables que sistemas en los cuales el voto no se imprime

## Requerimientos: Conteo de los Votos

- El conteo electrónico debe ser realizado por una máquina físicamente distinta de la máquina que emitió los votos e incapaz de sobrescribir electrónicamente los votos.
- Sistemas en los cuales se imprime en la boleta el voto en forma legible por humanos son mas confiables que sistemas en los cuales el voto no se imprime, **pero si esta impresión nunca se usa para efectivamente contar los votos, es irrelevante.** Por lo tanto:

## Requerimientos: Conteo de los Votos

- El conteo electrónico debe ser realizado por una máquina físicamente distinta de la máquina que emitió los votos e incapaz de sobrescribir electrónicamente los votos.
- Sistemas en los cuales se imprime en la boleta el voto en forma legible por humanos son mas confiables que sistemas en los cuales el voto no se imprime, **pero si esta impresión nunca se usa para efectivamente contar los votos, es irrelevante.** Por lo tanto:
- El voto debe imprimirse en la boleta y:

## Requerimientos: Conteo de los Votos

- El conteo electrónico debe ser realizado por una máquina físicamente distinta de la máquina que emitió los votos e incapaz de sobrescribir electrónicamente los votos.
- Sistemas en los cuales se imprime en la boleta el voto en forma legible por humanos son mas confiables que sistemas en los cuales el voto no se imprime, **pero si esta impresión nunca se usa para efectivamente contar los votos, es irrelevante.** Por lo tanto:
- El voto debe imprimirse en la boleta y:
- En una selección al azar de las urnas efectivamente usadas en la elección se realizará un conteo manual de los votos y se verificará que el conteo coincida con el conteo electrónico.

## Requerimientos: Conteo de los Votos

- Si el número de urnas en las cuales este test falla es mayor que un cierto umbral, el conteo electrónico de todas las urnas debe ser anulado, y se debe realizar el conteo manual de ellas.

## Requerimientos: Conteo de los Votos

- Si el número de urnas en las cuales este test falla es mayor que un cierto umbral, el conteo electrónico de todas las urnas debe ser anulado, y se debe realizar el conteo manual de ellas.
- Un sistema en el cual se fuerze el conteo manual en todas las mesas es preferible, pero nos damos cuenta que no es probable que se apruebe un tal sistema

## Requerimientos: Conteo de los Votos

- Si el número de urnas en las cuales este test falla es mayor que un cierto umbral, el conteo electrónico de todas las urnas debe ser anulado, y se debe realizar el conteo manual de ellas.
- Un sistema en el cual se fuerze el conteo manual en todas las mesas es preferible, pero nos damos cuenta que no es probable que se apruebe un tal sistema, aunque se podría hacer esto en los primeros ensayos de uso del sistema

## Requerimientos: Conteo de los Votos

- Si el número de urnas en las cuales este test falla es mayor que un cierto umbral, el conteo electrónico de todas las urnas debe ser anulado, y se debe realizar el conteo manual de ellas.
- Un sistema en el cual se fuerze el conteo manual en todas las mesas es preferible, pero nos damos cuenta que no es probable que se apruebe un tal sistema, aunque se podría hacer esto en los primeros ensayos de uso del sistema
- En ese caso, se debe asegurar que el sistema realmente fuerze a las autoridades de mesa a realizar el conteo manual antes de poder saber el resultado del conteo electrónico. (por ejemplo, usando criptografía).

## Requerimientos: Boleta

- Si la boleta usa algún registro electrónico del voto, debe haber medidas de protección para evitar que el mismo pueda ser leído y registrado externamente en forma no autorizada.

## Requerimientos: Boleta

- Si la boleta usa algún registro electrónico del voto, debe haber medidas de protección para evitar que el mismo pueda ser leído y registrado externamente en forma no autorizada. (incluyendo el propio votante, para garantizar la no coercibilidad)

## Requerimientos: Boleta

- Si la boleta usa algún registro electrónico del voto, debe haber medidas de protección para evitar que el mismo pueda ser leído y registrado externamente en forma no autorizada. (incluyendo el propio votante, para garantizar la no coercibilidad)
- En el caso de usar criptografía, se debe especificar cómo y quien se encargará de resguardar las claves criptográficas.

## Requerimientos: Boleta

- Si la boleta usa algún registro electrónico del voto, debe haber medidas de protección para evitar que el mismo pueda ser leído y registrado externamente en forma no autorizada. (incluyendo el propio votante, para garantizar la no coercibilidad)
- En el caso de usar criptografía, se debe especificar cómo y quien se encargará de resguardar las claves criptográficas.
- Las boletas no deben tener ninguna forma de identificación (como números en serie) que permita diferenciar una boleta de otra y permita saber quien voto a quien con el simple expediente de contar en que orden se votó.

