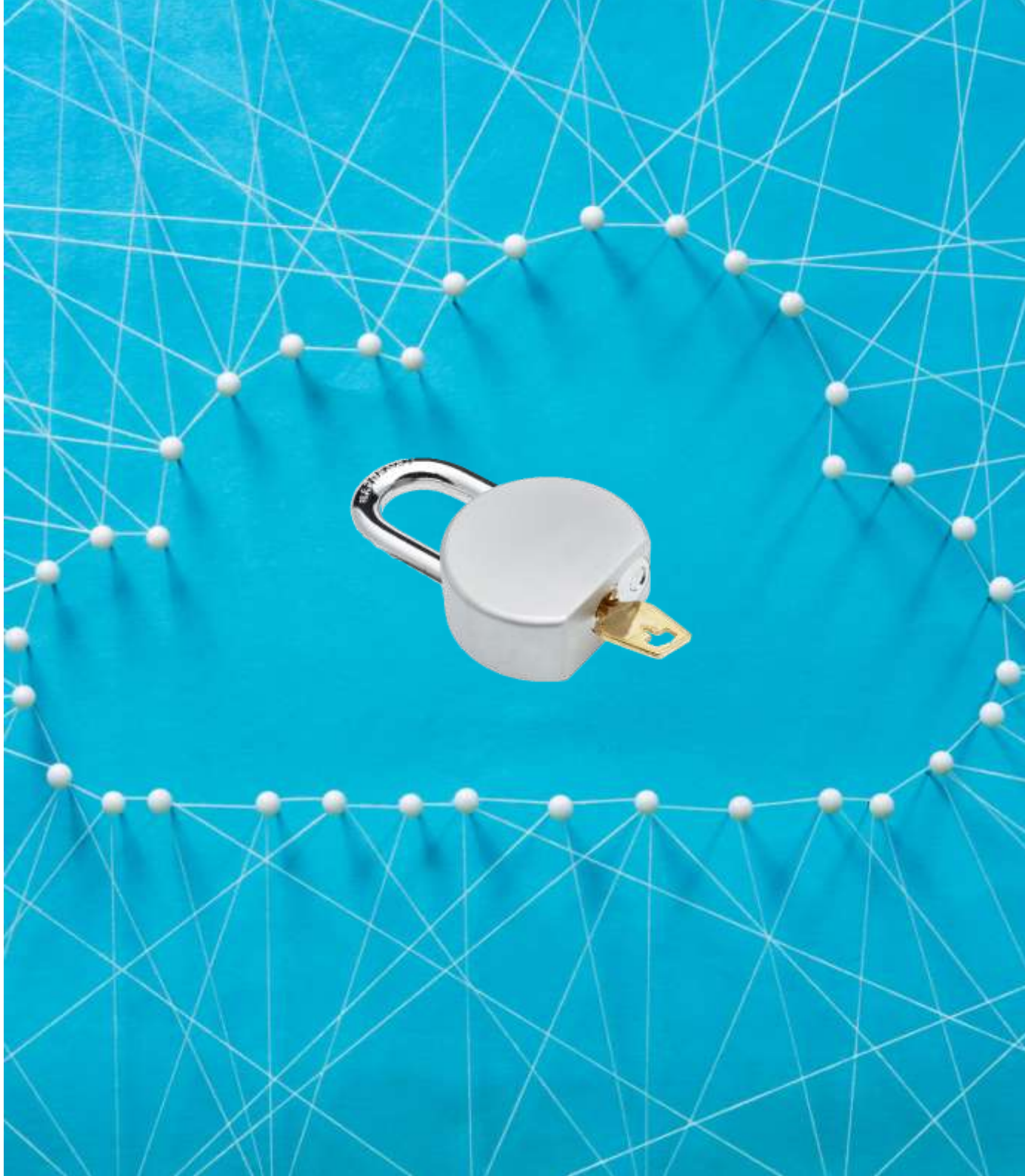
Seguridad en la Nube
Protegiendo nuestros Datos

