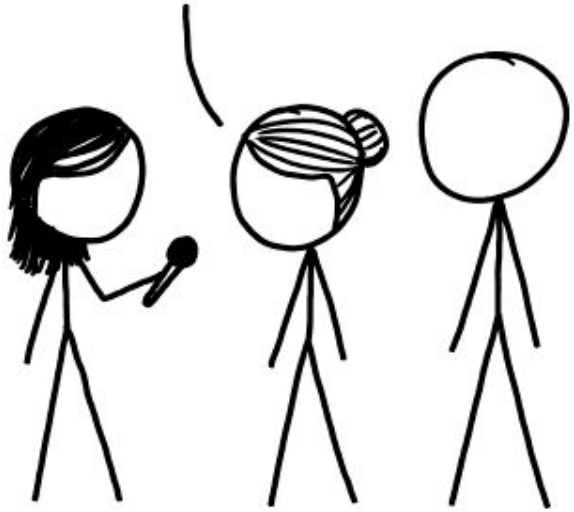
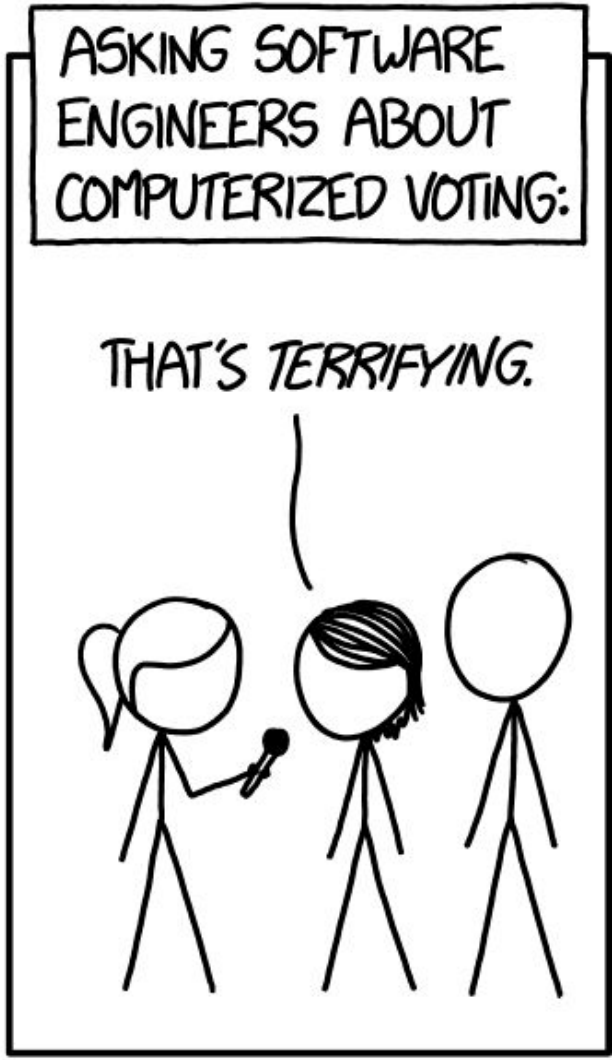
ASKING AIRCRAFT DESIGNERS ABOUT AIRPLANE SAFETY:

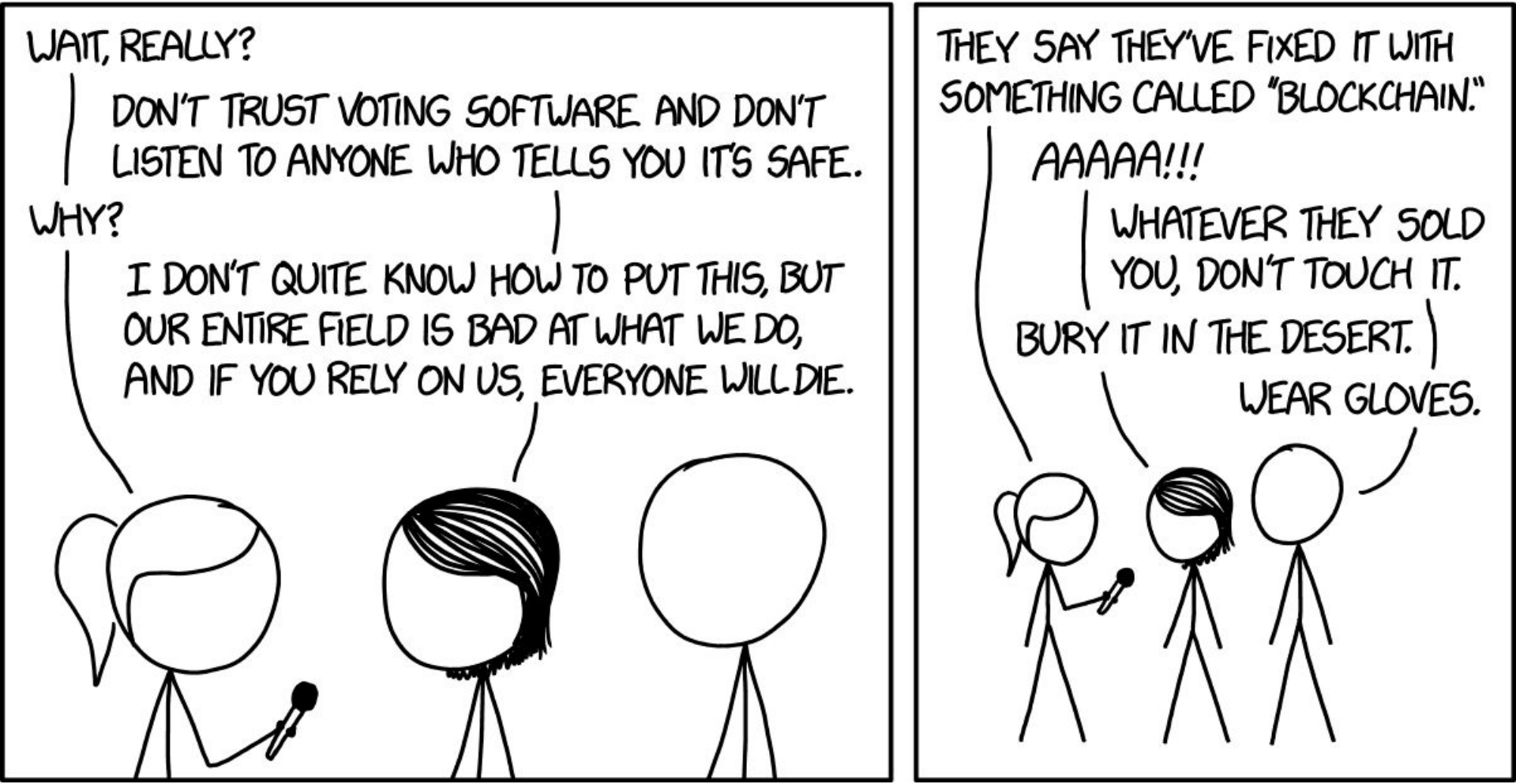
NOTHING IS EVER FOOLPROOF, BUT MODERN AIRLINERS ARE INCREDIBLY RESILIENT. FLYING IS THE SAFEST WAY TO TRAVEL.



