



# MacroS@guridad

MAYORISTA EN SOLUCIONES DE SEGURIDAD INFORMATICA

## Diego Laborero

TICAR – San Luis  
2do. Encuentro de Firma Digital

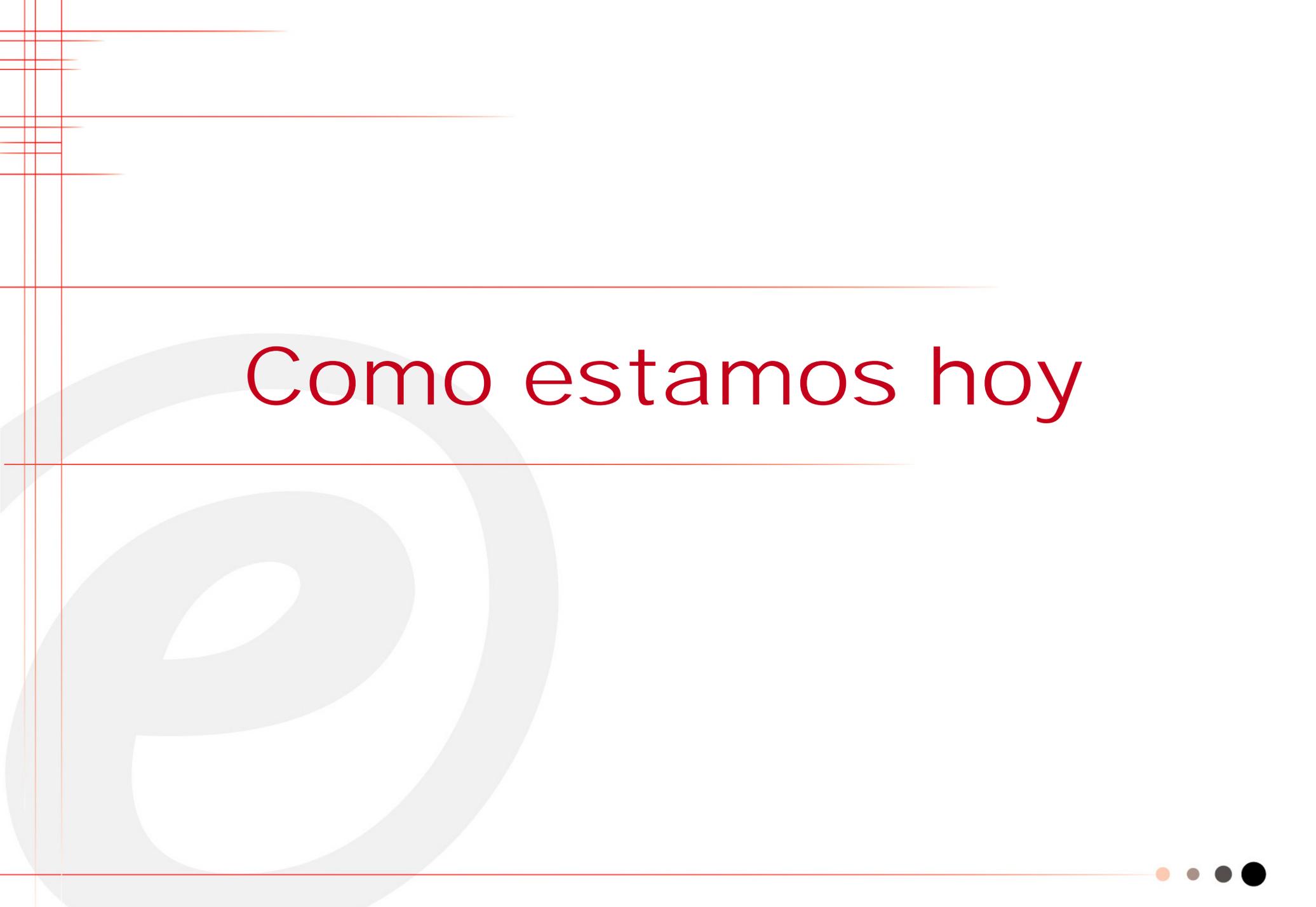
abril de 2015



# El ABC en proyectos de Firma Digital Macroseguridad.org

**Diego Laborero**  
Macroseguridad.org  
**Regional Product Manager**  
Latino America, Mexico y Caribe





Como estamos hoy

