



Ciberseguridad y Forense:

¿Qué estamos perdiendo?

Andrés Velázquez, CISSP, GCFA, IEM
Presidente / Fundador - MaTTica
@cibercrimen





**Cyber
security**



Shift

Caminos utilizados por los atacantes

+85% de las organizaciones han sufrido fugas de datos debido a Adware, malvertising o sitios web comunes.

Facebook y JavaScript

son los principales canales que utilizan los atacantes para ingresar a la red de las organizaciones.

\$34 millones de USD al año, son las ganancias que los ataques directos de cibercriminales obtienen tan solo en ransomware.

+221% creció el número de dominios de WordPress utilizados por los delincuentes entre febrero y octubre de 2015.

92% del malware conocido ha utilizado DNS como una llave de entrada, el 68% de las empresas no lo monitorean.

Monitoraggio



A problem has been detected and Windows has been shut down to prevent damage to your computer.

The problem seems to be caused by the following file: asyncmac.sys

SESSION5_INITIALIZATION_FAILED

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x530a0936 (0x77a8c321,0x4e2fef9a,0x2e5f507b,0x0a4db40f)

*** asyncmac.sys - Address 0x03ec4c4a base at 0x40c0f69b, DateStamp 6aa338c1



Data Loss Prevention's **MOST WANTED**

Data security is a top concern for global businesses. With an average worldwide cost of \$136 USD per exposed data record¹, organizations can't afford to let sensitive information leave their corporate network.

name: Suzy
dept: Payroll



Handles sensitive information

name: Bob
dept: Accounting



Handles sensitive information

name: Michelle
dept: Human Resources



Handles sensitive information



Almacenemos TODO!

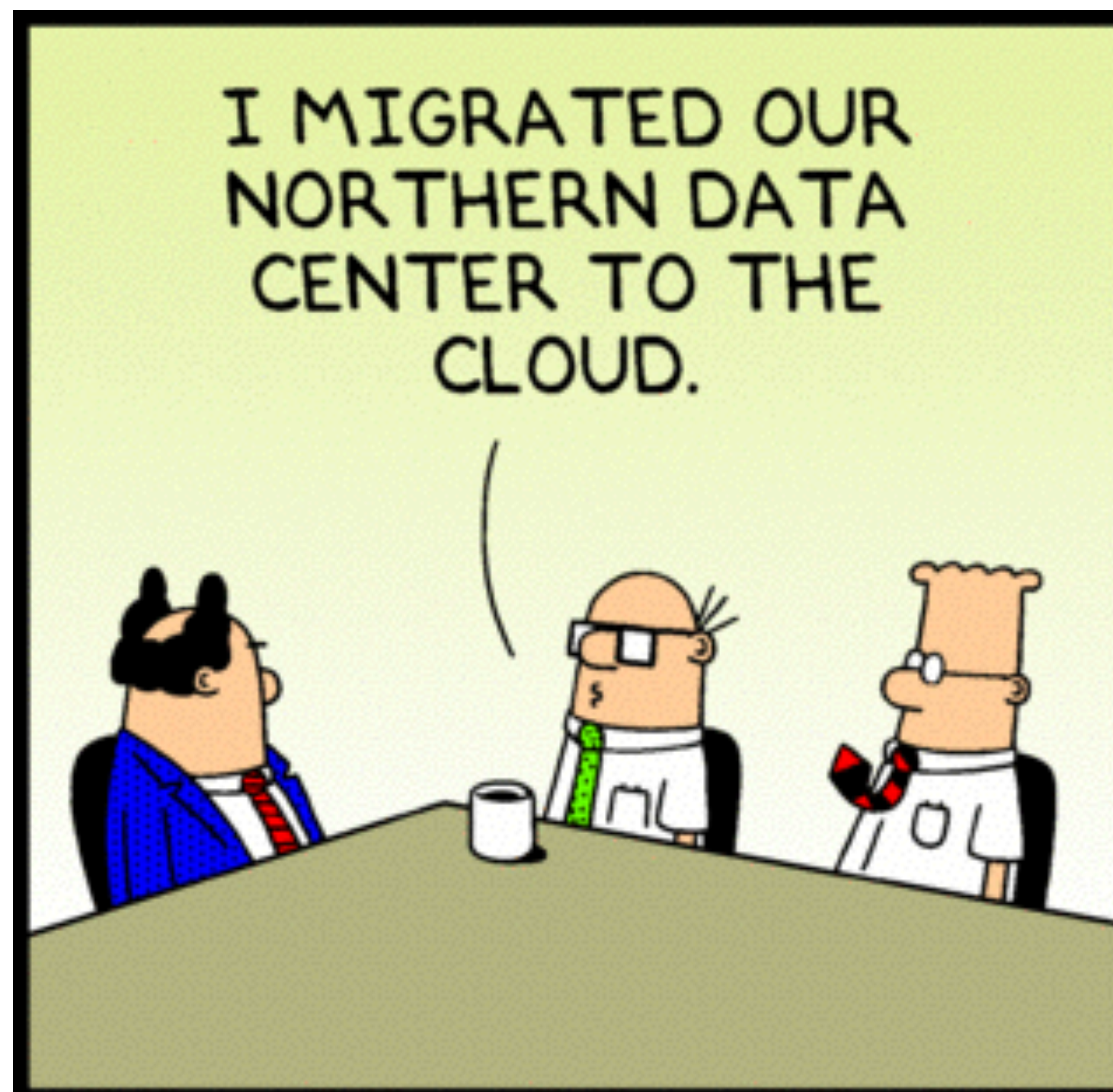
Find it?...

