



# 2<sup>nd</sup> International Symposium on Master Engineering

## *Booklets*



RENIECYT - LATINDEX - EBSCO - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - Google Scholar DOI - REDIB - Mendeley - DIALNET - ROAD - ORCID

# Title: Data Security Challenges: Big Data and Quantum Computing

## Author: MORALES-SANDOVAL, Miguel

Editorial label ECORFAN: 607-8695  
 BIMES Control Number: 2022-17  
 BIMES Classification (2022): 231122-0017

Pages: 80  
 RNA: 03-2010-032610115700-14

**ECORFAN-México, S.C.**  
 143 – 50 Itzopan Street  
 La Florida, Ecatepec Municipality  
 Mexico State, 55120 Zipcode  
 Phone: +52 1 55 6159 2296  
 Skype: ecorfan-mexico.s.c.  
 E-mail: contacto@ecorfan.org  
 Facebook: ECORFAN-México S. C.  
 Twitter: @EcorfanC

[www.ecorfan.org](http://www.ecorfan.org)

Holdings		
Mexico	Colombia	Guatemala
Bolivia	Cameroon	Democratic
Spain	El Salvador	Republic
Ecuador	Taiwan	of Congo
Peru	Paraguay	Nicaragua

# Contenido

- Seguridad y seguridad de datos
- Algoritmos y protocolos para la seguridad de datos
- Reto 1: Big data
  - Almacenamiento y compartición segura
  - Eficiencia
- Reto 2: Cómputo cuántico
  - Year to Quantum
  - Quantum safe
- Comentarios finales
  - Privacidad bajo responsabilidad del propietario

# Seguridad de datos

## – Objetivos:

- Robo de datos – compromete la **Confidencialidad**
- Modificación de datos – compromete la **Integridad**
- Acceso sin permiso – **Autenticación/ control de acceso**
- Ataque DoS – **Disponibilidad**

**Ataque activo:** acceso no autorizado, modifica los datos.

**Ataque pasivo:** acceso no autorizado, sin modificaciones en los datos, solo se leen.

### **Datos objetivo de ataques**

Datos sensibles de organizaciones

+ **Su ventaja competitiva**

Datos personales privados de personas

+ **Passwords, registros médicos, salarios, personales y de preferencias**

# Seguridad de datos

## – Objetivos:

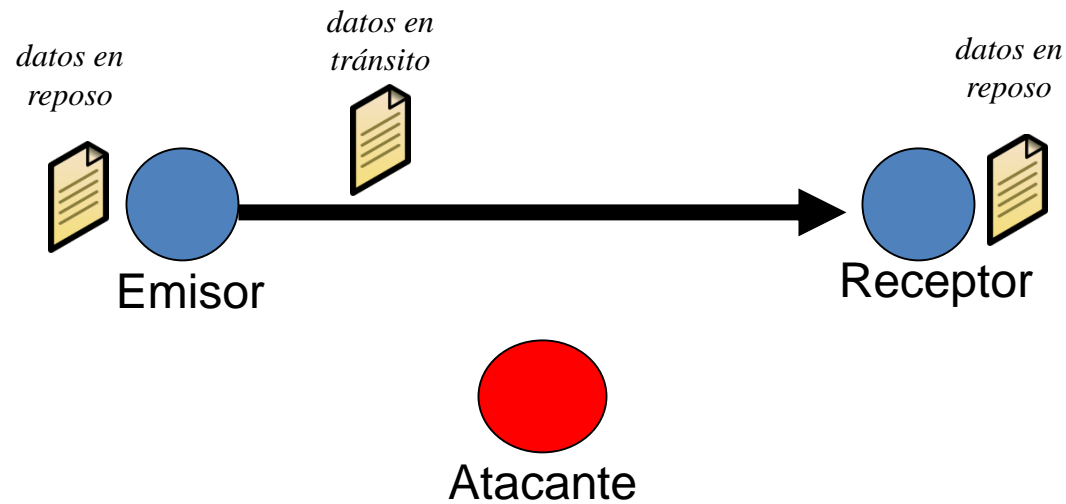
- Robo de datos – compromete la **Confidencialidad**
- Modificación de datos – compromete la **Integridad**
- Acceso sin permiso – **Autenticación/ control de acceso**
- Ataque DoS – **Disponibilidad**

## Garantizar los servicios de seguridad **CIA**

- **Confidencialidad** – acceso solo a entidades autorizadas
- **Integridad** – detectar cambios accidentales o intencionales
- **Autenticidad** – Verificar origen y destino de los datos

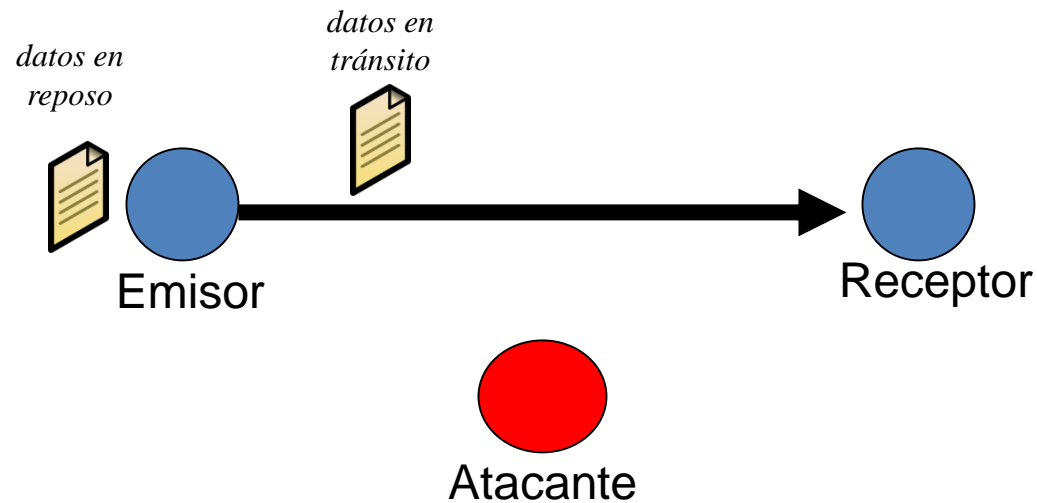
# Servicios, amenazas, ataques

Los datos están en *reposo* o en *tránsito*



# Servicios, amenazas, ataques

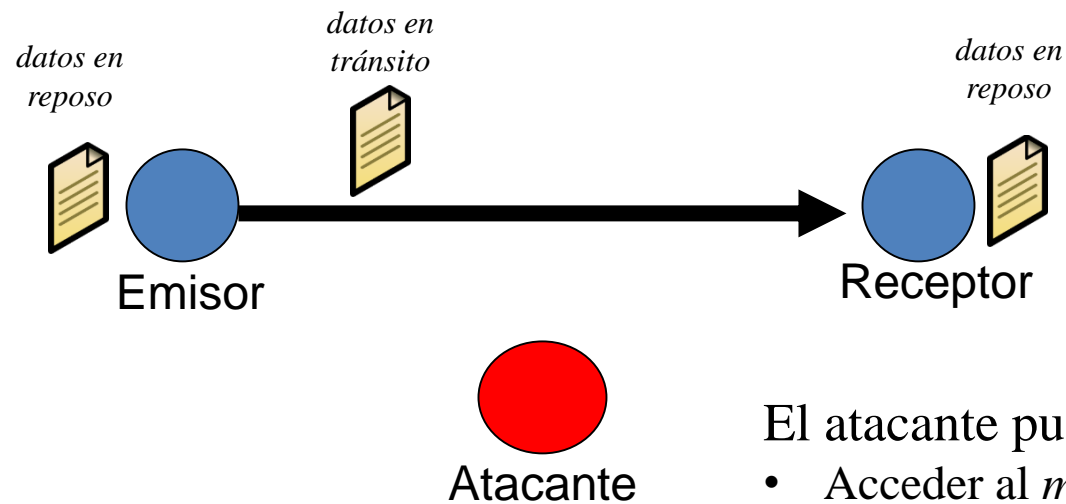
Los datos están en *reposo* o en *tránsito*