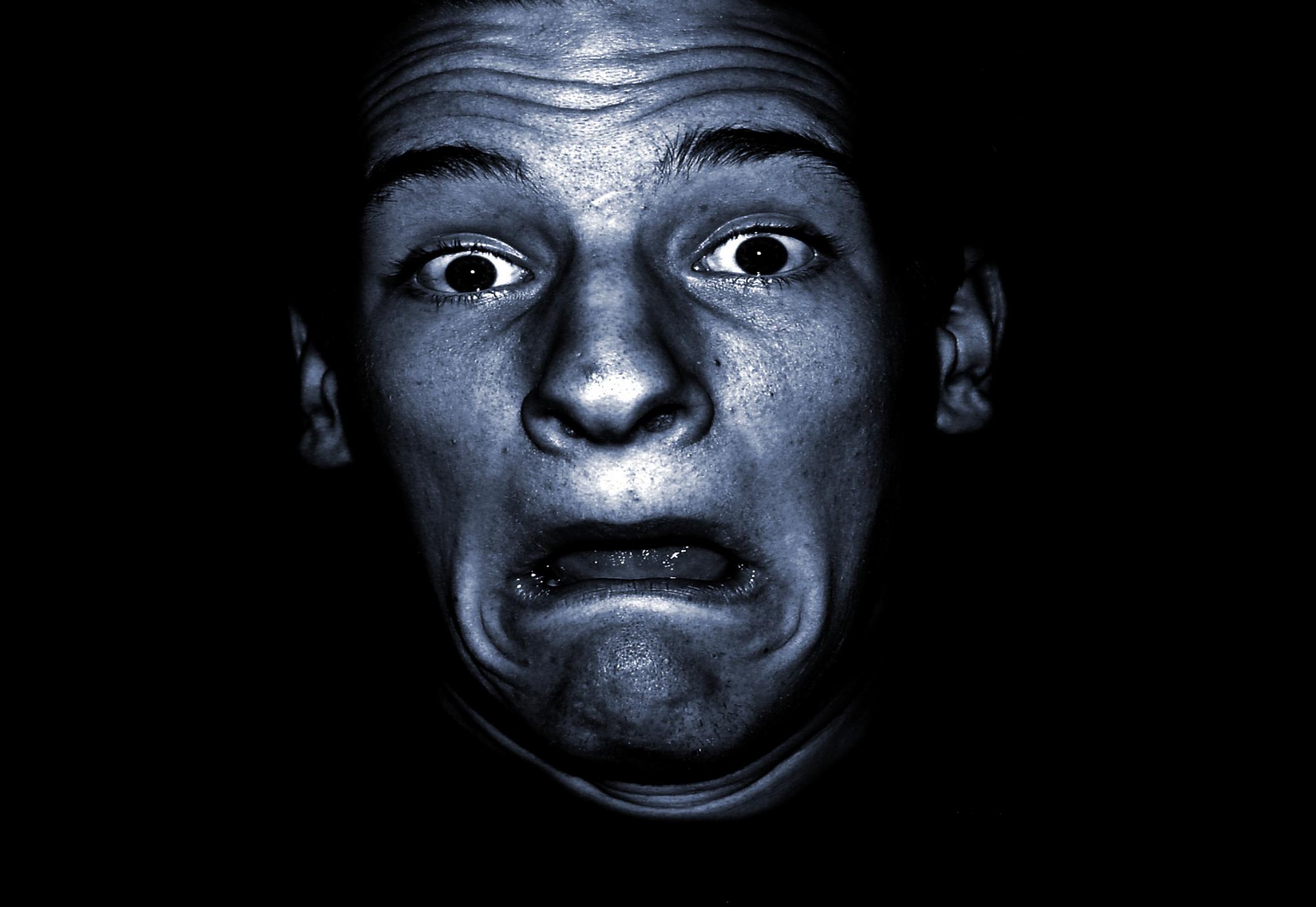






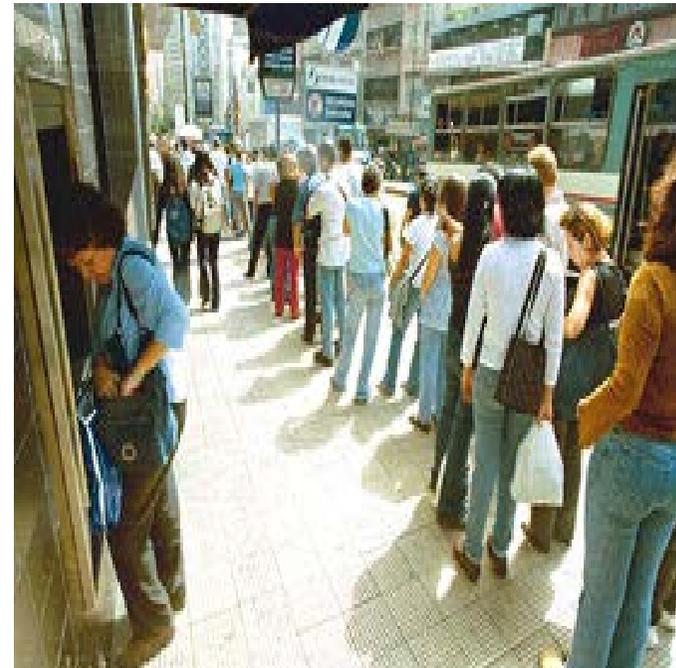
The Plan is no Plan





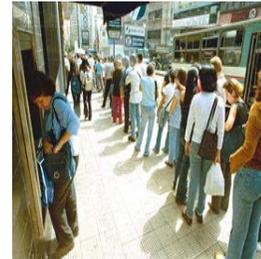
# Pasos básicos necesarios

- Decisión administrativa interna – resolución de una autoridad
- La firma como medio no como fin (ej. papel – Correo – DNRPA)



# Pasos básicos necesarios

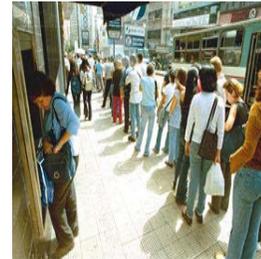
- Decisión administrativa – resolución de una autoridad