Nope.

**Mejor aún,
vámonos a la nube!!**



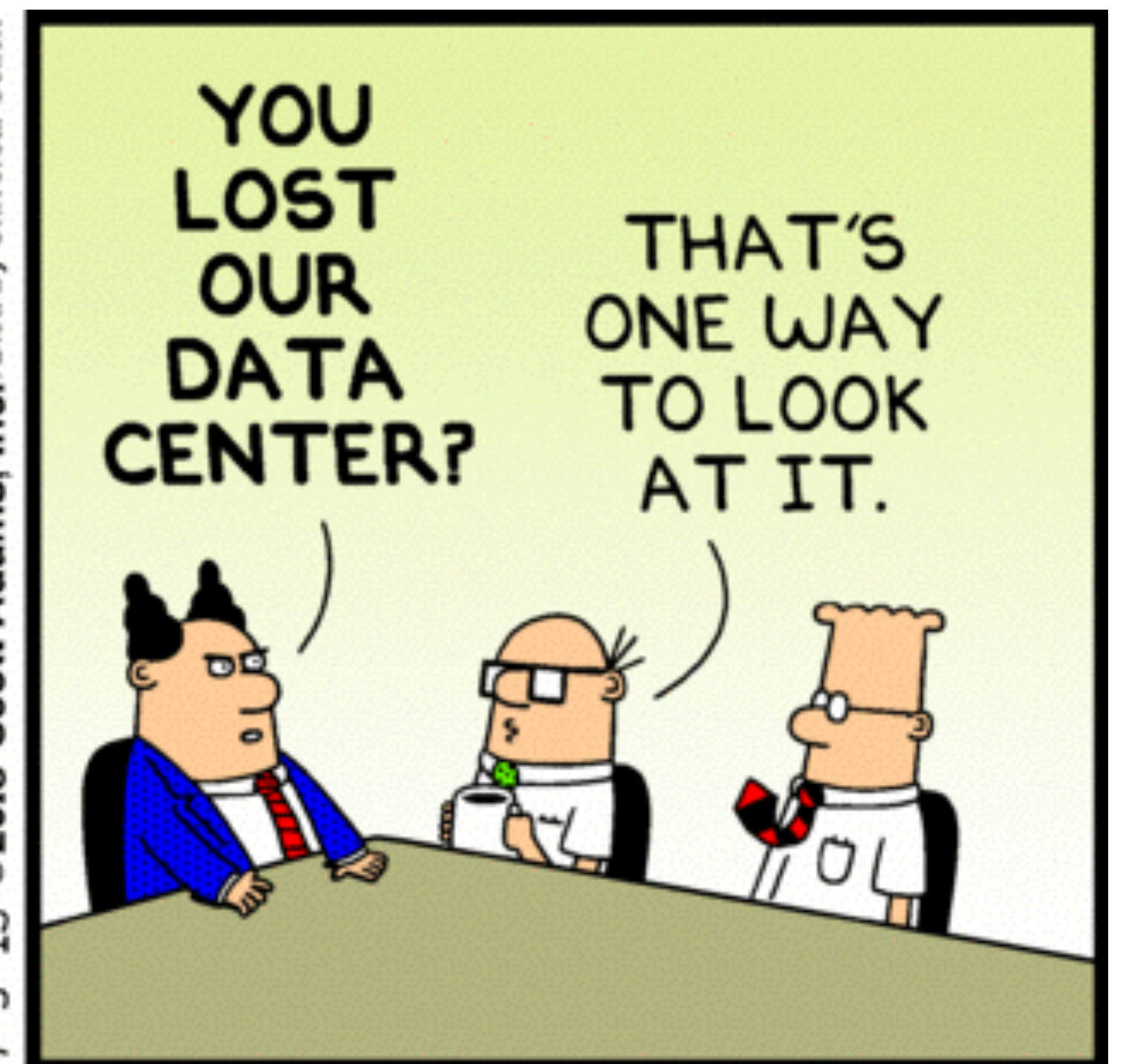
¿Cuáles son los retos de la nube?