## Requerimientos: Boleta

- Si la boleta usa algún registro electrónico del voto, debe haber medidas de protección para evitar que el mismo pueda ser leído y registrado externamente en forma no autorizada. (incluyendo el propio votante, para garantizar la no coercibilidad)
- En el caso de usar criptografía, se debe especificar cómo y quien se encargará de resguardar las claves criptográficas.
- Las boletas no deben tener ninguna forma de identificación (como números en serie) que permita diferenciar una boleta de otra y permita saber quien voto a quien con el simple expediente de contar en que orden se votó.
- Nota al margen: la Boleta Única en Papel de Córdoba no cumple este requerimiento pero es algo fácilmente modificable en este caso.

## Requerimientos: Otros

- Se realizará una selección al azar de las máquinas de votación el día de la elección para ser testeadas en frente de téstigos, con una votación falsa en la cual todos los votos queden registrados en forma independiente y luego los resultados verificados.

## Requerimientos: Otros

- Se realizará una selección al azar de las máquinas de votación el día de la elección para ser testeadas en frente de téstigos, con una votación falsa en la cual todos los votos queden registrados en forma independiente y luego los resultados verificados.
- Lo anterior sirve para detectar errores, pero no malicia activa, pues podría haber código que detecte si la máquina esta siendo usada para testeo o no.

## Requerimientos: Otros

- Se realizará una selección al azar de las máquinas de votación el día de la elección para ser testeadas en frente de téstigos, con una votación falsa en la cual todos los votos queden registrados en forma independiente y luego los resultados verificados.
- Lo anterior sirve para detectar errores, pero no malicia activa, pues podría haber código que detecte si la máquina esta siendo usada para testeo o no.
- Es una medida extra de seguridad, pero no es suficiente por si sola.

## Requerimientos: Otros

- Se realizará una selección al azar de las máquinas de votación el día de la elección para ser testeadas en frente de téstigos, con una votación falsa en la cual todos los votos queden registrados en forma independiente y luego los resultados verificados.
- Lo anterior sirve para detectar errores, pero no malicia activa, pues podría haber código que detecte si la máquina esta siendo usada para testeo o no.
- Es una medida extra de seguridad, pero no es suficiente por si sola.
- Debe haber al menos una auditoría independiente del sistema completo, incluyendo el hardware.

# Requerimientos: Autenticación y Gradualidad

- No tiene ningún sentido realizar una auditoría previa del sistema mas revisión del código y la estructura general del mismo si luego no hay garantías que el sistema usado el día de la elección es el mismo que se revisón.

# Requerimientos: Autenticación y Gradualidad

- No tiene ningún sentido realizar una auditoría previa del sistema mas revisión del código y la estructura general del mismo si luego no hay garantías que el sistema usado el día de la elección es el mismo que se revisón.
- Por lo tanto debe haber un mecanismo de autenticación del sistema a ser usado el dia de la elección.

# Requerimientos: Autenticación y Gradualidad

- No tiene ningún sentido realizar una auditoría previa del sistema mas revisión del código y la estructura general del mismo si luego no hay garantías que el sistema usado el día de la elección es el mismo que se revisón.
- Por lo tanto debe haber un mecanismo de autenticación del sistema a ser usado el dia de la elección.
- Internacionalmente se recomienda que cualquier implementación del VE siga un **camino de gradualidad** y experiencias pilotos antes de ser adoptado masivamente.

# Brasil

- DRE.

# Brasil

- DRE.
- Falla en la protección del secreto del voto:

# Brasil

- DRE.
- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.

# Brasil

- DRE.
- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.
  - El sistema de verificación de identidad del votante esta enlazado con la máquina de votación.

# Brasil

- DRE.
- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.
  - El sistema de verificación de identidad del votante esta enlazado con la máquina de votación.
- Uso de algoritmos criptográficos obsoletos.

# Brasil

- DRE.
- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.
  - El sistema de verificación de identidad del votante esta enlazado con la máquina de votación.
- Uso de algoritmos criptográficos obsoletos.
- Vulnerables a amenazas internas.

# Brasil

- DRE.
- Falla en la protección del secreto del voto:
  - Se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes.
  - El sistema de verificación de identidad del votante esta enlazado con la máquina de votación.
- Uso de algoritmos criptográficos obsoletos.
- Vulnerables a amenazas internas.
- Falla en el uso de mecanismos de encriptación.