Mauro Flores
mauflores@deloitte.com

@DeloitteUySeg
@mauro_fcib

SEGURINFO
Congreso y Feria Iberoamericana de Seguridad de la información



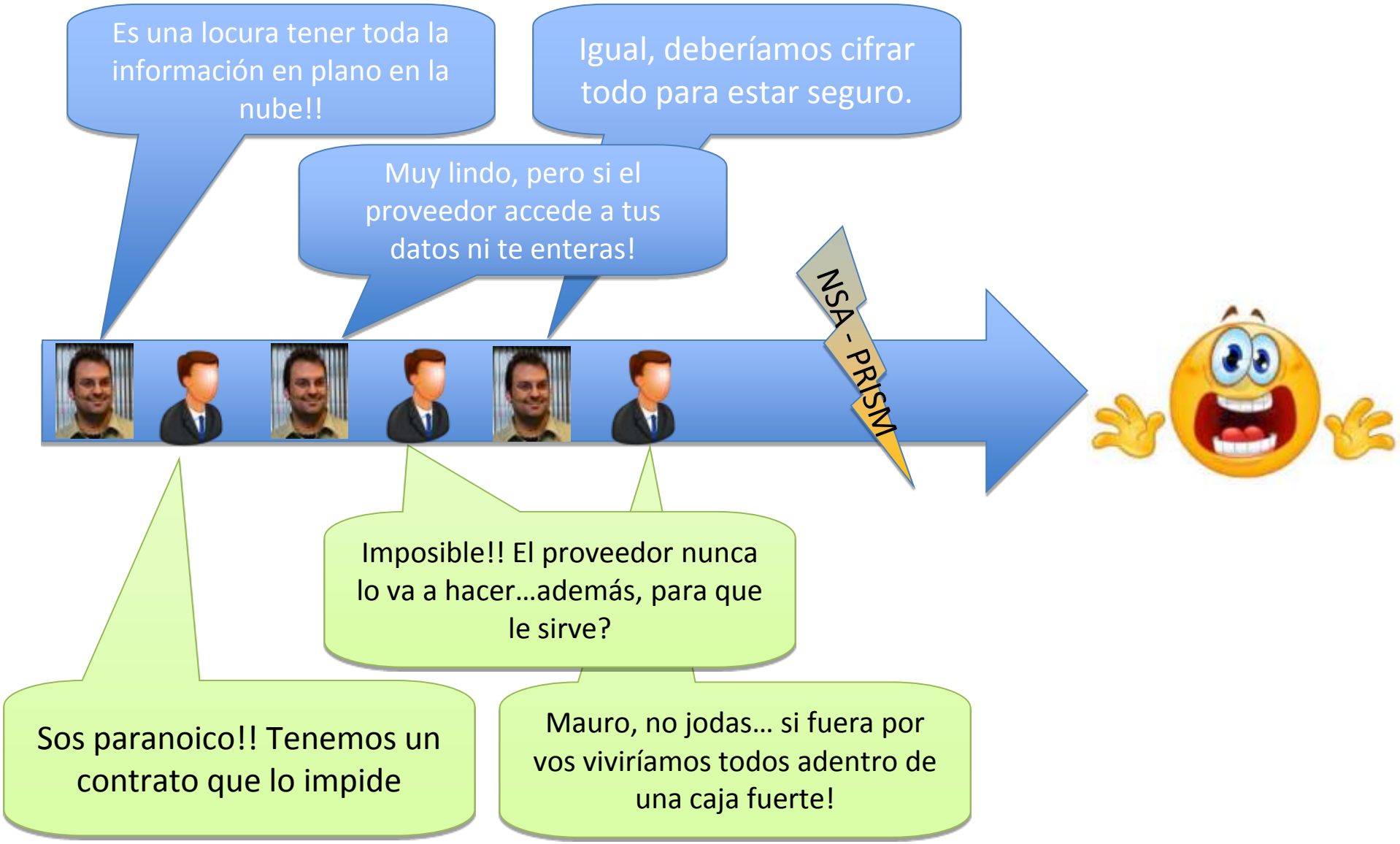
R1/R5 –Data Ownership, Privacy and Secondary Usage

De quien es la información?

- Dependemos 100% del proveedor
- Puedo garantizar que el proveedor:
  - No los utiliza para otros fines (estadísticos, etc)
  - No se los vende a la competencia
- El único resguardo, un contrato… es suficiente?