Dilbert.com DilbertCartoonist@gmail.com



7-5-13 ©2013 Scott Adams, Inc./Dist. by Universal Uclick



VIRUS

CRACKER

INTRUDER

SPYWARE

PASSWORD

IDENTITY

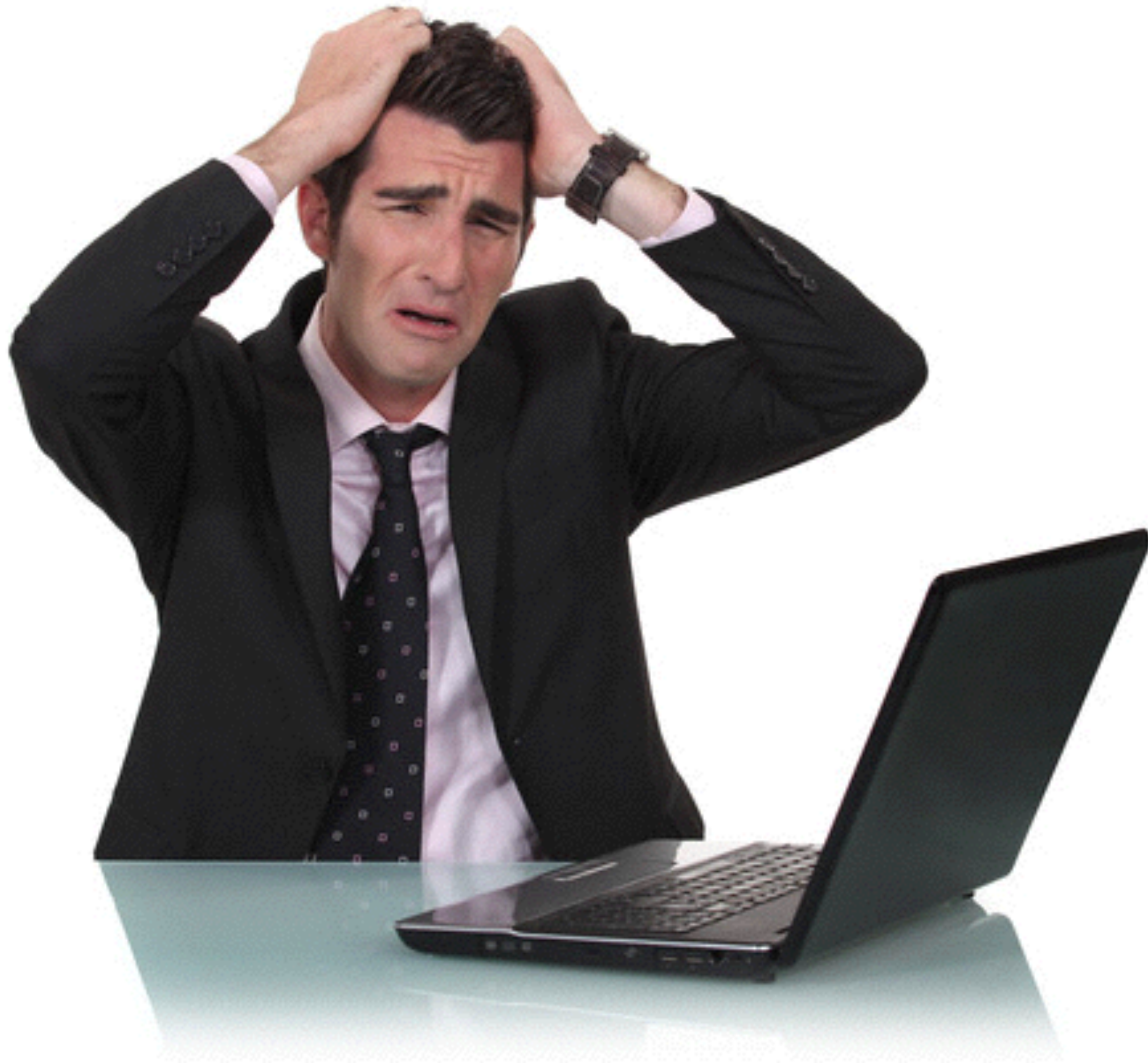
CODE

UNSAFE

HACKER

THEFT

Y aún así....Tenemos un INCIDENTE!!



¿Qué hago ante un
incidente?

¿A quién involucro?

¿Cómo trabajamos?

¿A quién le grito?

¿A quién le aviso?

¿Quién fue?

¿A quién le hablo?

Nos peleamos Nos gritamos Nos echamos la culpa

- Estamos tan mal acostumbrados a la operación, perdiendo la oportunidad de innovar y prepararnos contra los nuevos retos.
- No conocemos nuestra infraestructura
- No sabemos qué hacer ante un incidente
- No sabemos a quién llamar ante un incidente
- No sabemos a quién involucrar
- No sabemos la repercusión legal