- CASO “NORMAL”
  - Los mensajes no son accedidos por entidades **externas no autorizadas**

# Servicios, amenazas, ataques

Los datos están en *reposo* o en *tránsito*

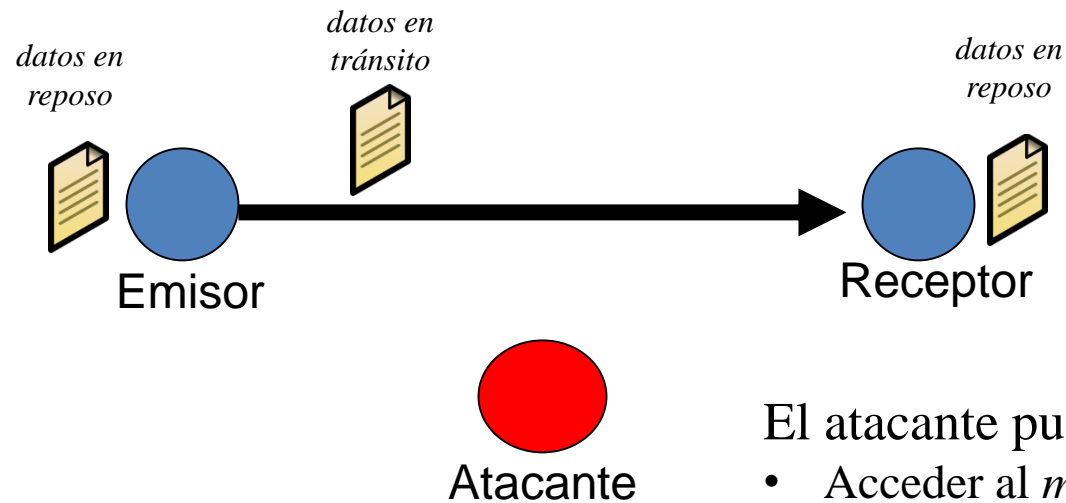


El atacante puede:

- Acceder al *medio de comunicación* (inalámbrico o cableado)
  - Acceder a la red
- Acceder al *dispositivo*
- Acceder a *los sistemas*
- **Acceder a los datos**

# Servicios, amenazas, ataques

Los datos están en *reposo* o en *tránsito*



El atacante puede:

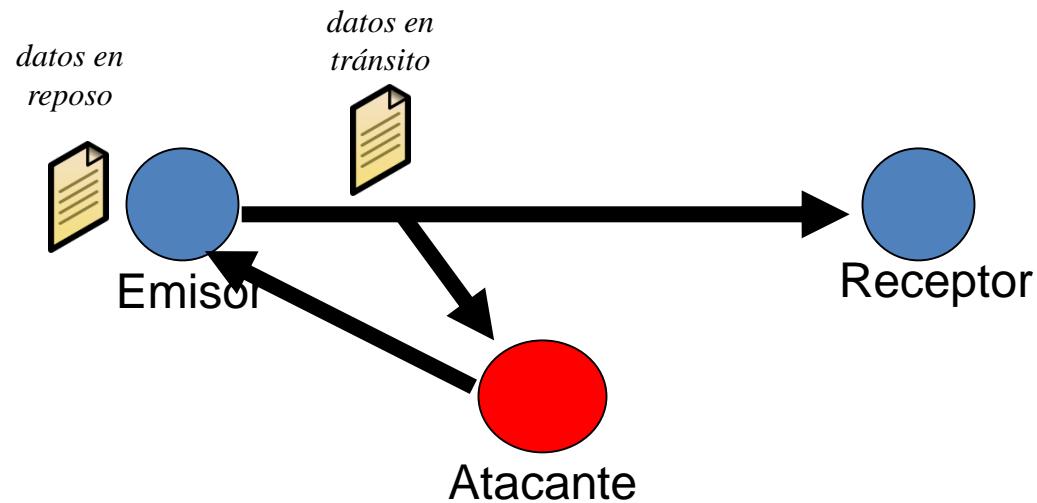
- Acceder al *medio de comunicación* (inalámbrico o cableado)
  - Acceder a la red
- Acceder al *dispositivo*
- Acceder a *los sistemas*
- **Acceder a los datos**

Última línea  
de defensa



# Servicios, amenazas, ataques

Los datos están en *reposo* o en *tránsito*

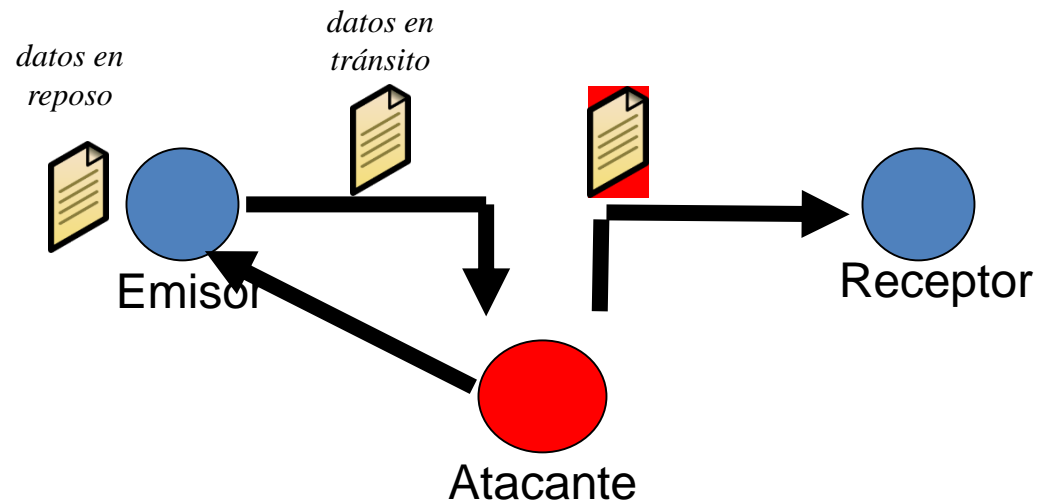


- **INTERCEPCION**

- El atacante logra el acceso al medio de comunicación
- Es un ataque contra la **Confidencialidad**.
- Ejemplos: Escuchas electrónicos, copias ilícitas de programas o datos, escalamiento de privilegios.

# Servicios, amenazas, ataques

Los datos están en *reposo* o en *tránsito*

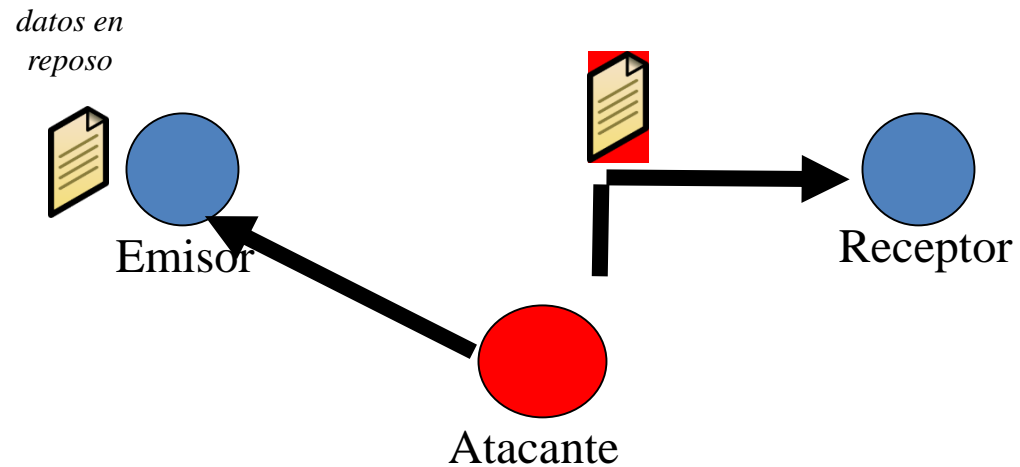


- MODIFICACION

- La persona sin autorización, además de lograr el acceso, modifica el mensaje.
- Este es un ataque contra la *Integridad*.
- Ejemplos: Alterar la información que se transmite desde una base de datos, modificar los mensajes entre programas para que se comporten diferente.