R1/R5 –Data Ownership, Privacy and Secondary Usage

De quien es la información?



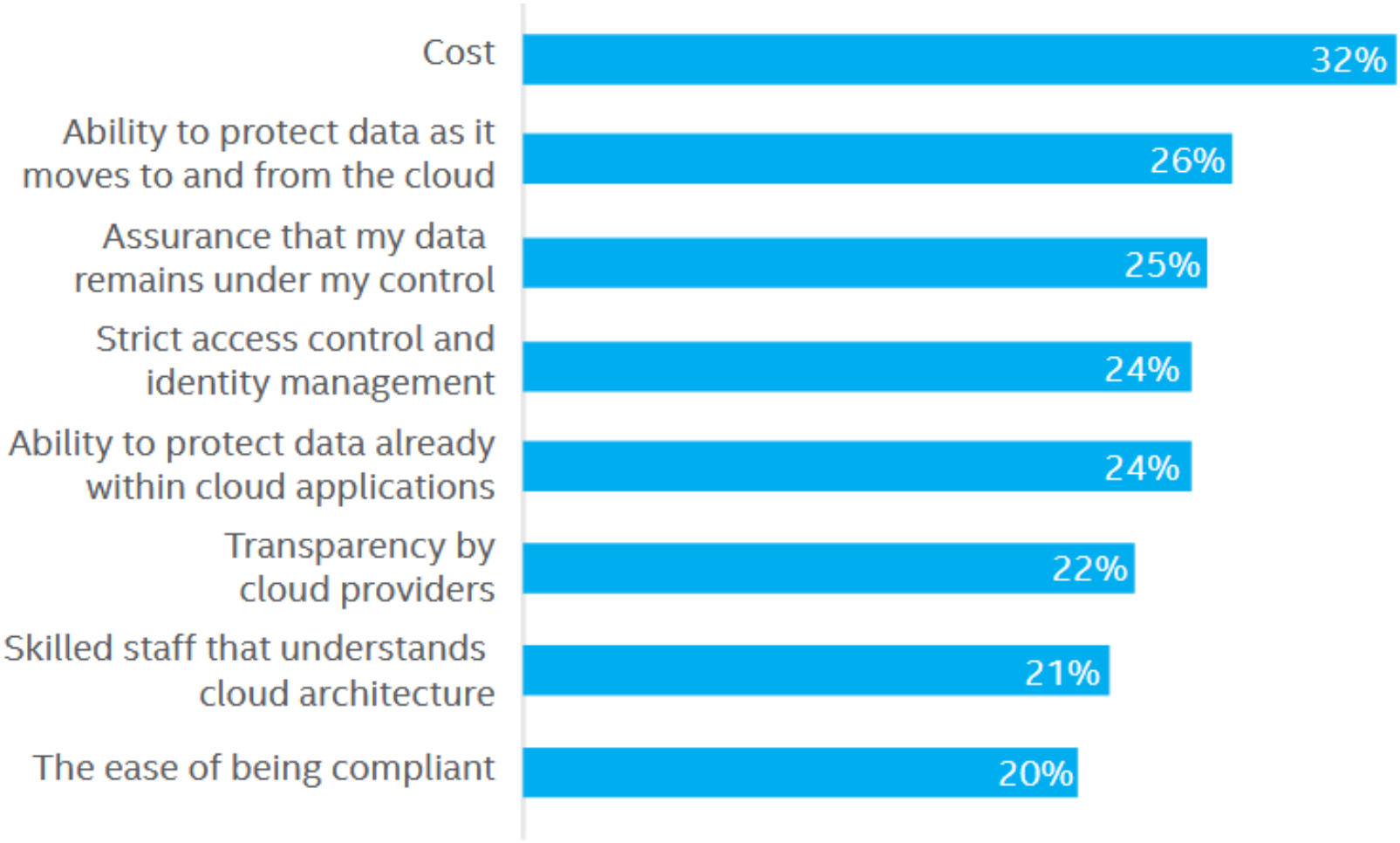
R1/R5 –Data Ownership, Privacy and Secondary Usage