## Otros países

**Alemania** los sistemas usados hasta ese momento se declararon inconstitucionales.

## Otros países

**Alemania** los sistemas usados hasta ese momento se declararon inconstitucionales.

**Holanda** dejó de usarse en 2007 al probarse que los votos podían ser leídos a varios metros de distancia (en algunas máquinas), y que los programas podían ser alterados.

## Otros países

- Alemania** los sistemas usados hasta ese momento se declararon inconstitucionales.
- Holanda** dejó de usarse en 2007 al probarse que los votos podían ser leídos a varios metros de distancia (en algunas máquinas), y que los programas podían ser alterados.
- EEUU** múltiples errores en diversos estados. En varios se discontinuó el VE.

## Otros países

- Alemania** los sistemas usados hasta ese momento se declararon inconstitucionales.
- Holanda** dejó de usarse en 2007 al probarse que los votos podían ser leídos a varios metros de distancia (en algunas máquinas), y que los programas podían ser alterados.
- EEUU** múltiples errores en diversos estados. En varios se discontinuó el VE.
- India** hackers lograron manipular los resultados con un celular.

## Otros países

- Alemania** los sistemas usados hasta ese momento se declararon inconstitucionales.
- Holanda** dejó de usarse en 2007 al probarse que los votos podían ser leídos a varios metros de distancia (en algunas máquinas), y que los programas podían ser alterados.
- EEUU** múltiples errores en diversos estados. En varios se discontinuó el VE.
- India** hackers lograron manipular los resultados con un celular.
- Irlanda** evaluaron un sistema en elecciones piloto y determinaron que no se podía garantizar la integridad de ninguna elección que usara ese sistema. Costo del experimento: 54 millones de euros.

## Argentina: BUE

- No es DRE sino EBP, en este sentido es mucho mejor que el sistema brasilero. (lo cual no significa que sea bueno)

## Argentina: BUE

- No es DRE sino EBP, en este sentido es mucho mejor que el sistema brasilero. (lo cual no significa que sea bueno)
- Se puede generar mas de un voto.

## Argentina: BUE

- No es DRE sino EBP, en este sentido es mucho mejor que el sistema brasilero. (lo cual no significa que sea bueno)
- Se puede generar mas de un voto.
- El voto puede ser leído por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra o coacción de votos.

## Argentina: BUE

- No es DRE sino EBP, en este sentido es mucho mejor que el sistema brasilero. (lo cual no significa que sea bueno)
- Se puede generar mas de un voto.
- El voto puede ser leído por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra o coacción de votos.
- Los votos no están encriptados.

## Argentina: BUE

- No es DRE sino EBP, en este sentido es mucho mejor que el sistema brasilero. (lo cual no significa que sea bueno)
- Se puede generar mas de un voto.
- El voto puede ser leído por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra o coacción de votos.
- Los votos no están encriptados.
- Las boletas se pueden individualizar.

## Argentina: BUE

- No es DRE sino EBP, en este sentido es mucho mejor que el sistema brasilero. (lo cual no significa que sea bueno)
- Se puede generar mas de un voto.
- El voto puede ser leído por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra o coacción de votos.
- Los votos no están encriptados.
- Las boletas se pueden individualizar.
- La emisora de votos tiene un segundo núcleo de CPU oculto.

## Argentina: BUE

- No es DRE sino EBP, en este sentido es mucho mejor que el sistema brasilero. (lo cual no significa que sea bueno)
- Se puede generar mas de un voto.
- El voto puede ser leído por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra o coacción de votos.
- Los votos no están encriptados.
- Las boletas se pueden individualizar.
- La emisora de votos tiene un segundo núcleo de CPU oculto.
- La máquina que emite los votos, la que los chequea y la que los cuenta es la misma.

## Argentina: BUE

- No es DRE sino EBP, en este sentido es mucho mejor que el sistema brasilero. (lo cual no significa que sea bueno)
- Se puede generar mas de un voto.
- El voto puede ser leído por un celular llevado por el votante con solo acercarlo a la boleta, permitiendo la compra o coacción de votos.
- Los votos no están encriptados.
- Las boletas se pueden individualizar.
- La emisora de votos tiene un segundo núcleo de CPU oculto.
- La máquina que emite los votos, la que los chequea y la que los cuenta es la misma.
- En Buenos Aires no hubo testeo aleatorio de las urnas, pero en Salta si.