# Servicios, amenazas, ataques

Los datos están en *reposo* o en *tránsito*

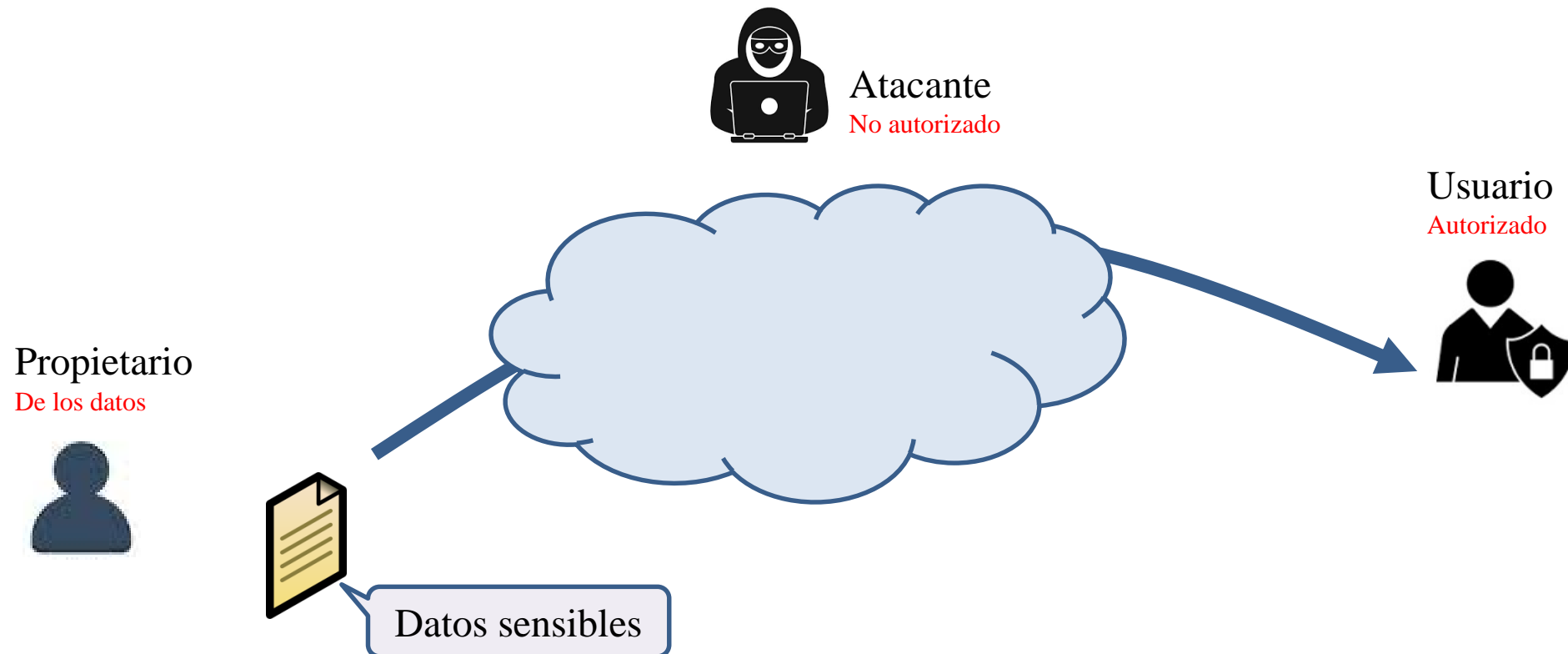


- **FABRICACION**
  - Una persona sin autorización inserta objetos falsos en el sistema.
  - Es un ataque contra la *Autenticidad*.
  - Ejemplos: Suplantación de identidades, robo de sesiones, robo de contraseñas, robo de direcciones IP, etc...
- Es muy difícil estar seguro de quién está al otro lado de la línea.

# Solución de seguridad de datos

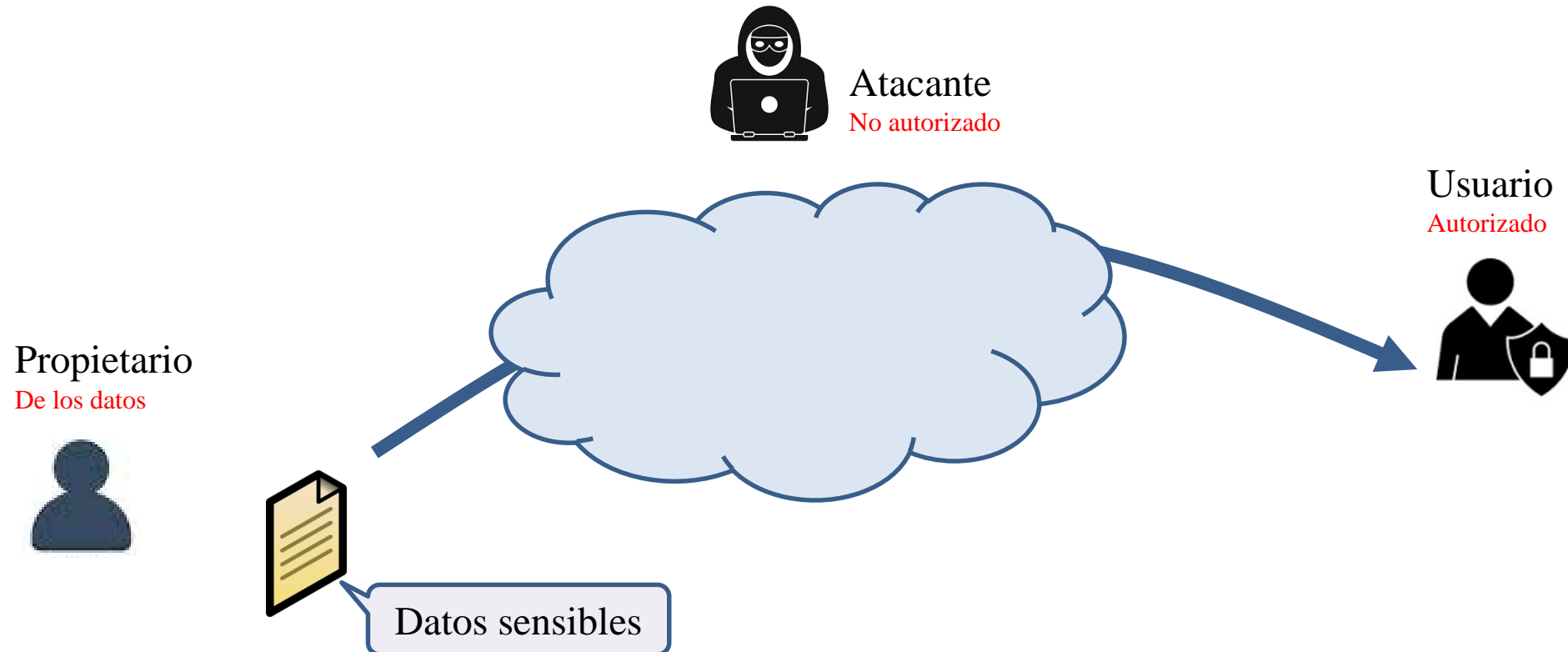
¿Cómo podemos garantizar CIA?

¿Cómo podemos prevenir ataques a CIA?