El impacto de PRISM en la Nube

- Desconfianza en la nube (especialmente con base en U.S.)
  - 10% de cancelación de contratos
  - 56% no contrataría servicios en la nube en U.S.
- Mayores exigencias de cumplimiento de Habeas Data
- Estrategias de nubes híbridas

http://www2.itif.org/2013-cloud-computing-costs.pdf
https://spideroak.com/privacypost/online-privacy/will-prism-destroy-the-u-s-cloud/

R1/R5 –Data Ownership, Privacy and Secondary Usage



Which of the following would increase public cloud adoption within your organization?

https://www.mcafee.com/us/resources/reports/rp-building-trust-cloudy-sky.pdf

R1/R5 –Data Ownership, Privacy and Secondary Usage

La nube después de PRISM

- Los contratos son importantes pero no son suficientes
- Necesitamos incluir tecnología que garantice la privacidad… y hacerlo bien!
- Debemos establecer una cadena de confianza que nazca fuera de la nube...

Protegiendo el almacenamiento

Iniciando la cadena de confianza fuera de la nube

- Ej: DropBox, GoogleDrive, etc.
- Sincronizan una carpeta local con la nube
- Utilizar esquemas de cifrado de archivos de la carpeta local
- Debemos utilizar una herramienta que NO utilice contenedores (facilita la sincronización)

Protegiendo el almacenamiento

Iniciando la cadena de confianza fuera de la nube

- Herramientas: EncFs, eCryptFS
- Ejemplo:

```
#### Creo el FS cifrado (EncFS)

mkdir ~/Dropbox/.encrypted

encfs ~/Dropbox/.encrypted   ~/DropBox_Private

### Demosnto el FS

fusermount  -u  ~/DropBox_Private
```

- Trabajo sobre ~/DropBox_Private

Protegiendo las aplicaciones

OP1: Criptografía Homomórfica

- Permite operar sobre la información cifrada
- En un sistema homomórfico:
  - E(a+b) = E(a) + E(b)
  - E(a*b) = E(a) * E(b)
- Ejemplo (no formal solo a efectos ilustrativos)

  ROTx(ch) = ASCII(ch) + x Donde x es ‘la clave’

  D_ROTx(ch) = ROTx(ch) - x

  ROT13(‘A’) = ASCII(A) + 13 = 65 + 13 = 78 (Ar)

  ROT13(‘B’) = ASCII(B) + 13 = 66 + 13 = 79 (Br)