ASKING BUILDING ENGINEERS ABOUT ELEVATOR SAFETY:

ELEVATORS ARE PROTECTED BY MULTIPLE TRIED-AND-TESTED FAILSAFE MECHANISMS. THEY'RE NEARLY INCAPABLE OF FALLING.


ASKING SOFTWARE ENGINEERS ABOUT COMPUTERIZED VOTING:
THAT'S TERRIFYING.


WAIT, REALLY?
DON'T TRUST VOTING SOFTWARE AND DON'T LISTEN TO ANYONE WHO TELLS YOU IT'S SAFE.
WHY?
I DON'T QUITE KNOW HOW TO PUT THIS, BUT OUR ENTIRE FIELD IS BAD AT WHAT WE DO, AND IF YOU RELY ON US, EVERYONE WILL DIE.
THEY SAY THEY'VE FIXED IT WITH SOMETHING CALLED "BLOCKCHAIN."
AAAAA!!!
WHATEVER THEY SOLD YOU, DON'T TOUCH IT.
BURY IT IN THE DESERT.
WEAR GLOVES.

FARADAY

The (in)*definite* story behind *not-so*-SmartMatic

...

Charla "*opinacional*" *criolla*

Algo de historia


MINISTERIO DEL INTERIOR
SERVICIO DE ELECCIONES NACIONALES
INSTRUCCIONES

Urna tipo "C"- Elecciones Primarias 2011.
Se utilizan en todos los distritos electorales del país, excepto la provincia de Buenos Aires.


LA UNICA
NO VENDAIS EL VOTO

Locutor transmite resultados (noviembre de 1931).
Fuente: Archivo General de la Nación.

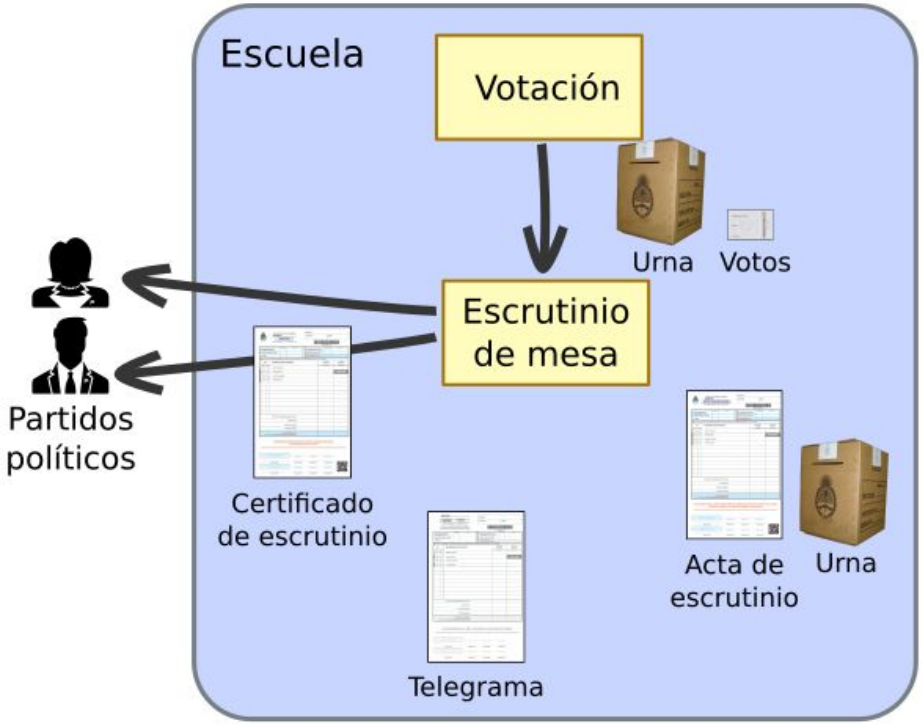
Resultados del escrutinio (abril de 1931).
Fuente: Archivo General de la Nación.