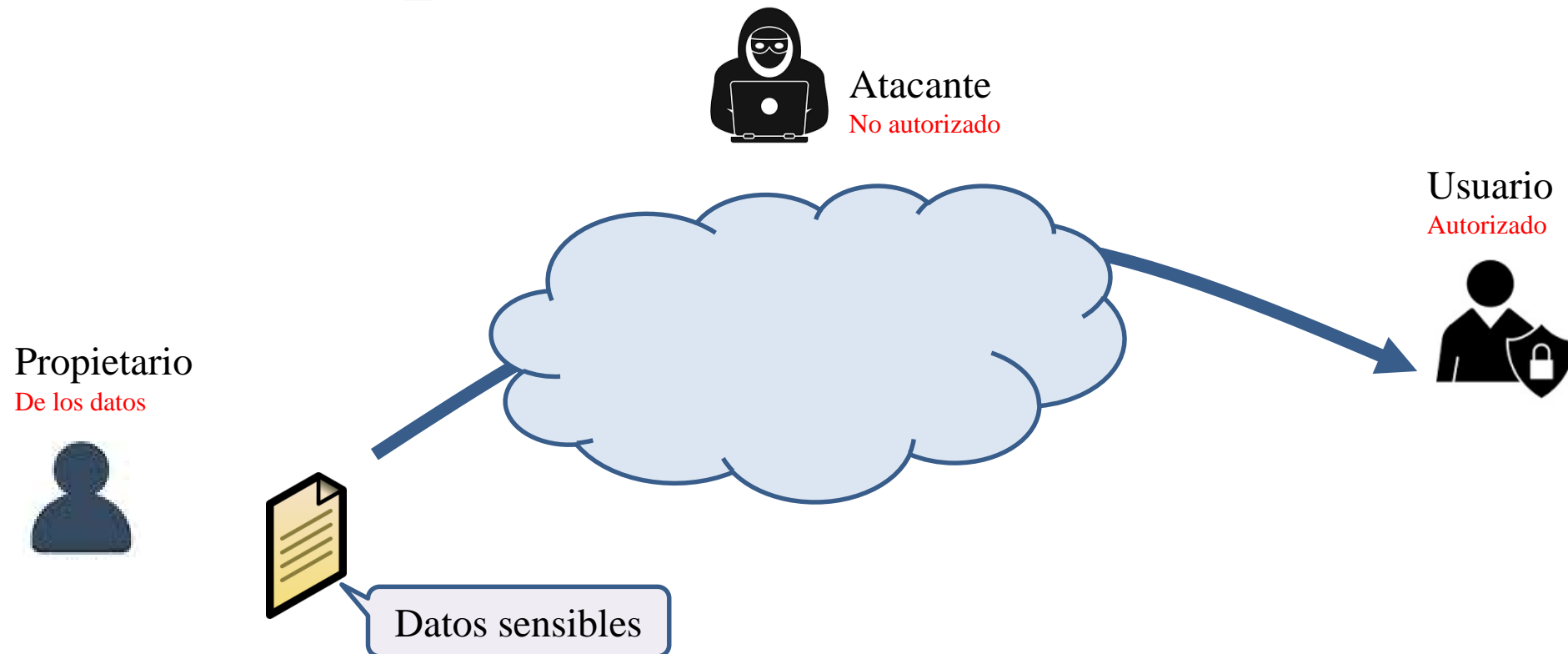


# Solución de seguridad de datos

**R = Criptografía**

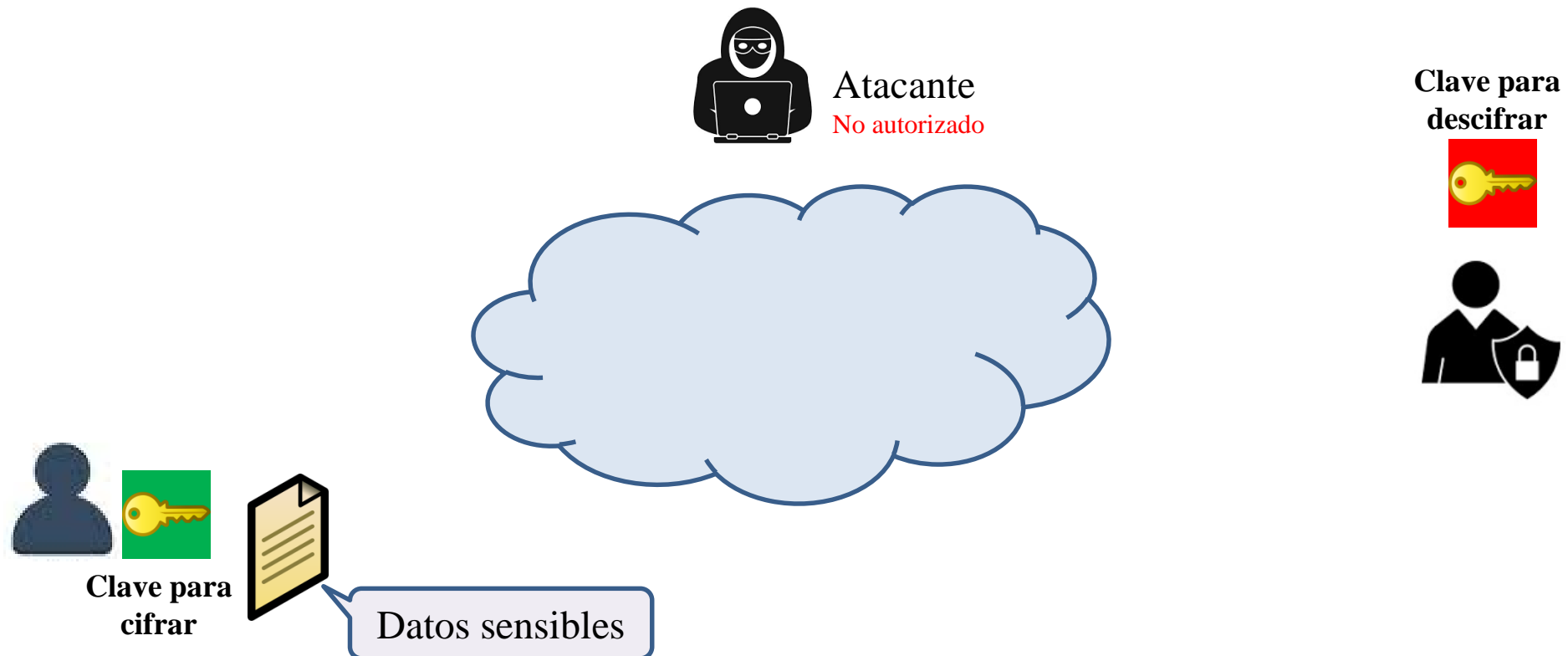


- Desde los más *antiguos* hasta los *modernos* y *futuros*, todos basan su funcionamiento a partir de tres algoritmos: `gen_claves()`, `cifrar_datos()`, `descifrar_datos()`