  ‘A’ + ‘B’ = ASCII(A) + ASCII(B) = 66 + 65 = 131

  ROTx(ch1) + ROTx(ch2) + … + ROTx(chN) = ch1 + x + ch2 + x +…+ chN +x =

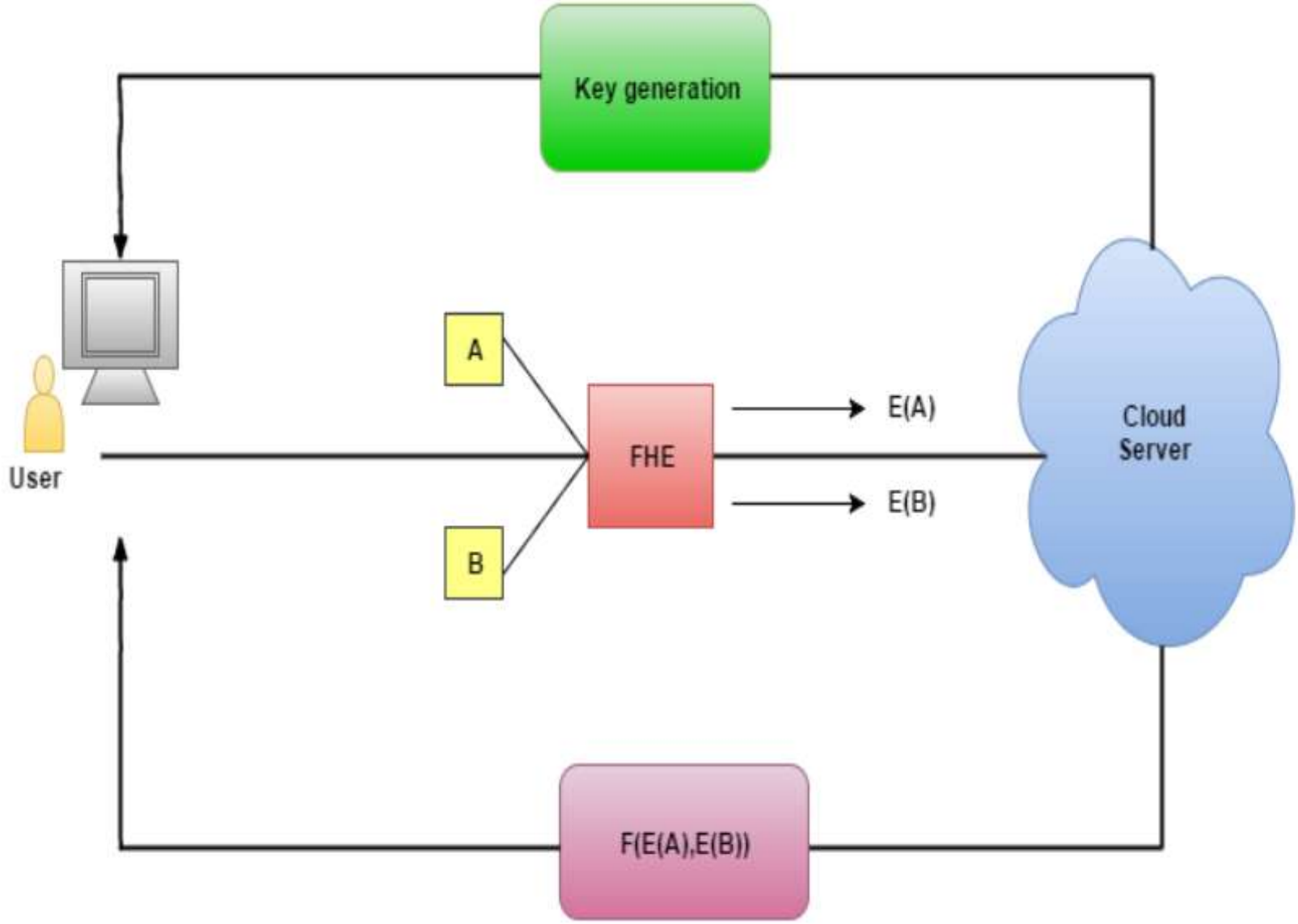
  Nx + $\sum ch_i$ => D_ROTx(ch1 + ch2 +…+ chN) = $\sum ch_i$ - Nx

  Ar + Br = 78 + 79 = 157

  D_ROT13(157) = 157 – 2*13 = 157 – 26 = 131 = ‘A’ + ‘B’

Protegiendo las aplicaciones

OP1: Criptografía Homomórfica



http://www.ijcaonline.org/archives/volume160/number6/biksham-2017-ijca-913063.pdf