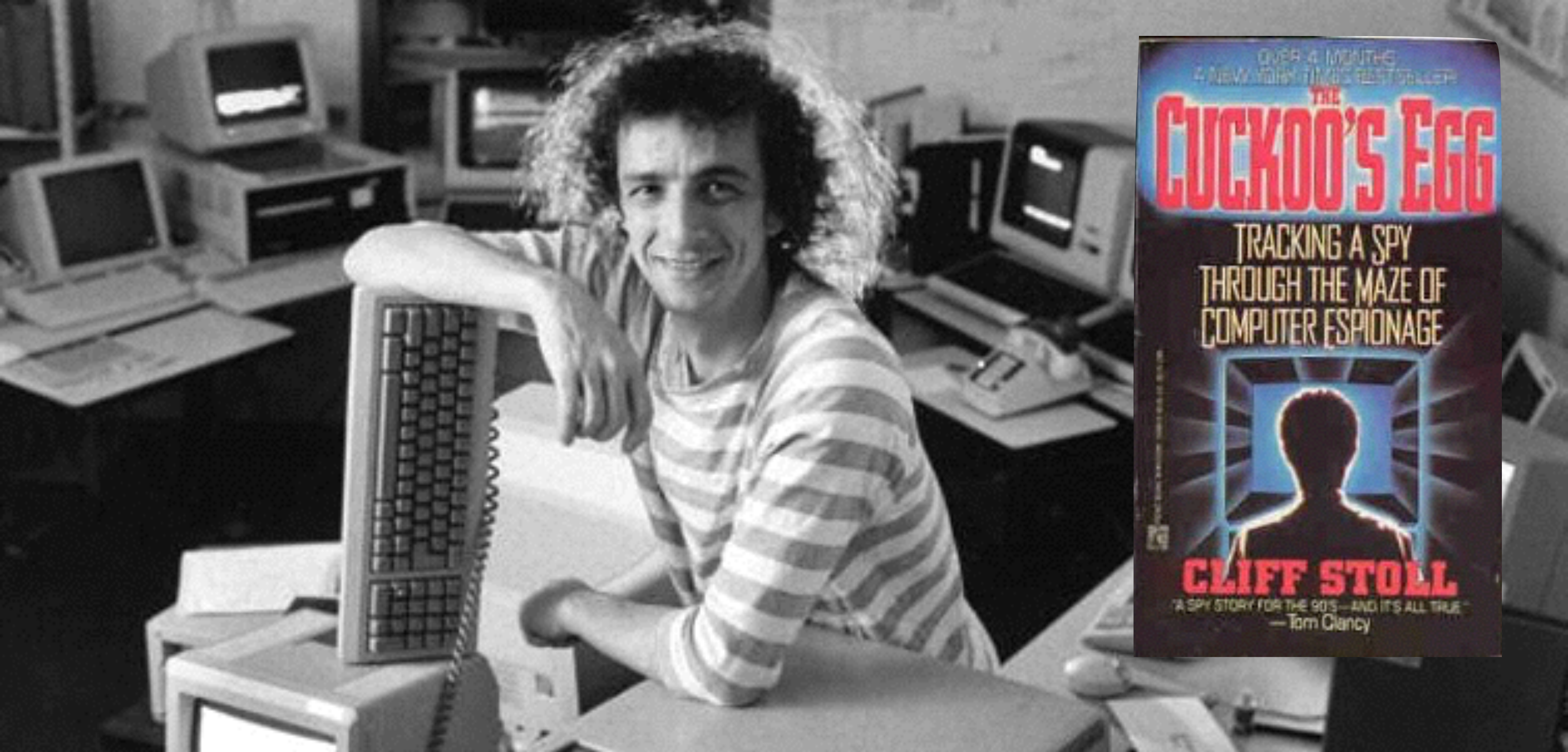
**¿Qué está pasando
en el medio?**

Cómputo Forense



¿Para qué investigar ante un incidente?