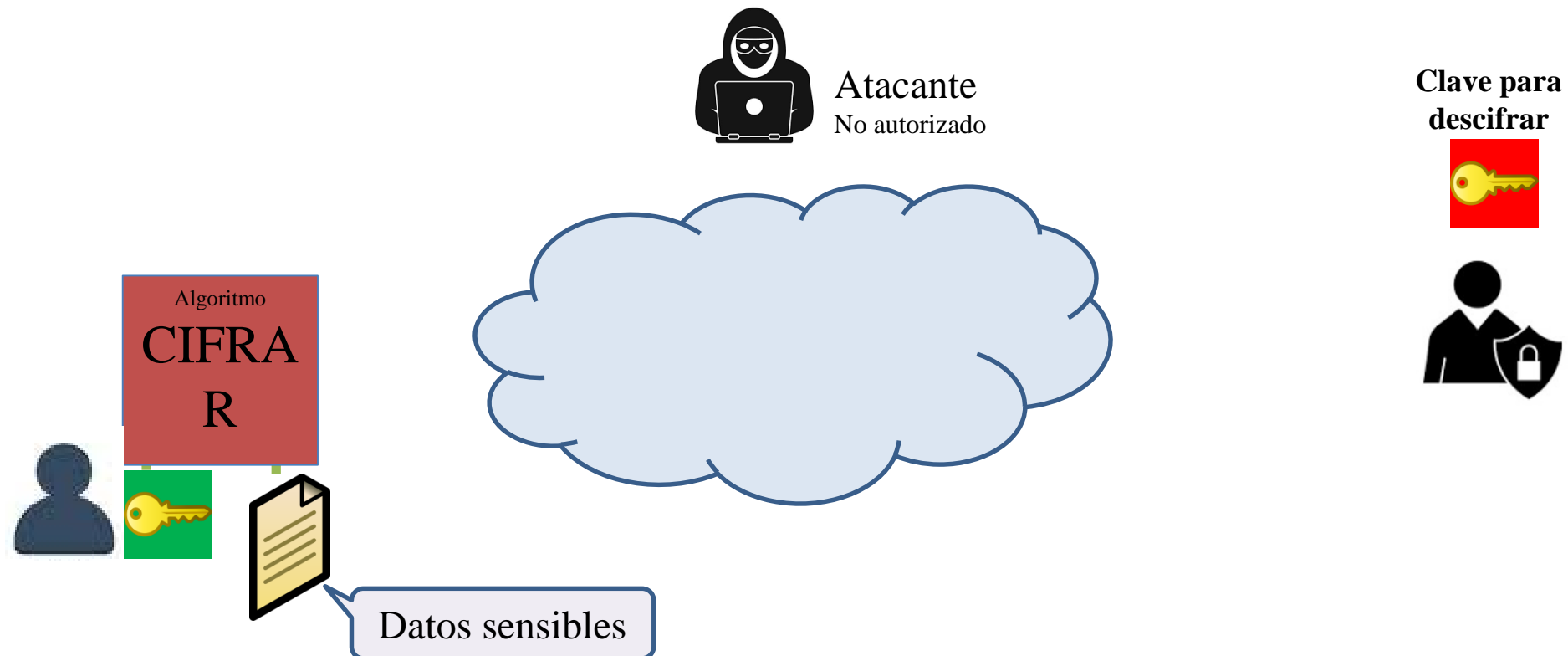
# Criptosistemas

- Desde los más *antiguos* hasta los *modernos* y *futuros*, todos basan su funcionamiento a partir de tres algoritmos: `gen_claves()`, `cifrar_datos()`, `descifrar_datos()`



# Criptosistemas

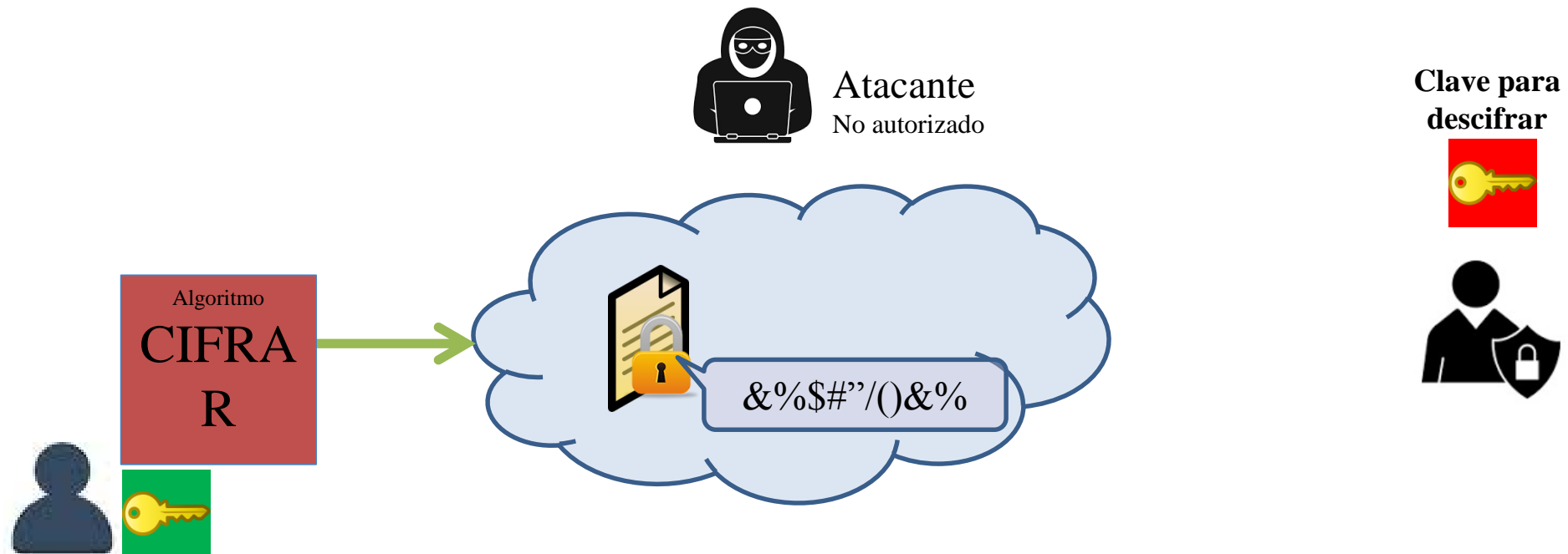
- Desde los más *antiguos* hasta los *modernos* y *futuros*, todos basan su funcionamiento a partir de tres algoritmos: `gen_claves()`, `cifrar_datos()`, `descifrar_datos()`





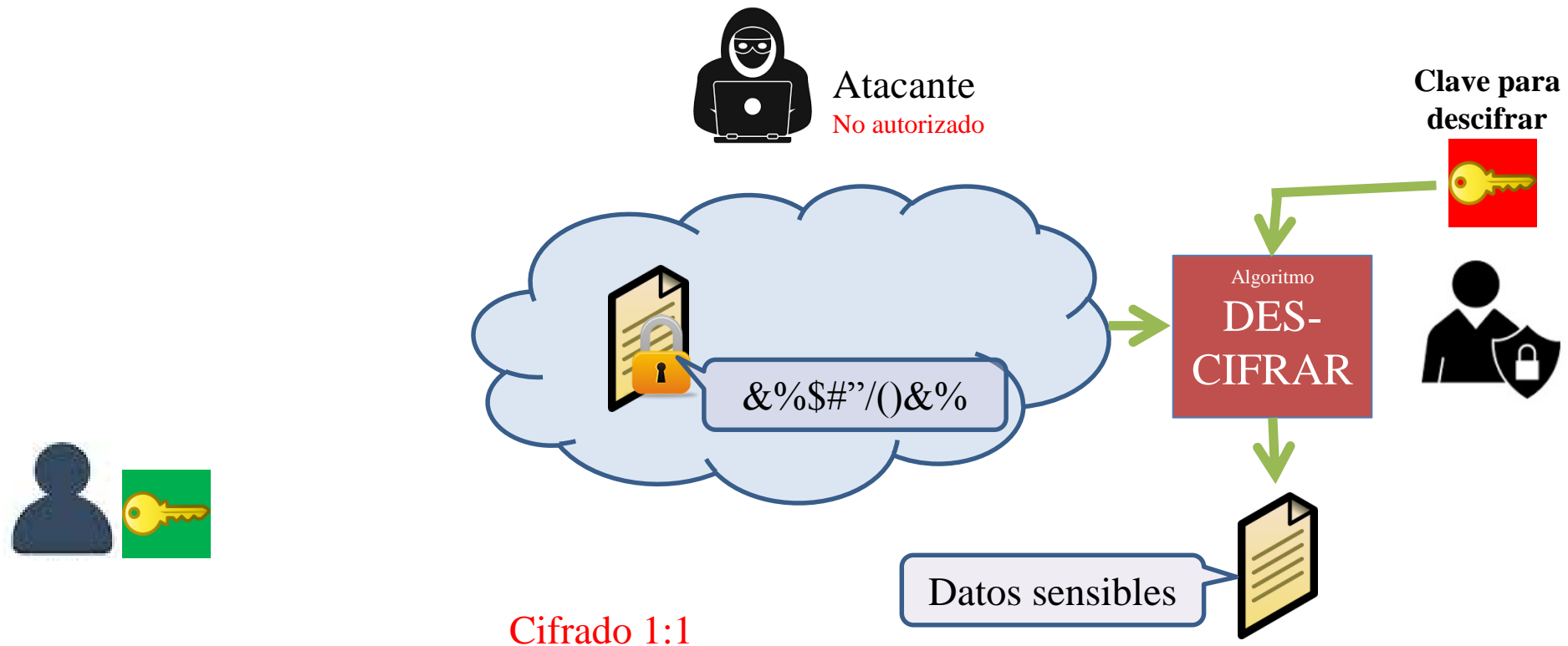
# Criptosistemas

- Desde los más antiguos hasta los modernos y futuros, basan su funcionamiento a partir de tres algoritmos: `gen_claves()`, `cifrar_datos()`, `descifrar_datos()`