Protegiendo las aplicaciones

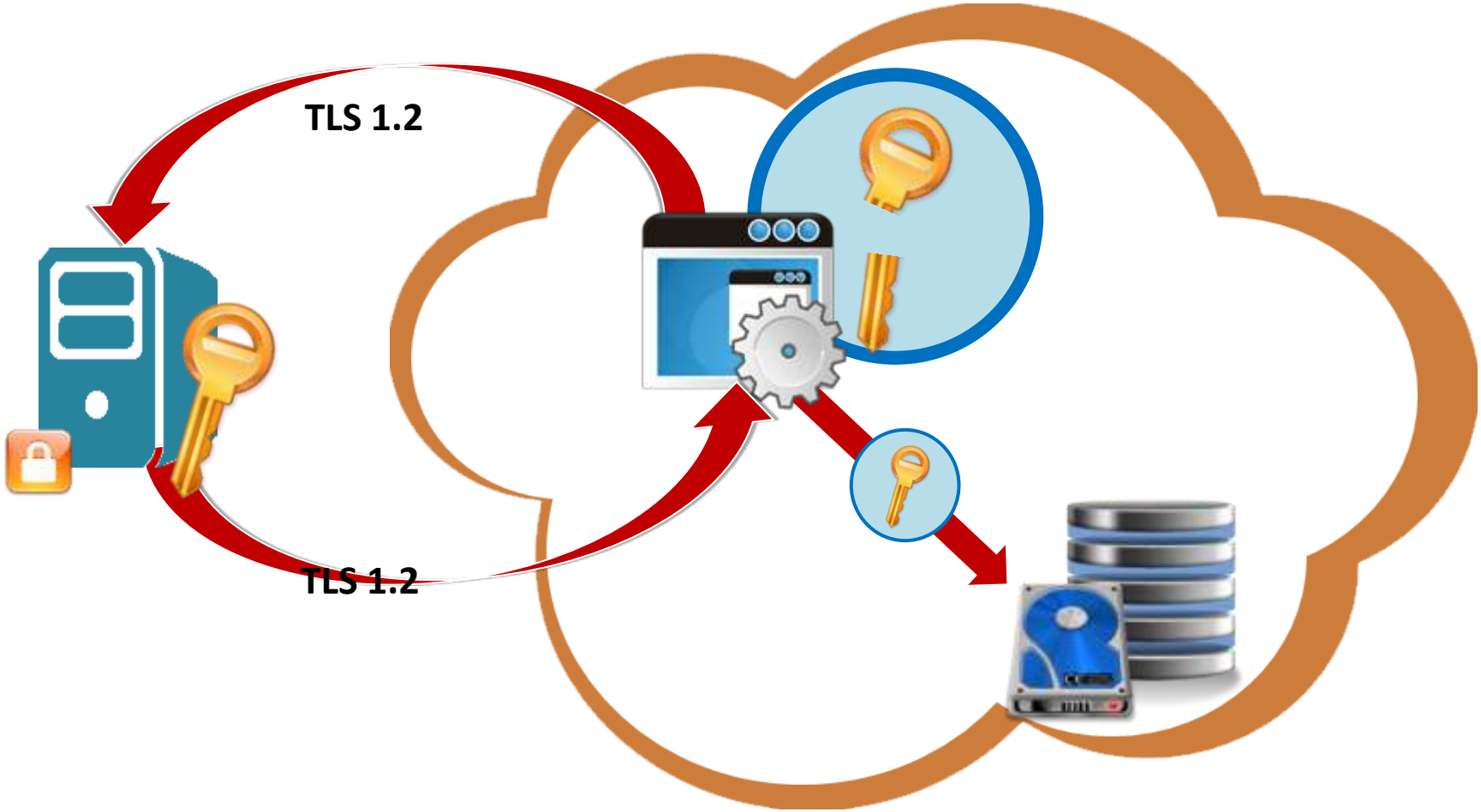
OP1: Criptografía Homomórfica

- Sumé los “cifrados” de A y B (Ar y Br) y a partir de la clave llegué al resultado descifrado.

- La Criptografía Homomórfica permite:
  - Cifro la información antes de subirla a la nube
  - la proceso en la nube sin descifrarla
  - Me transfiero el resultado y lo descifro en mi equipamiento

Protegiendo las aplicaciones

OP2: Iniciando la cadena de confianza fuera de la nube



Protegiendo las aplicaciones

OP2: Iniciando la cadena de confianza fuera de la nube

- Primitivas que almacenan la información segura en memoria:
  - Java: SecureString()
    https://github.com/c-a-m/passfault/blob/master/core/src/main/java/org/owasp/passfault/SecureString.java
  - .Net: SecureString()
    http://msdn.microsoft.com/en-us/library/system.security.securestring%28v=vs.110%29.aspx