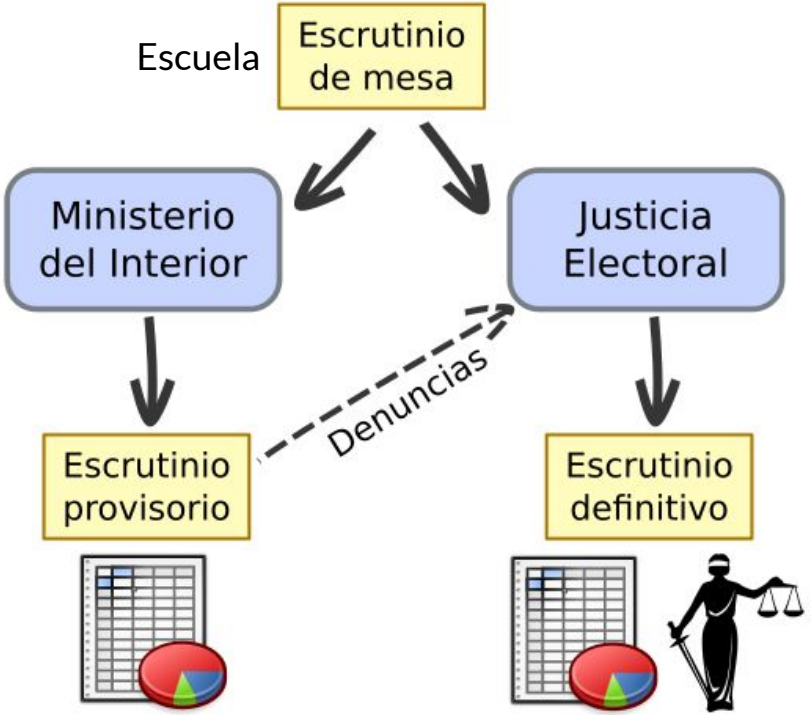
1912 - Ley Sáenz Peña

1946 - Elección Perón

Proceso completo

según Código Electoral Nacional





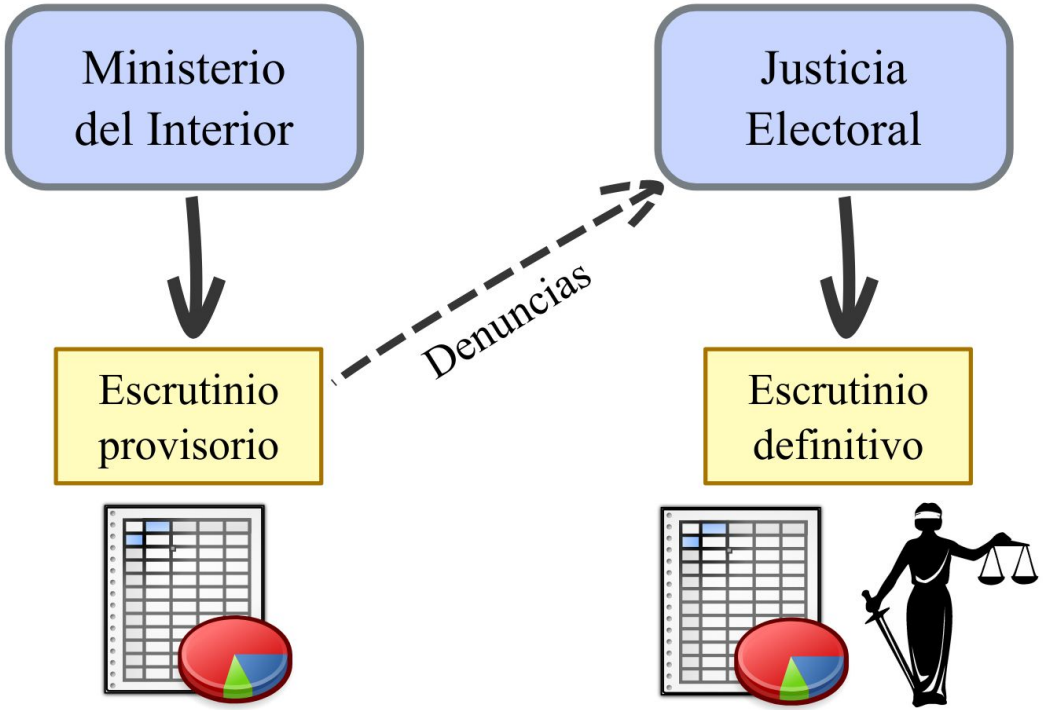
¿Qué es el escrutinio provisorio?
¿y el definitivo?

Escrutinio provisorio

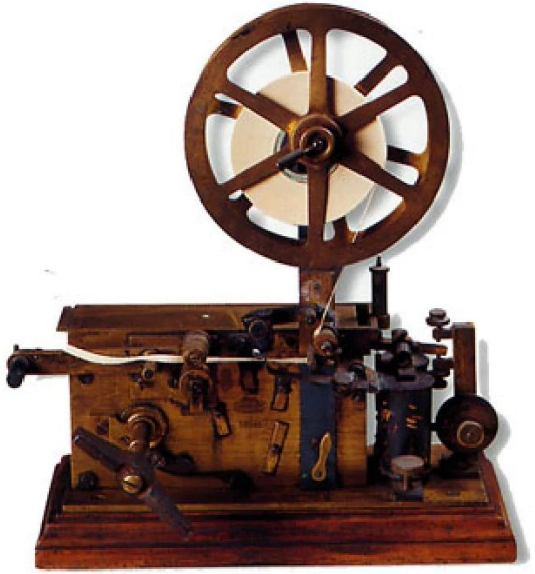
Escrutinio definitivo

Un *poco* más

Telegrama


Ministerio del Interior
Justicia Electoral
Denuncias
Escrutinio provisorio
Escrutinio definitivo

Telegrama

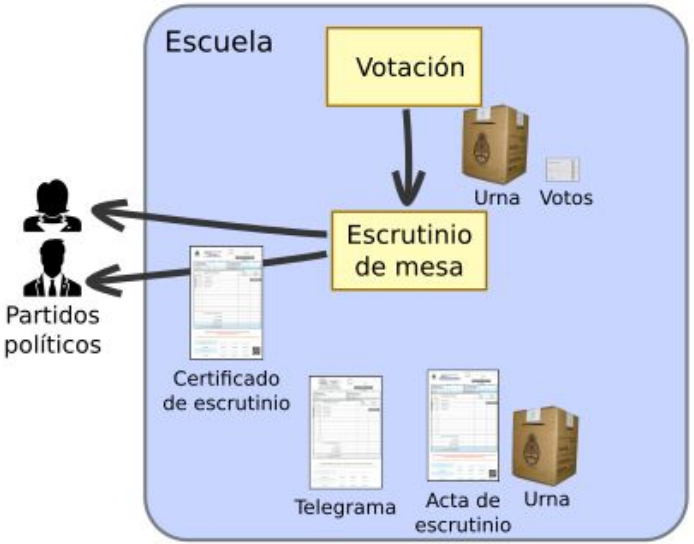


antes - 1997
papel > papel

1997 - 2015
papel > sis. Inf.

2017 - 2019
sis. inf. > sis. inf.

indra


Escuela
Votación
Urna
Votos
Escrutinio de mesa
Partidos políticos
Certificado de escrutinio
Telegrama
Acta de escrutinio
Urna

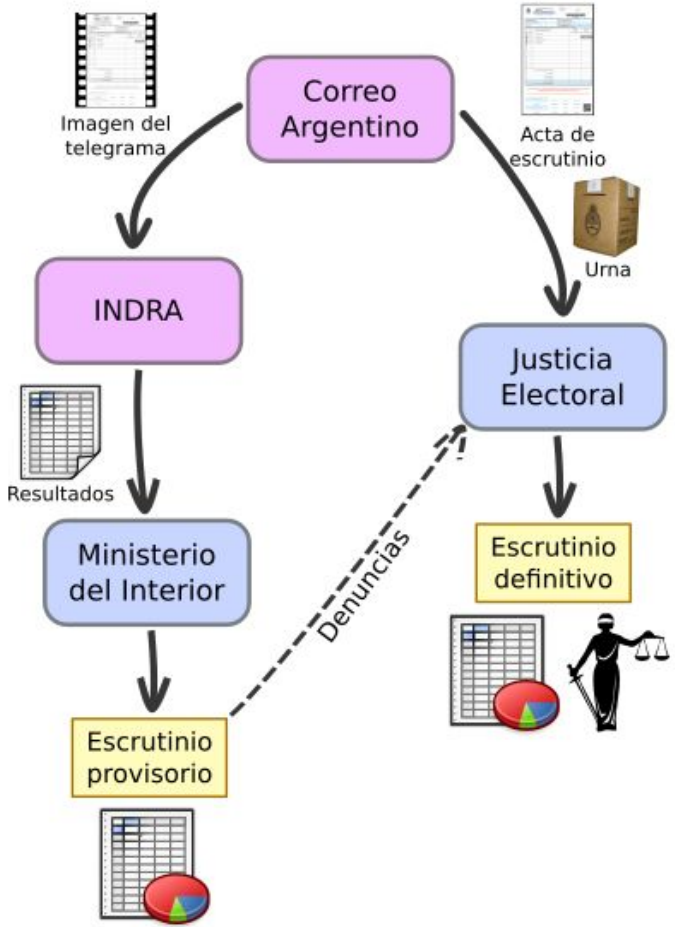


Imagen del telegrama
Correo Argentino
Acta de escrutinio
Urna
INDRA
Justicia Electoral
Resultados
Ministerio del Interior
Escrutinio definitivo
Denuncias
Escrutinio provisorio

Santa Fé

Santa Fé

Sistema nuevo, formato viejo

Nº	NOMBRE DEL OFERENTE	MONTO DE LA OFERTA	POLIZA DE CAUCION MANTENIMIENTO OFERTA 5%
1	INDRA S.I.S.A	USD 19.235.000.- OPCIONAL. USD 384.000.-	USD 1.400.000.-
2	SCYTL SECURE ELECTRONIC VOTING	USD 17.899.042.- ALT. USD 17.471.088.-	USD 820.000.-
3	SMARTMATIC INTERNATIONAL HOLDING B.V. SUCURSAL ARGENTINA	USD 17.093.888.- ALT. USD 17.351.018.-	USD 1.500.000.-

En este acto se recibe, sobre cerrado con copias de los Estados Contables del año 2018 de las Empresas precedentemente enunciadas.