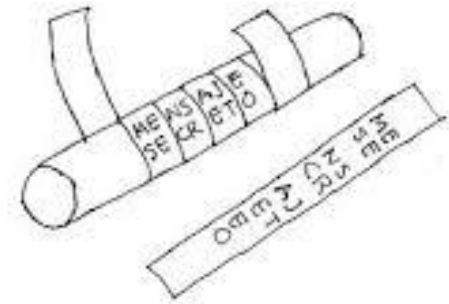
# Criptosistemas

- Desde los más antiguos hasta los modernos y futuros, basan su funcionamiento a partir de tres algoritmos: `gen_claves()`, `cifrar_datos()`, `descifrar_datos()`



# Criptografía e historia

- Criptografía – Arte de ocultar información
  - “*Cryptos*” → Ocultar
  - “*Graphe*” → Escritura
- Primeros cifradores desde antes de nuestra era (Grecia)
- Rol relevante en la historia - 2da Guerra mundial
  - Criptografía (Enigma) fue una de las principales armas del bloque alemán
  - Motivó la creación de máquinas de propósito específico para romper el cifrado alemán → bases de la computación actual y de la inteligencia artificial (Alan Turing)



Escitala



# Criptografía moderna

- Criptografía moderna a partir de 1976
  - creación del primer estándar de cifrado *DES*
  - *Protocolo Diffie-Hellman* para establecimiento de secretos usados para ocultar la información digital

# Criptografía moderna

- Criptografía moderna a partir de 1976
  - creación del primer estándar de cifrado *DES*
  - *Protocolo Diffie-Hellman* para establecimiento de secretos usados para ocultar la información digital



# Criptografía en la actualidad



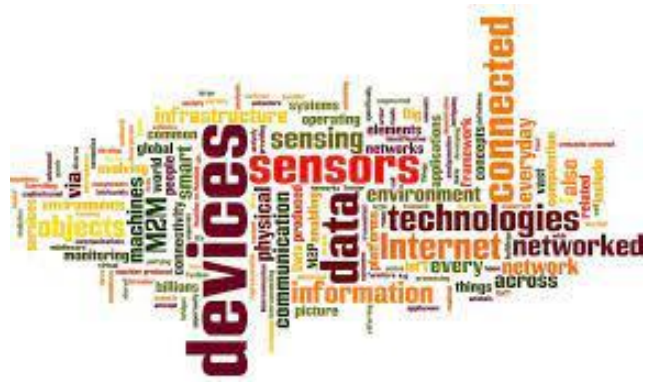
# Criptografía en la actualidad







# Criptografía en la actualidad





# Criptografía en la actualidad



# Reto 1: Big data

- “*Data-centric world*”
  - **Valor** en colectar y usar datos

# Reto 1: Big data

- “*Data-centric world*”
  - **Valor** en colectar y usar datos

Hospitales inteligentes:

# Reto 1: Big data

- “*Data-centric world*”
  - **Valor** en colectar y usar datos

Ciudades inteligentes

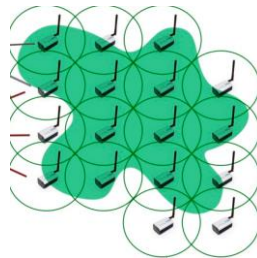


# Reto 1: Big data

- “*Data-centric world*”