- La firma como medio no como fin (ej. papel – Correo – DNRPA)



- Que cuesta no usarla?
  - Procesos Físicos (idas y vueltas)

# Pasos básicos necesarios

- Decisión administrativa – resolución de una autoridad
- La firma como medio no como fin (ej. papel – Correo – DNRPA)



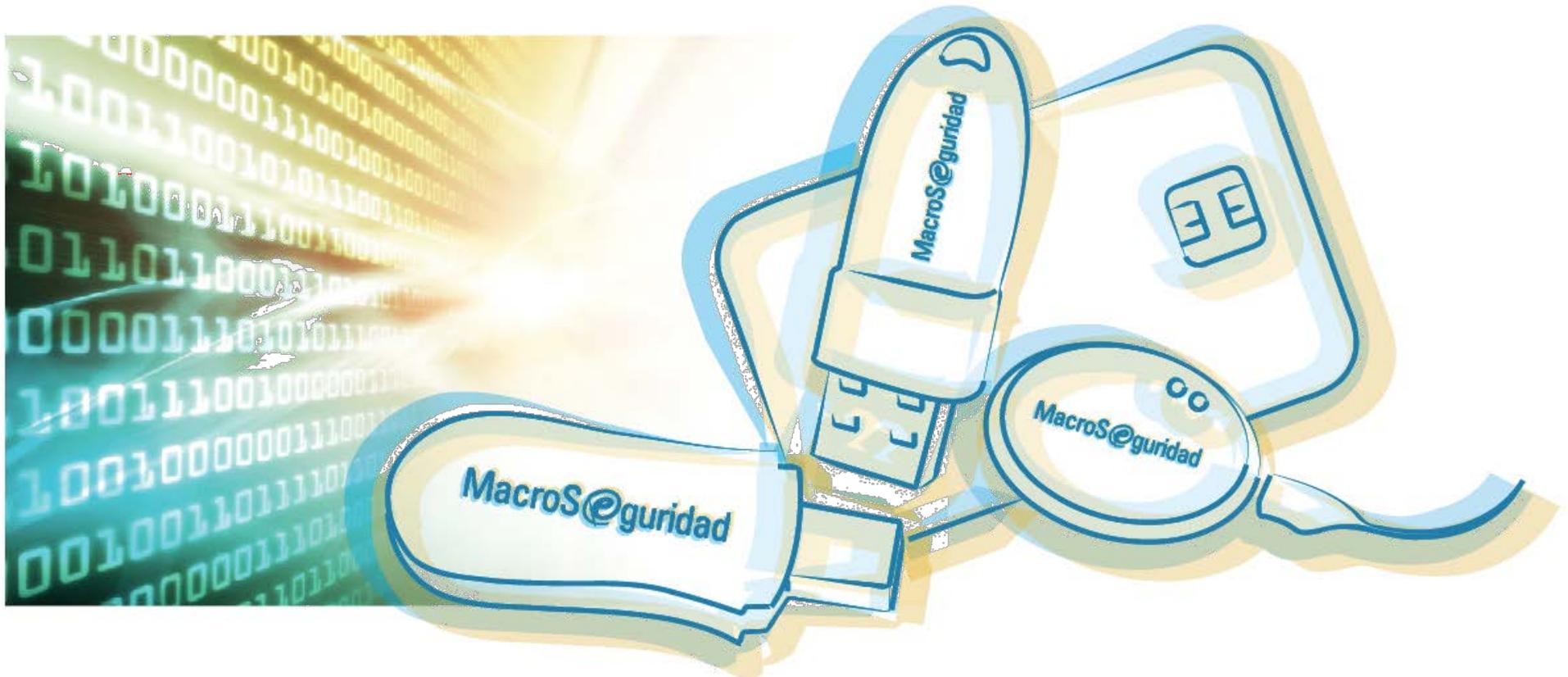
- Que cuesta no usarla?
  - Procesos Físicos (idas y vueltas)
- Como doy el primer paso