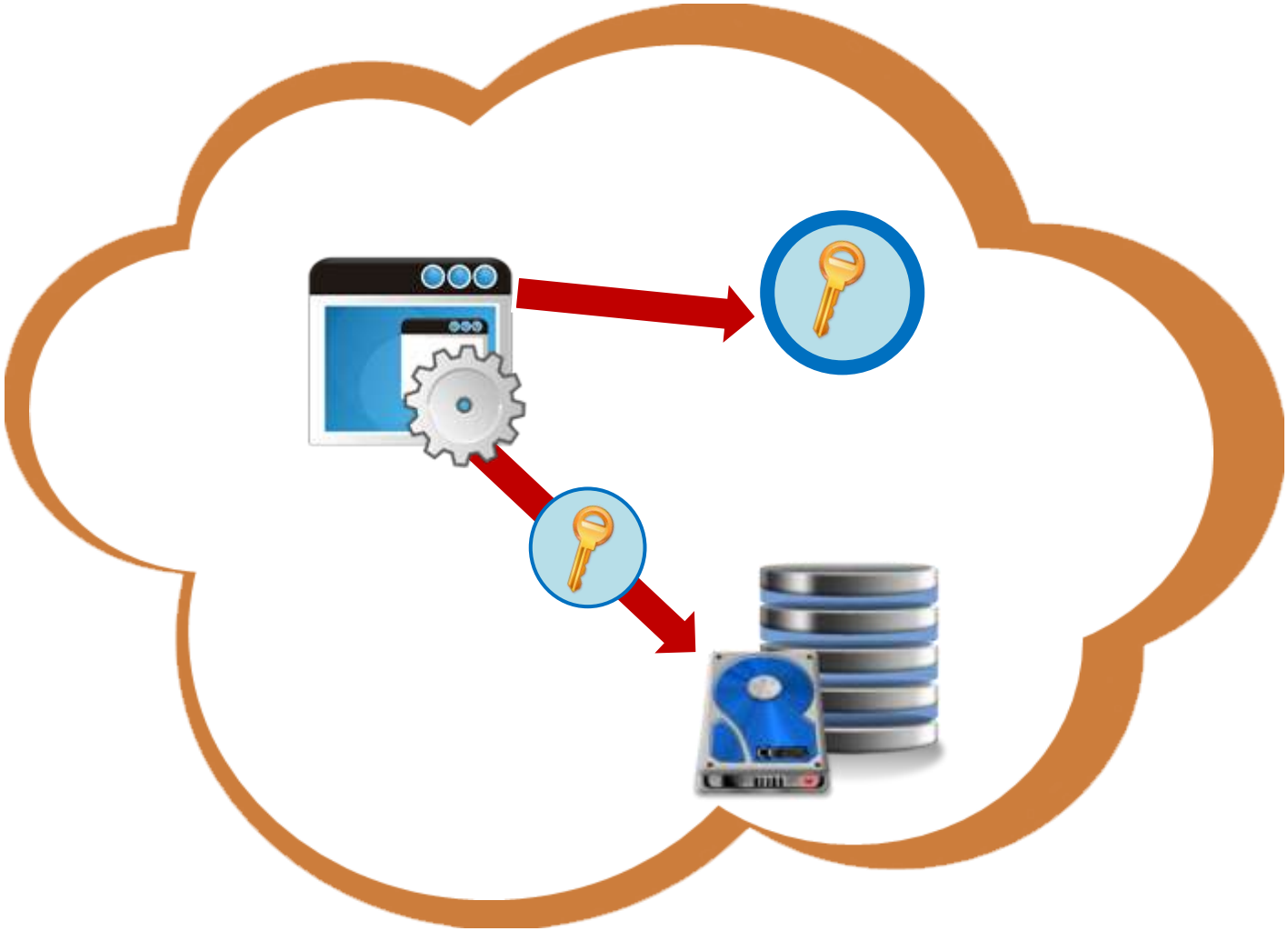
Protegiendo las aplicaciones

OP3: Cifrado en la Nube

- Soluciones tipo TDE o cifrado de disco
- Almaceno cifrado pero las llaves están en la nube
- Podría utilizar un HSM del proveedor de la nube

Protegiendo las aplicaciones

OP3: Cifrado en la Nube



Recomendaciones

Diseñar las aplicaciones para la nube

- Evaluar que información llevaremos a la nube y como la vamos a proteger
- Usar algoritmos robustos de cifrado
- No persistir en la nube las claves de cifrado
- Proteger las claves en memoria
  - No usar strings fácilmente reconocibles
  - Ofuscar o fragmentar la clave en memoria
- Utilizar múltiples claves de cifrado
  - Diferentes claves para diferentes grupos de datos

Deloitte.