Cliff Stoll, Berkley University

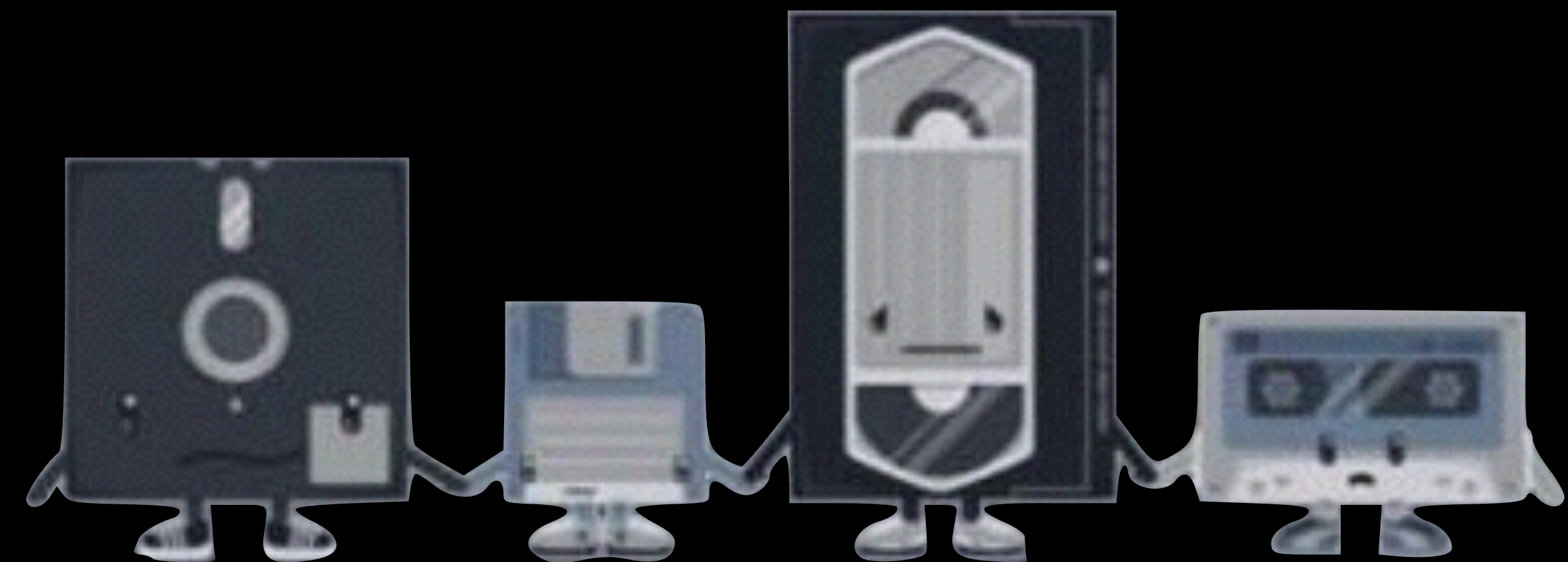
La Tecnología ha cambiado mucho...