Nº	NOMBRE DEL OFERENTE	PRESENTA SOBRE
1	INDRA S.I.S.A	CUMPLIDO
2	SCYTL SECURE ELECTRONIC VOTING	CUMPLIDO
3	SMARTMATIC INTERNATIONAL HOLDING B.V. SUCURSAL ARGENTINA	CUMPLIDO

2019 Año de la Exportación

ENRIQUE FALCES
CORREO OFICIAL DE LA REP. ARG. S.A.

MARIA DE LOS ANGELES AGUIRRE
DPTO. COMPRAS
CORREO OFICIAL
DE LA REPUBLICA ARGENTINA S.A.

LEANDRO CAPUTO
GERENTE DE ABASTECIMIENTO
CORREO OFICIAL DE LA
REPUBLICA ARGENTINA S.A.

Wohoooo, ¡nos *actualizamos*!

¡Como todos los demás países!

¡Qué *alegría*!

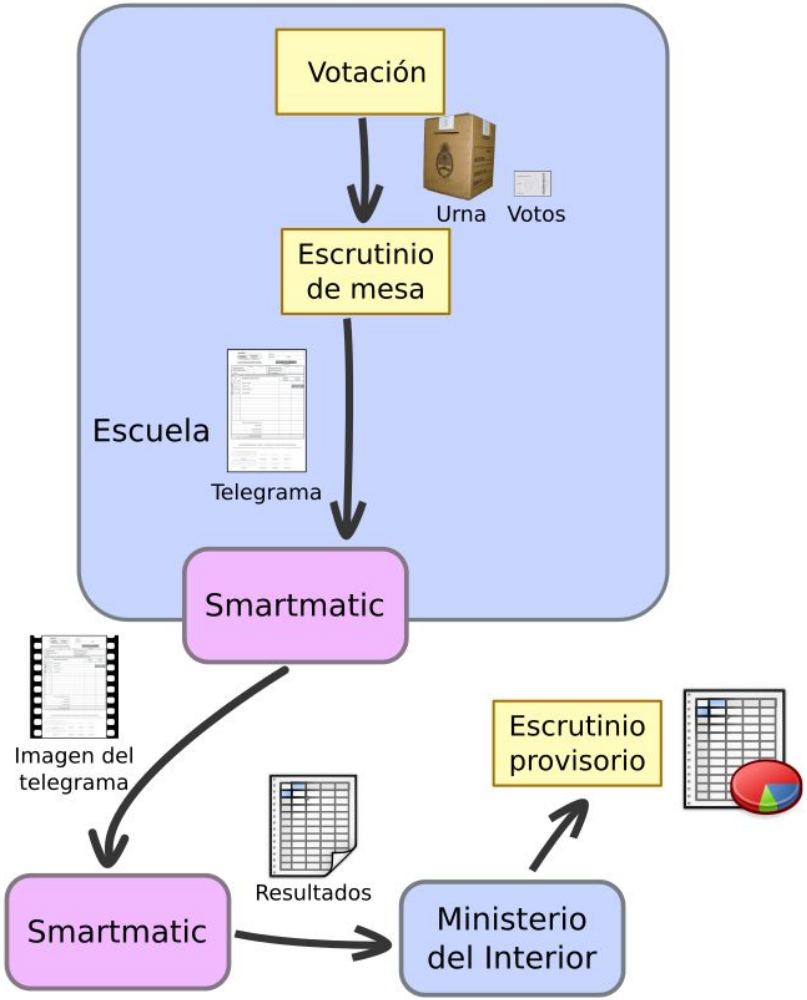
Dijo *nunca*, nadie.

US$1.500.000

AR$90.000.000

No, se *alquiló*.

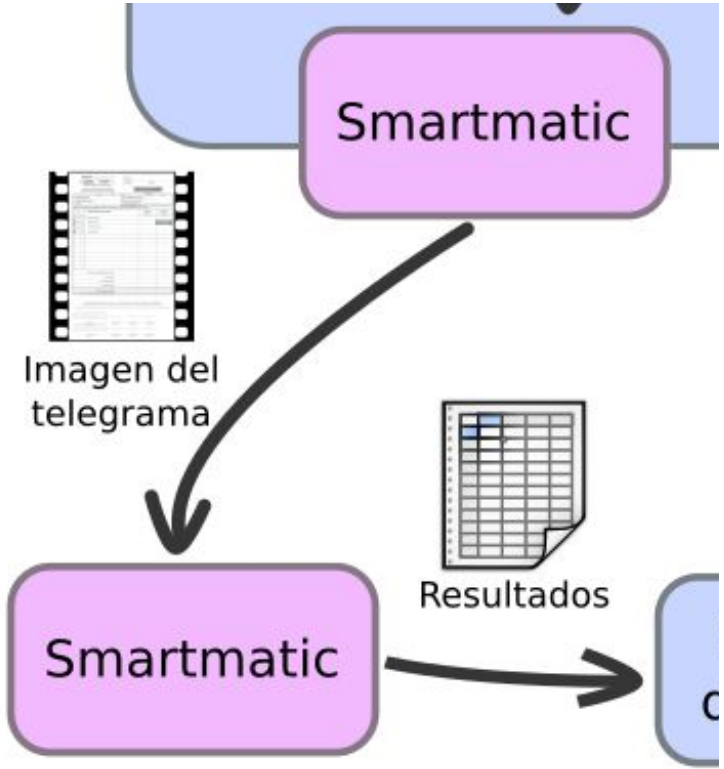
SmartMatic


Votación
Urna
Votos
Escrutinio de mesa
Escuela
Telegrama
Smartmatic
Imagen del telegrama
Escrutinio provisorio
Resultados
Smartmatic
Ministerio del Interior

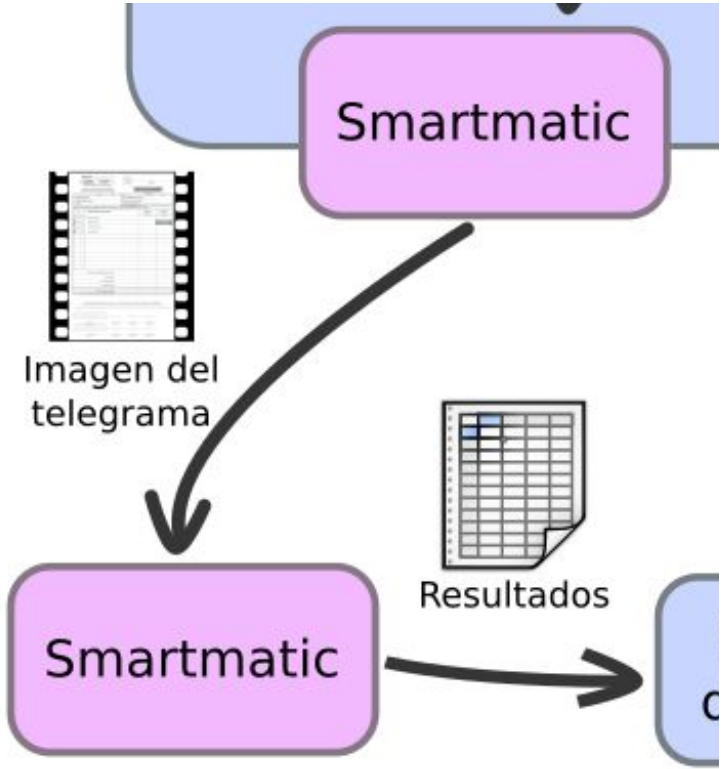
Simulacro

NO.