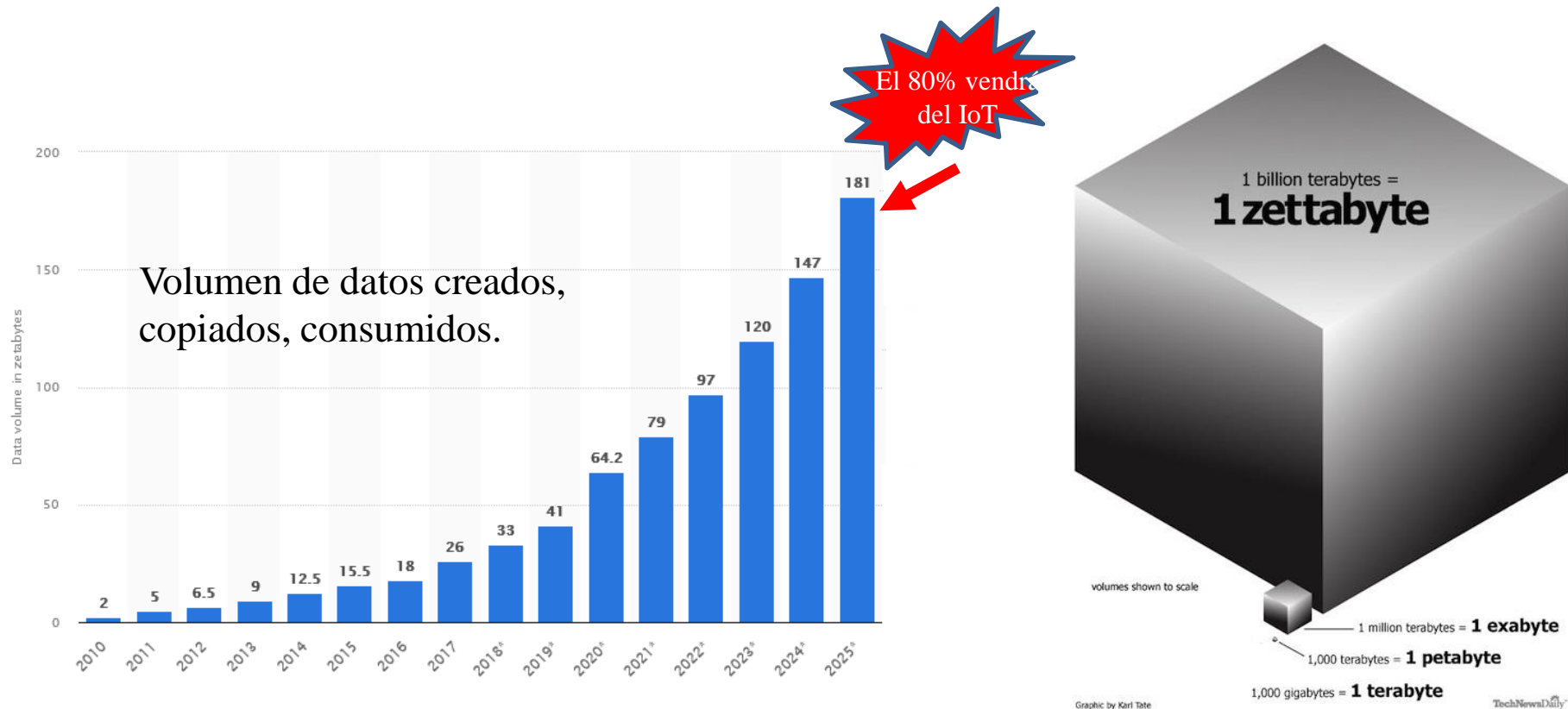
**BigData**



**Enorme cantidad de datos producidos por varias fuentes, en múltiples formatos y a una gran velocidad.**

# Reto 1: Big data

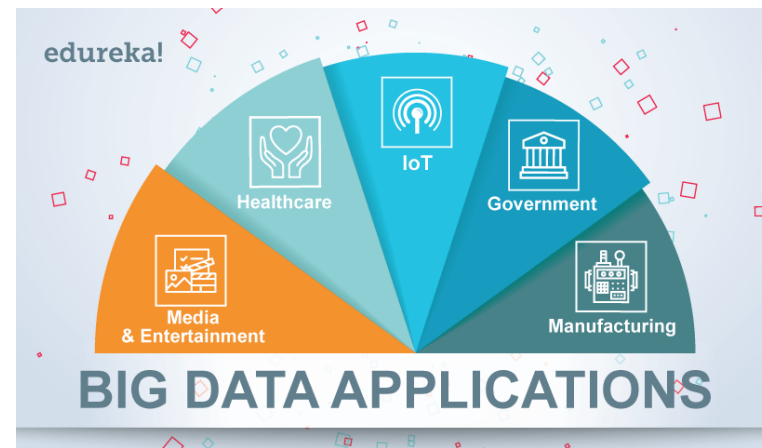
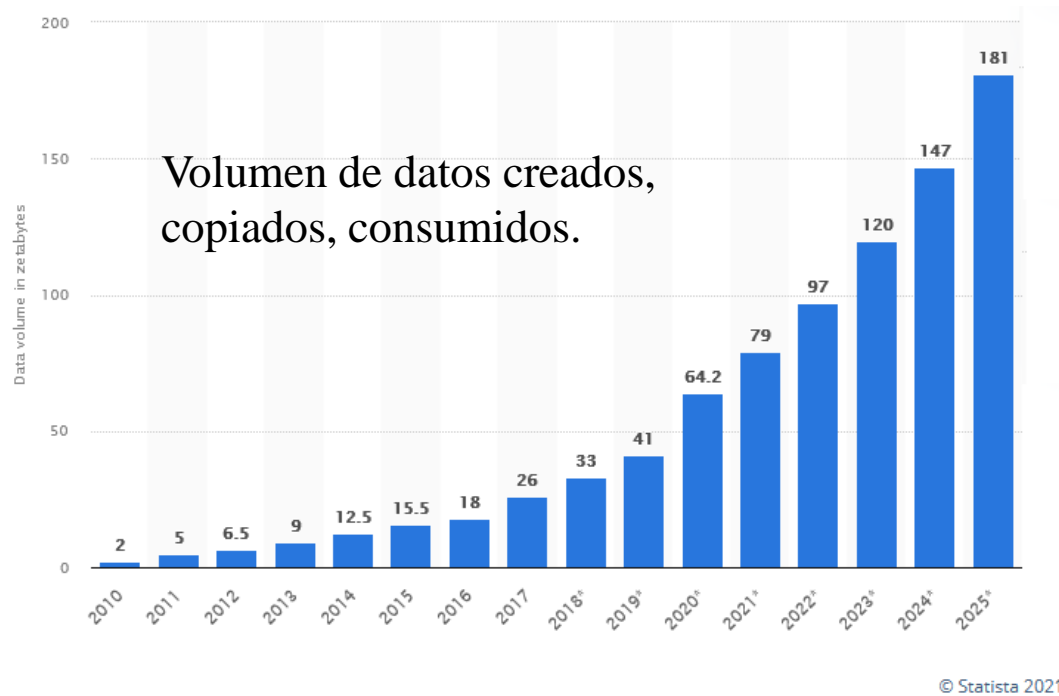
- “*Data-centric world*” → **BigData**





# Reto 1: Big data

- “*Data-centric world*” → **BigData**

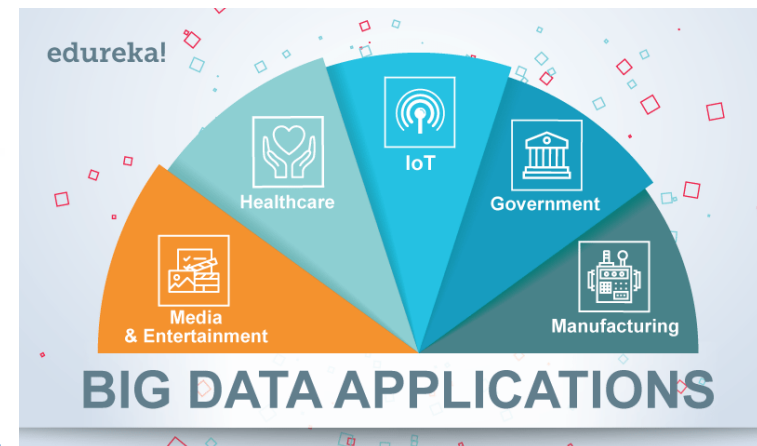
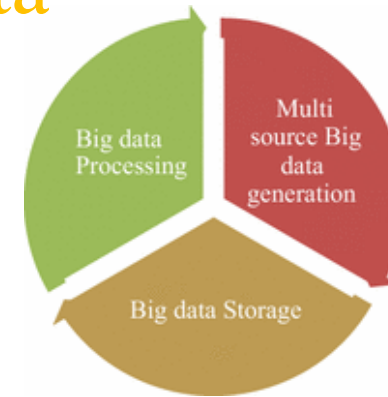


# Reto 1: Big data

- “*Data-centric world*” → **BigData**



© Statista 2021



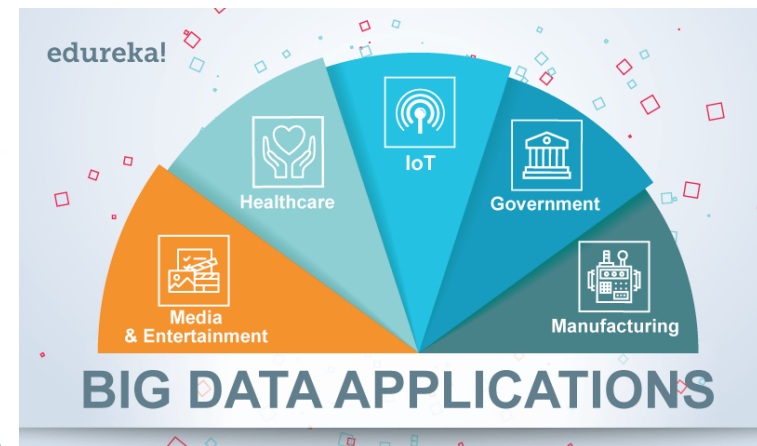
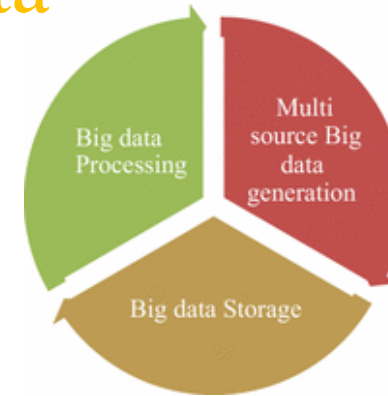
# Reto 1: Big data