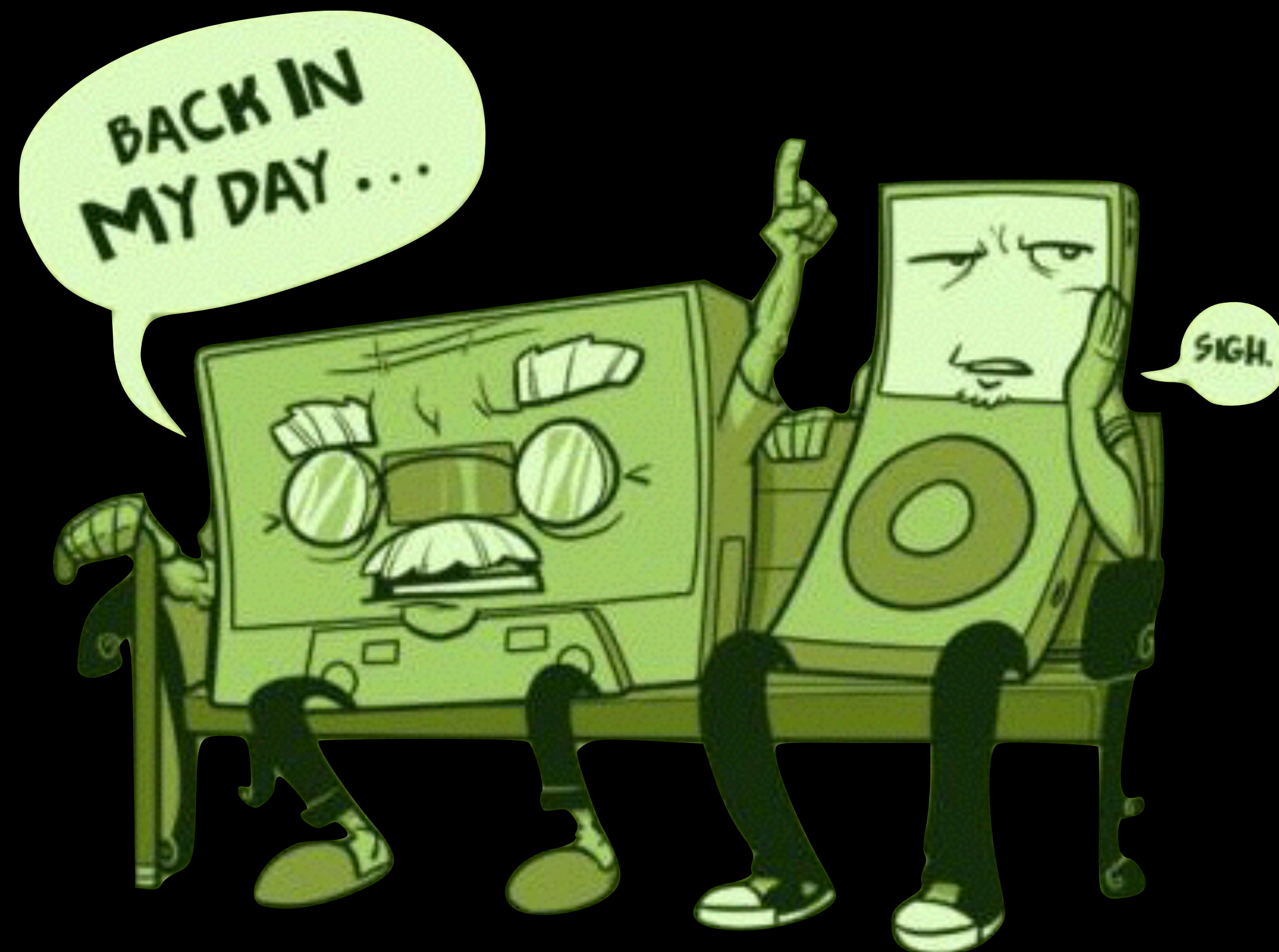
El Gran Invento:

EI GRAN

Teléfono Celular!



NEVER FORGET





Este era un Disco Duro de Platos

**Hay más dinero en “medios digitales”
que en papel moneda**



**¿Es un problema
de tecnología?**





¿Somos
los usuarios?

¿Es un problema de leyes?



Perfilar:

- A partir de acciones**
- A partir de hallazgos**
- A partir de información compartida**
- A partir de elementos externos**



Son las personas las que comenten acciones que nos afectan en nuestra red y no las computadoras