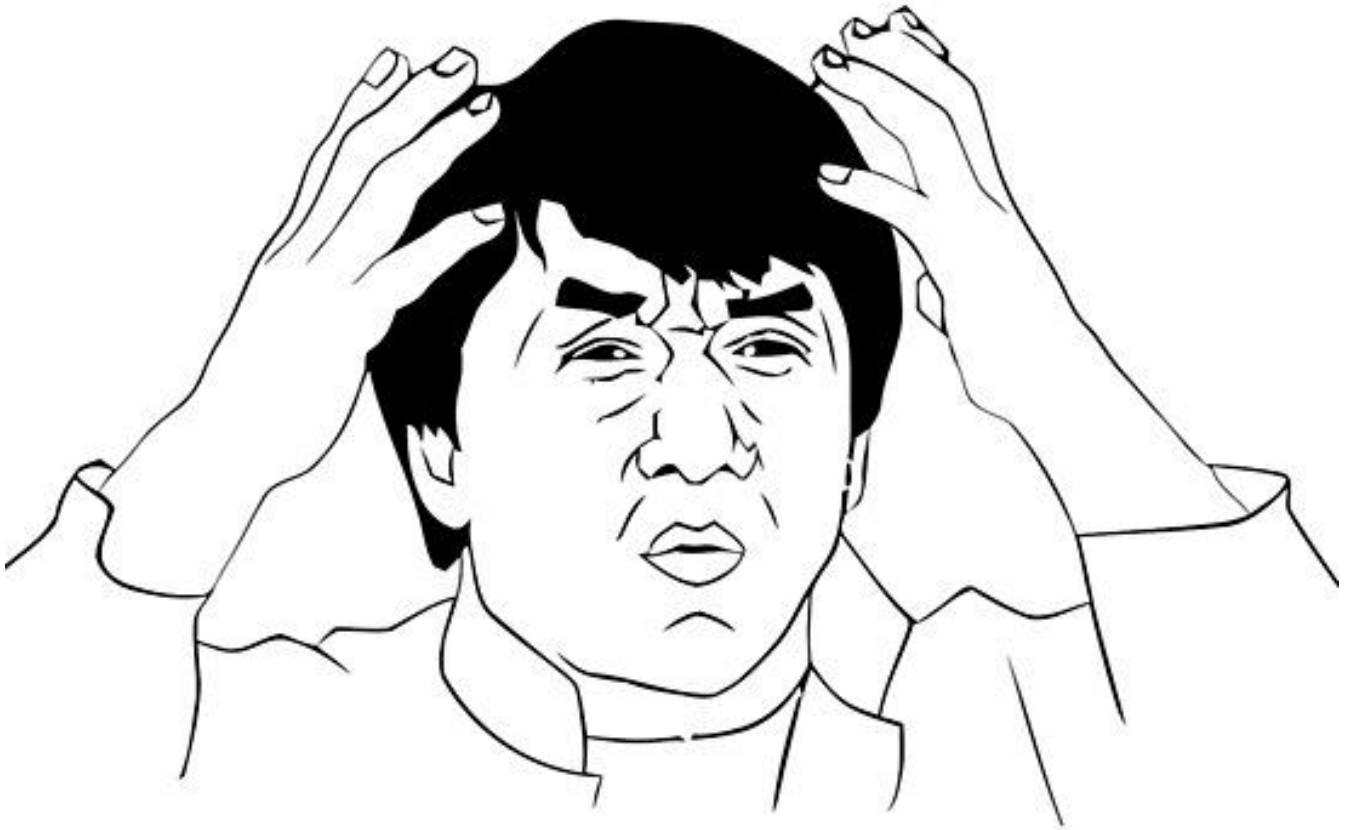
TIFF -> PDF



TIFF?



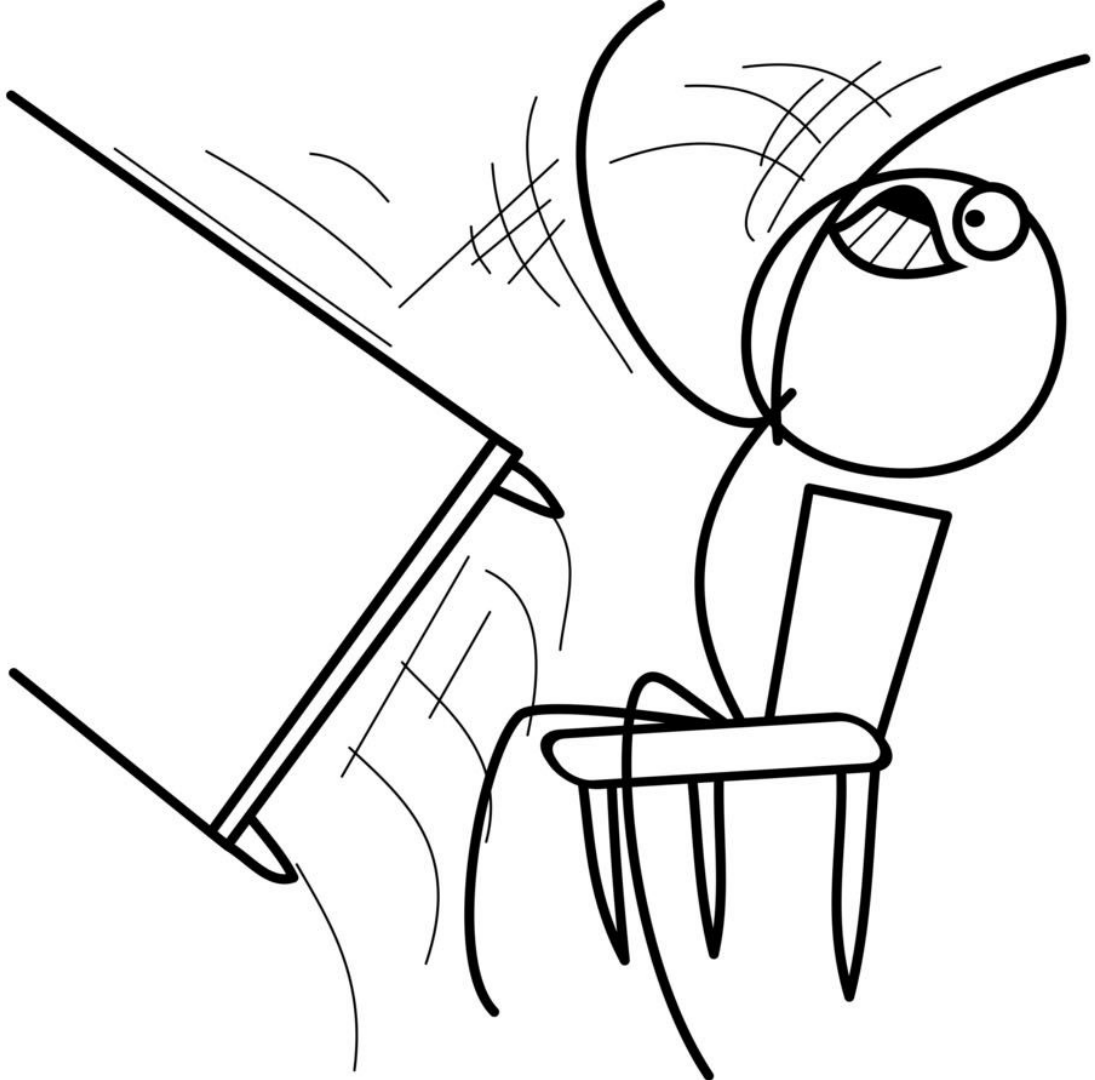
"Porque está hecho así"