## – Herramientas de que tipo utilizar?



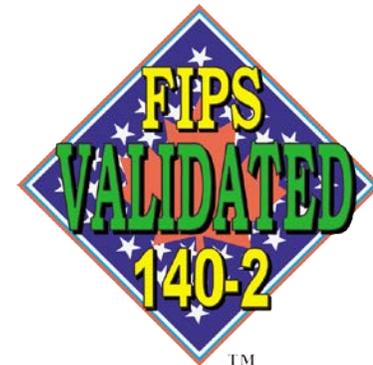
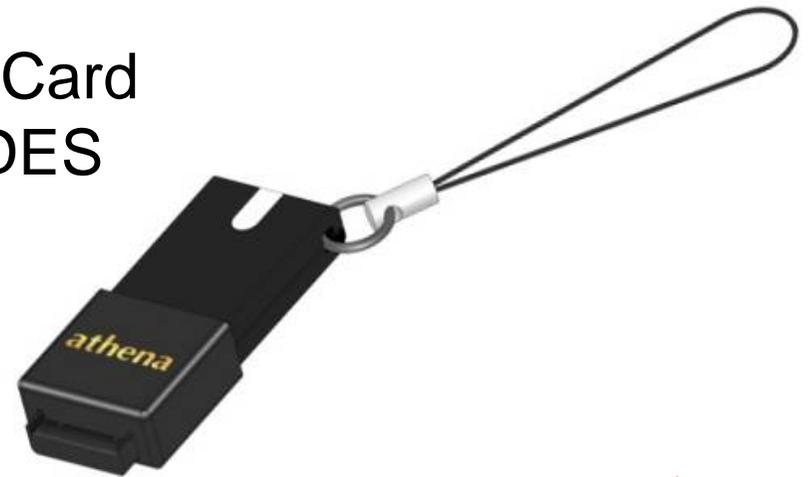
- PDF 417 o Código QR
- XML DSing
- Portable Signer - Xolido
- Sourceforge.net (centro de recursos)
- Que lenguaje de desarrollo?
  - CAPI - PKCS#11 – JAVA
- Firma Masiva (server) vs One to One
- Control Absoluto de la llave privada
- TSS – Perdurabilidad en el tiempo

# Dispositivos de Autenticación



# MS-ID Protect key

- Generación “on Board” de la clave privada del Certificado
- Token USB Criptográfico JAVA Card
- Algoritmos RSA (2048), 3DES, DES y AES. 72KB de memoria
- FIPS 140-2 Level 3 #1750
- SO Java Card 2.2.2
- Global Platform 2.1.1
- Certificado IP58 e IP69
- Licencia Perpetua y actualizaciones sin cargo
- Totalmente en castellano



# Las conclusiones