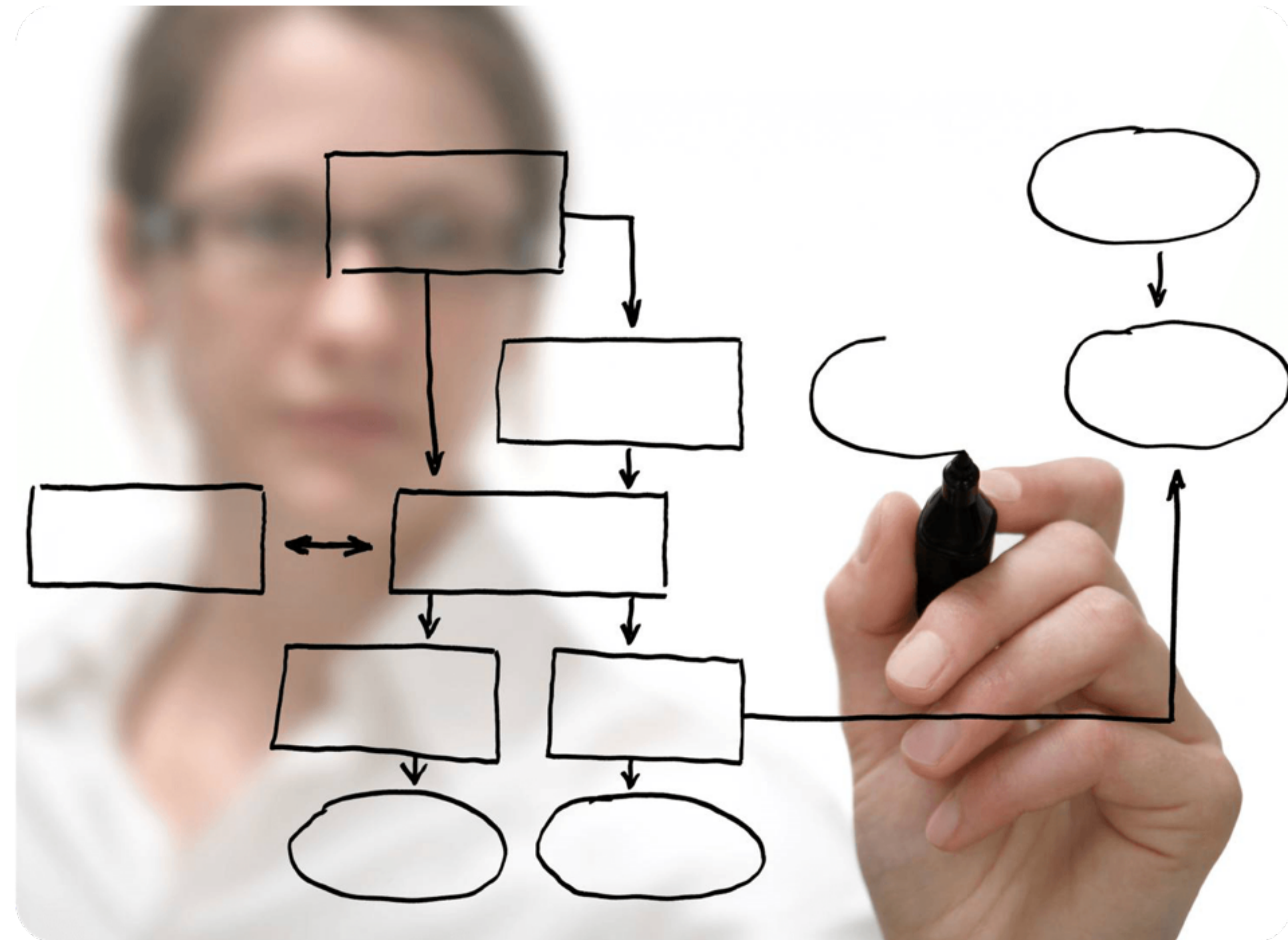


**Las personas mienten,
las computadoras o
sus celulares no**



Recuerde: Ante un incidente...

- Mantener la operación
- No olvidar dejar huellas (documentar)
- Investigar
- Identificar siguientes pasos
- Realizar iniciativas
- APRENDER DE LO QUE SUCEDIÓ
- Créale más a la computadora que a las personas!



Conclusiones

Prevenir

Reaccionar

Esperar

No hacer nada

Crear Equipos

Reflexionar

Ingenieros y Abogados

CEO's

¿Y qué estamos haciendo por los más pequeños?





**No todo el Internet
es malo**



Cliff Stoll, Monterey, CA - 2011



Andrés Velázquez, CISSP, GCFA, IEM

Presidente y Fundador de MaTTica

www.mattica.com



@cibercrimen



Andres Velazquez

Blog:

www.andresvelazquez.com



Podcast: Crimen Digital

www.crimendigital.com