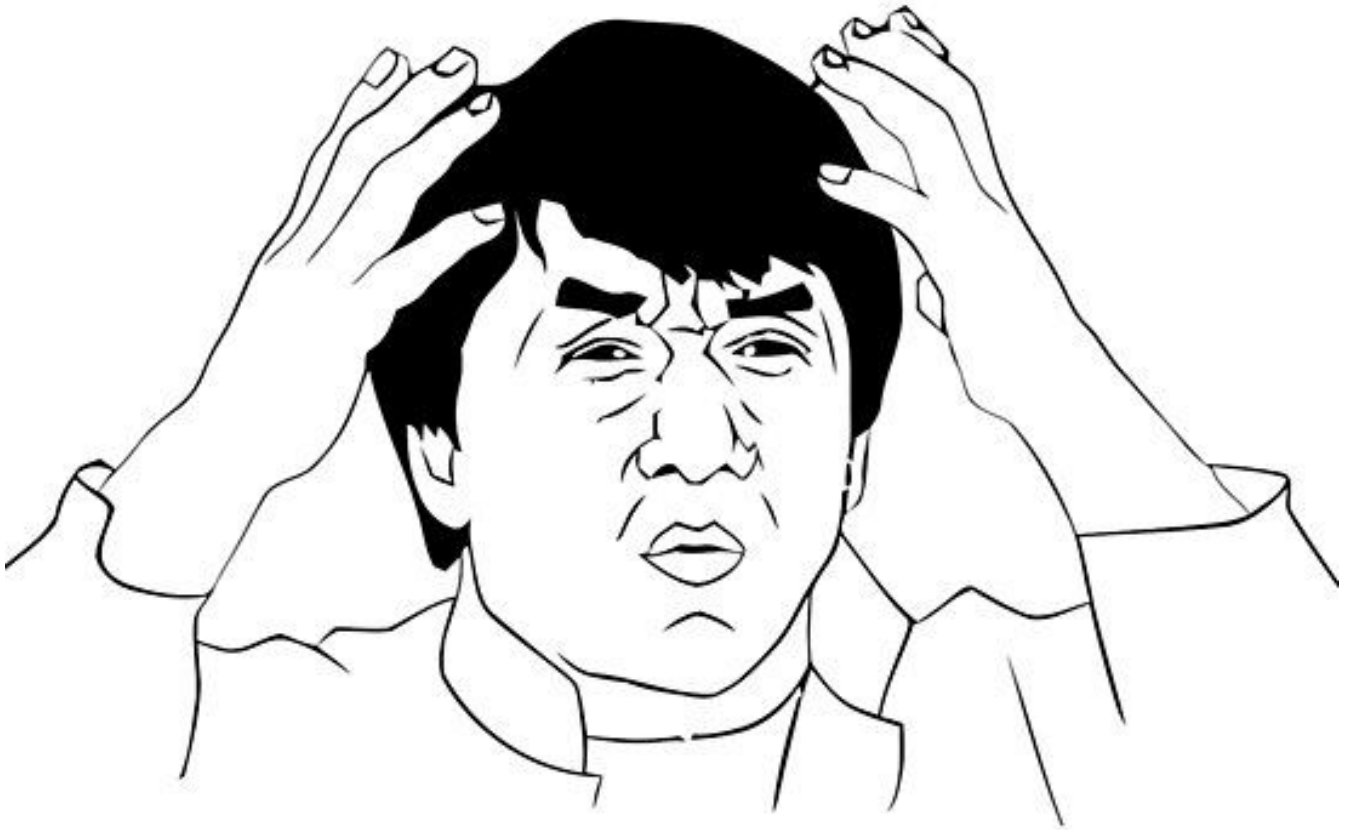
TIFF *vs* PDF

Ok, but *why*?

"Porque está hecho así"



"esa modificación ocurrió siempre, incluso en tiempos del kirchnerismo"



Sí, sí, *exitosamente*..

SIMULACRO 2019

TELEGRAMA

SIMULACRO 2

6200100001X0101

Sección	DEPARTAMENTO CAPITAL
Circuito	LOCALIDAD LA RIOJA (CAPITAL)
Mesa	00001

LA RIOJA

Acta Tipo X - HOJA 01/01

N°	PARTIDO POLÍTICO	LISTA INTERNA	PRESIDENTE Y VICEPRESIDENTE DE LA REPÚBLICA	DIPUTADOS NACIONALES
166	ORG. POLÍTICA 38	LISTA A	22	22
189	ORG. POLÍTICA 05	LISTA A	10	NO USAR
210	ORG. POLÍTICA 39	LISTA A	5	NO USAR
240	ORG. POLÍTICA 60	LISTA A	360	NO USAR
284	ORG. POLÍTICA 25	LISTA A	14	NO USAR
285	ORG. POLÍTICA 26	LISTA A	16	NO USAR
654	ORG. POLÍTICA 21	LISTA A	12	38
288	ORG. POLÍTICA 35	LISTA A	369	NO USAR
656	ORG. POLÍTICA 22	LISTA A	12	40
290	ORG. POLÍTICA 10	LISTA A	10	NO USAR
186	ORG. POLÍTICA 59	LISTA A	NO USAR	5
235	ORG. POLÍTICA 09	LISTA A	NO USAR	28
655	ORG. POLÍTICA 36	LISTA A	NO USAR	35
		VOTOS BLANCOS	47	35
		VOTOS NULOS	94	70
		VOTOS RECURRIDOS	1	1
		VOTOS DE IDENTIDAD IMPUGNADA	3	2
		CANT. COBRES CUBIERTA DEL COMANDO ELECTORAL	5	4
		TOTALES	280	280

PRESIDENTE DE MESA

Apellido y Nombres

Firma | Nro. De Documento

SUPLENTE DE MESA

Apellido y Nombres

Firma | Nro. De Documento

Firma Fiscal Lista:

Firma Fiscal Lista:

Firma Fiscal Lista:

Firma Fiscal Lista:

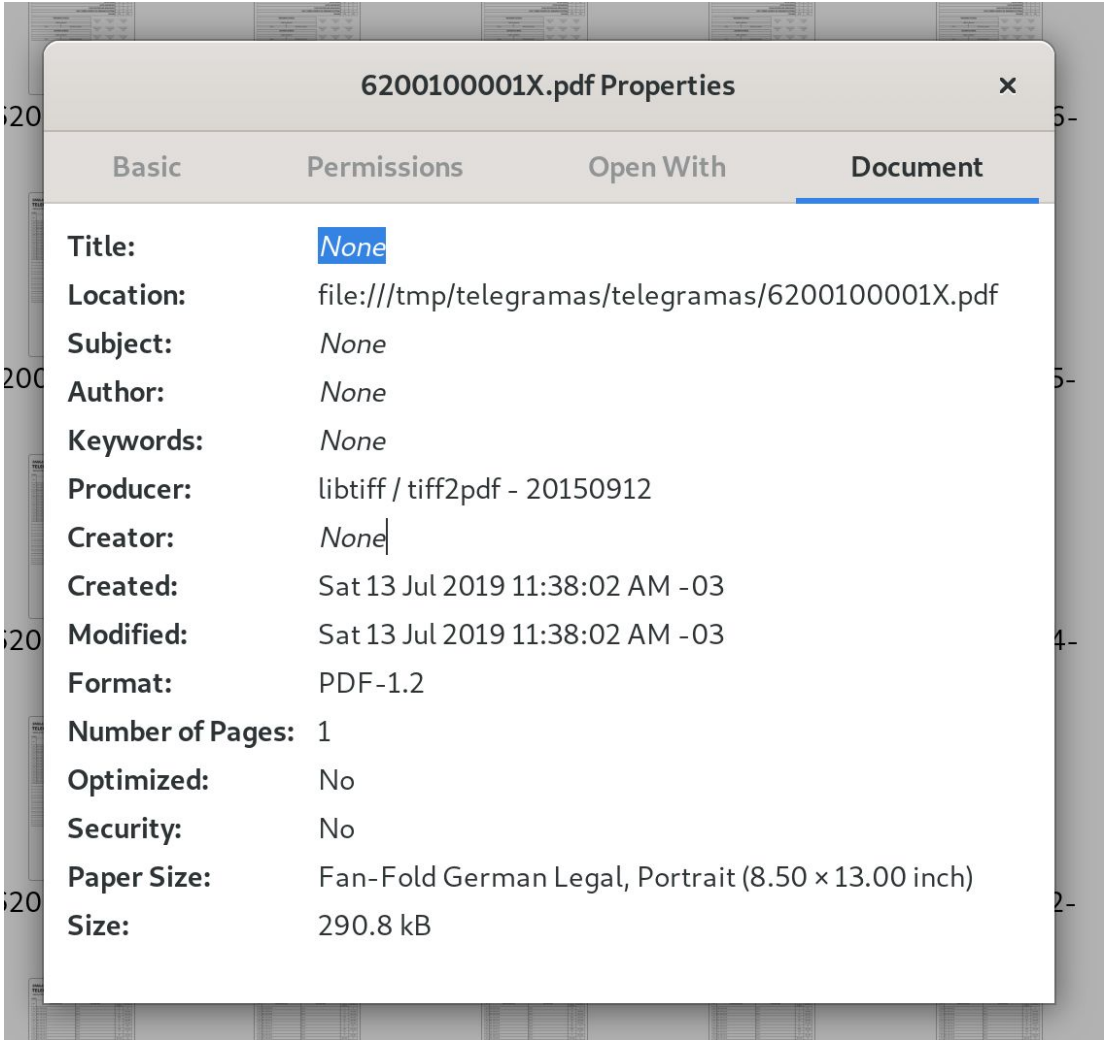
Firma Fiscal Lista:

Firma Fiscal Lista:

Firma Fiscal Lista:

Firma Fiscal Lista:

Firma Fiscal Lista:


6200100001X.pdf Properties
Basic
Permissions
Open With
Document
Title: None
Location: file:///tmp/telegramas/telegramas/6200100001X.pdf
Subject: None
Author: None
Keywords: None
Producer: libtiff / tiff2pdf - 20150912
Creator: None
Created: Sat 13 Jul 2019 11:38:02 AM -03
Modified: Sat 13 Jul 2019 11:38:02 AM -03
Format: PDF-1.2
Number of Pages: 1
Optimized: No
Security: No
Paper Size: Fan-Fold German Legal, Portrait (8.50 × 13.00 inch)
Size: 290.8 kB

```
/tmp/telegramas
➜ pdfinfo telegramas/6200100001X.pdf

Producer: libtiff / tiff2pdf - 20150912
CreationDate: Sat Jul 13 11:38:02 2019 -03
ModDate: Sat Jul 13 11:38:02 2019 -03
...
```

Hablando de fechas..

Created: Sat 13 Jul 2019 11

Modified: Sat 13 Jul 2019 11:


¿Y la justicia?

"...bla bla bla ***componentes de software*** bla bla bla involucrados en los procedimientos de bla bla bla ***deberán ponerse a disposición de las agrupaciones políticas*** que participen en los comicios con la mayor antelación posible y ***al menos treinta (30) días antes*** de la fecha del acto electoral."


Propuesta

¿Qué hace realmente SmartMatic?

Esto *no*

- Impresoras, netbooks, modems.
- Internet. 3 proveedores de telefonía celular.
- Infraestructura de servidores y red.
- Espacio físico, puestos trabajo, computad.
- Servidores resultado escrutinio provisorio.

Esto *sí*

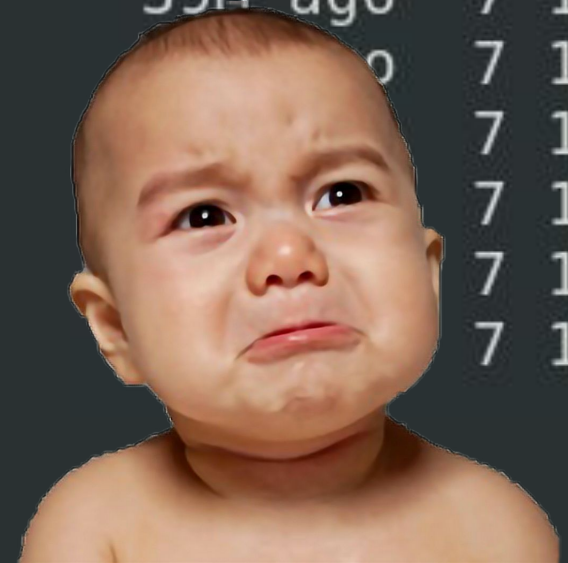
- El software que se ejecuta en las netbooks.
- El software para a los operadores.
- El software que publica los resultados.
- Los operadores de transmisión y carga.

Lo que pasó

PASO

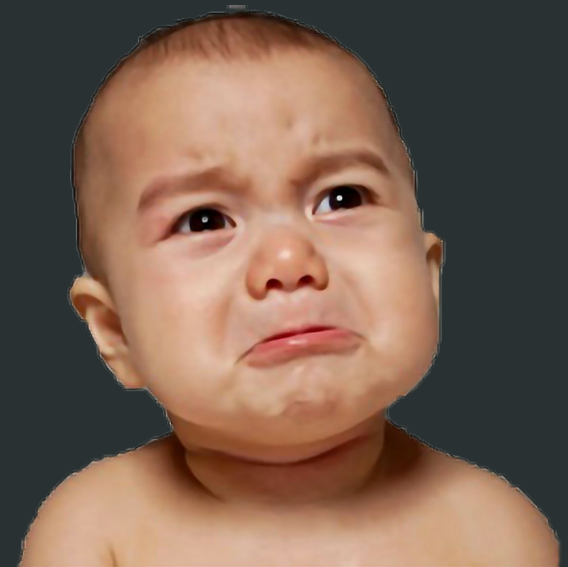
Finalmente entregaron el software

```
811 ago  7 11:00 listado_hash_cnt1.txt.gpg
488 ago  7 11:00 listado_hash_cnt1.txt.gpg.sig
62M ago  7 11:00 rcl.war.gpg
488 ago  7 11:00 rcl.war.gpg.sig
39M ago  7 11:00 SDT_1.0.23-1.0.22.zip.gpg
   o     7 11:00 SDT_1.0.23-1.0.22.zip.gpg.sig
         7 11:00 Smartmatic.SDT.1.exe.gpg
         7 11:00 Smartmatic.SDT.1.exe.gpg.sig
         7 11:00 Smartmatic.SDT.23.exe.gpg
         7 11:00 Smartmatic.SDT.23.exe.gpg.sig
```

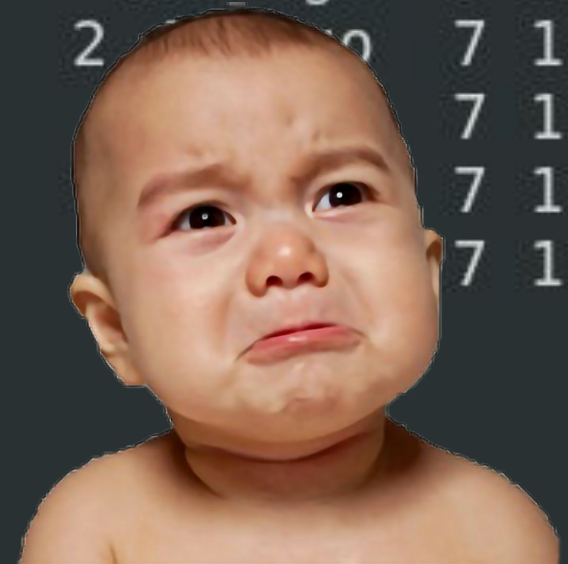


```
$ file rcl.war.gpg.sig
rcl.war.gpg.sig: PGP signature Signature (old)

$ file rcl.war.gpg
rcl.war.gpg: PGP symmetric key encrypted data -
AES with 256-bit key salted & iterated - SHA512
```



```
 61M ago  7 11:00 arg-1901-emp.war.gpg
 488 ago  7 11:00 arg-1901-emp.war.gpg.sig
4,5M ago  7 11:00 arg-1901-listener.war.gpg
 488 ago  7 11:00 arg-1901-listener.war.gpg.sig
2         7 11:00 listado_hash_cnt1_RCT.txt.gpg
          7 11:00 listado_hash_cnt1_RCT.txt.sig
          7 11:00 rct.war.gpg
          7 11:00 rct.war.gpg.sig
```



6.2 Proceso de Validación de firmas

Validar las firmas de los artefactos firmados en el dispositivo con la llave pública fijada en el acta de cadena de custodia

Calcular los digeridos criptográficos con SHA256SUM de todos los artefactos y comparar con los registrados en el acta de cadena de custodia.

6.3 Proceso de Descifrado

Descifrar los artefactos cifrados identificados en el acta de cadena de custodia de evidencia digital utilizando el utilitario GPG #gpg -o file.txt.gpg –symmetric –cipher-algo AES256 file.txt

Colocar los primeros 16 (dieciséis) caracteres Smartmatic y los segundos 16 (dieciséis) caracteres del Correo Argentino


No tenés vulnerabilidades
Si realmente nunca
te auditan

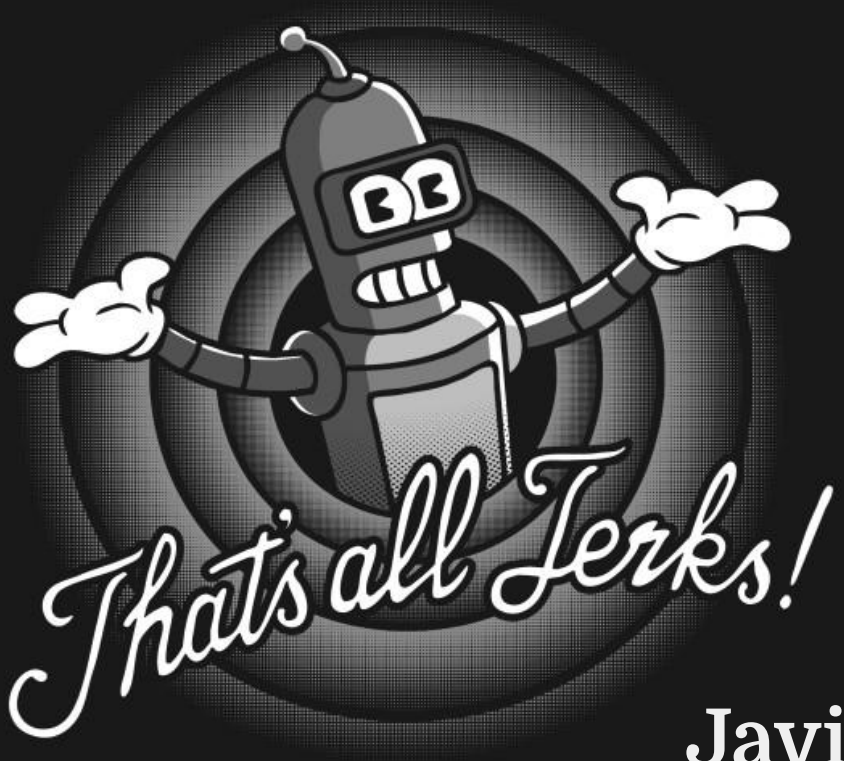
Respuesta de la DNE

"Con respecto a la posibilidad de que cualquier equipo se pueda conectar al ***sistema***, cabe aclarar que el mismo ***cuenta con los niveles de seguridad adecuados para el proceso requerido.***"

ke

FARADAY

Iván Arce
@4Dgifts



Javier Smaldone
@mis2centavos

¡Unite!

Meetup TandilSec

slack tandilsec.slack.com

twitter @TandilSec

Gmail aereal@gmail.com

GitHub @mattaereal/seginfoFAQ

Matías A. Ré Medina
Security Researcher
@mattaereal

¿Acaso *queremos* como sociedad, el confort y la conveniencia de una *integración digital invisible*, tecnológicamente *en incremento*, lo suficiente como para pagar esos beneficios con las *libertades* que deben ser *sacrificadas* para estar protegidas de las desventajas de dicha integración?

Dan Geer.