- “*Data-centric world*” → **BigData**

## Seguridad y privacidad en Big Data



© Statista 2021



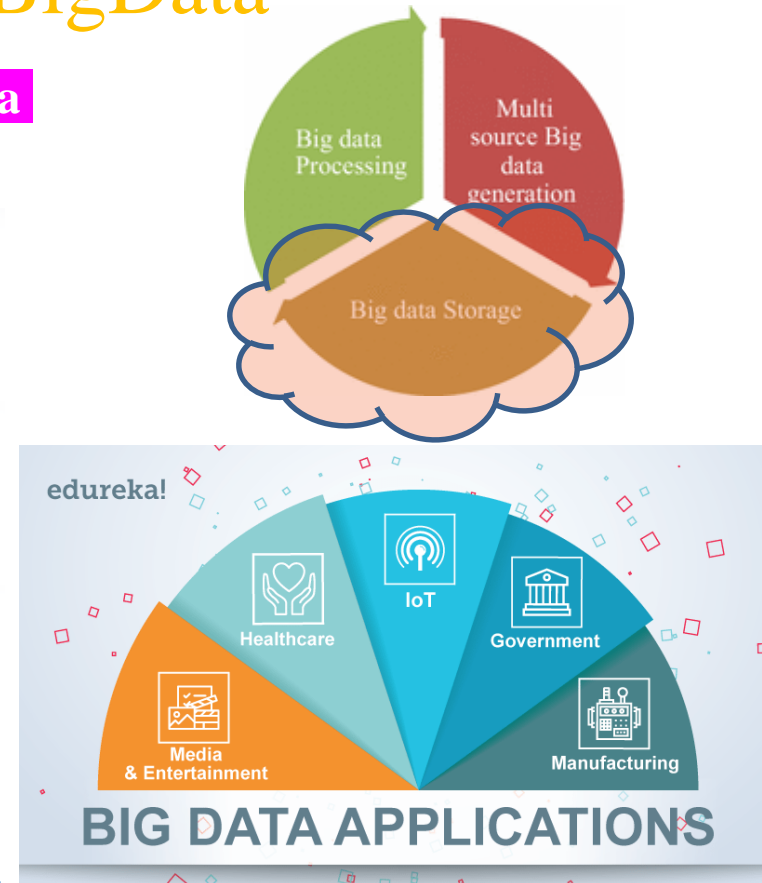
# Reto 1: Big data

- “*Data-centric world*” → **BigData**

## Seguridad y privacidad en Big Data

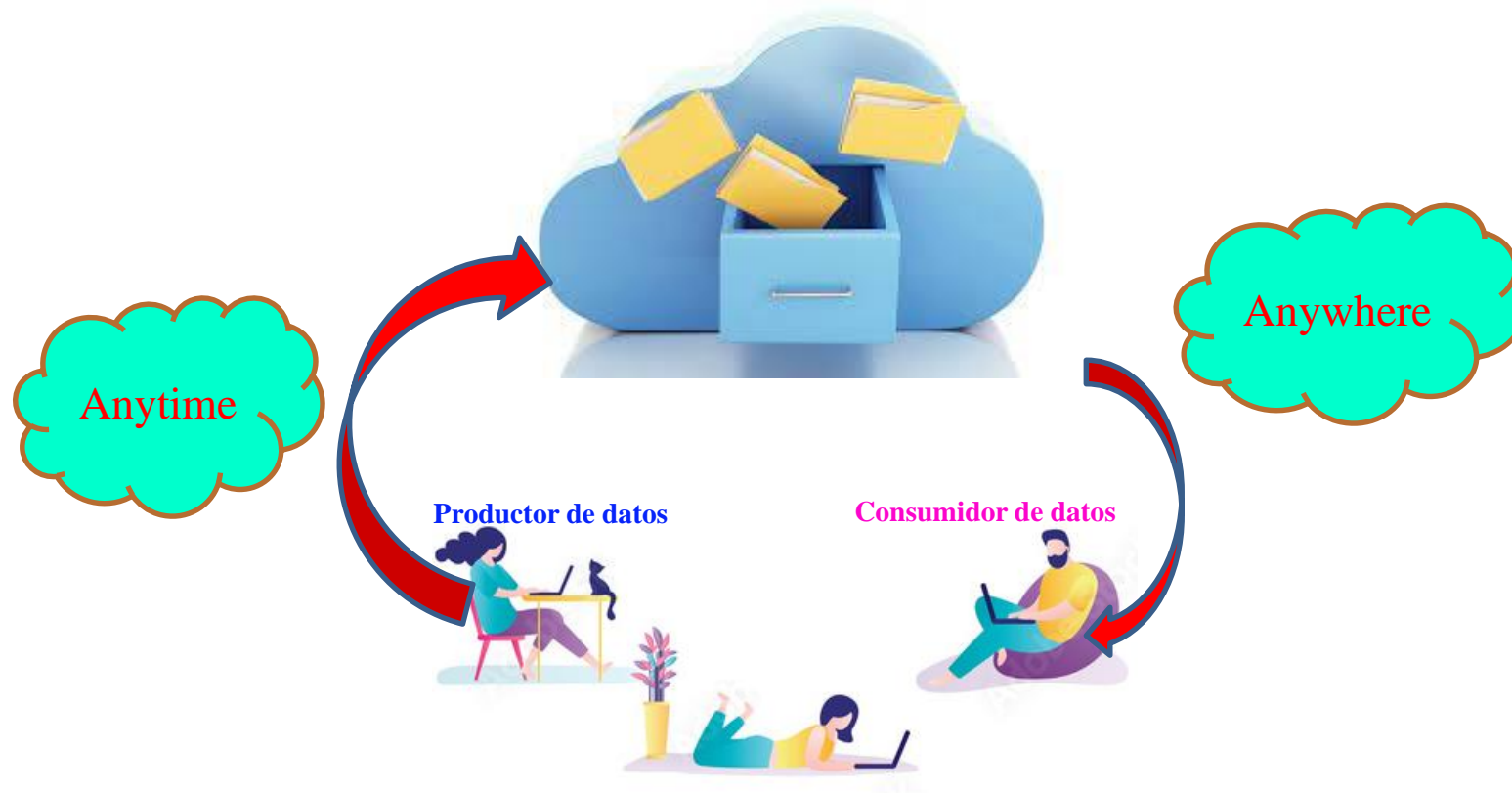


© Statista 2021



# Datos en la nube

- Almacenamiento y compartición de datos en la nube

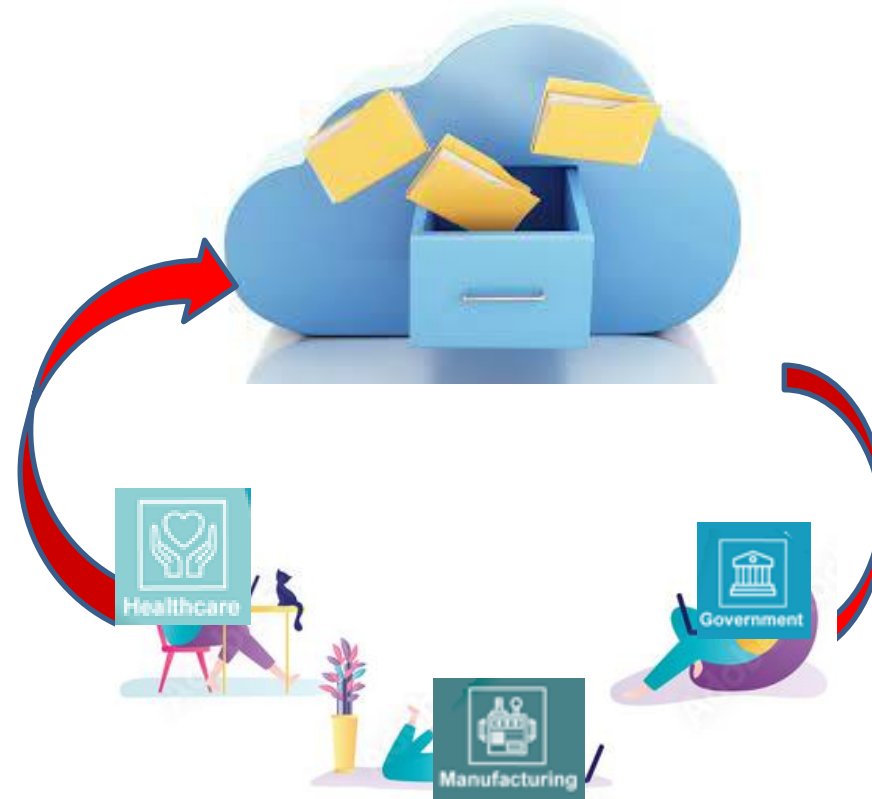


# Datos sensibles en la nube

- Almacenamiento y compartición de **datos sensibles en la nube**

Ejemplos:

- Registros médicos
- Datos personales
- Datos biométricos
- Datos empresariales/negocio
- Datos financieros



# Seguridad de datos sensibles en la nube

- Almacenamiento y compartición de datos **sensibles en la nube**



# Seguridad de datos sensibles en la nube

- Almacenamiento y compartición de datos **sensibles** en la **nube**

Servidor honesto pero curioso

Forbes MEXICO

Portada / Últimas Noticias /

**Javier Arreola**  
abril 26, 2016 @ 6:30 am

## Padrón electoral en la nube: ¿ciberproblemas a la mexicana?

*El 70% del tráfico de internet del mundo pasa por servidores en el norte de Virginia (EU), por lo que el padrón electoral filtrado en la nube de Amazon no será el último caso. ¿Podemos confiar en el uso que dan autoridades a nuestros datos?*

ad:

dad

esos no

ceso

una



# Seguridad de datos sensibles en la nube: un enfoque **criptográfico**



## Sobres digitales

# Seguridad de datos sensibles en la nube: un enfoque criptográfico



- Cifrado basado en atributos (ABE)
  - Cifrado asimétrico, “nuevo” (2005)
    - ...vs cifrado convencional (1976)
  - Fundamentada en la teoría de emparejamientos bilineales sobre grupos (estructuras algebraicas)
    - Grupo multiplicativo ( $*$  mod  $p$ )
    - Grupo aditivo (curvas elípticas)
      - Definido sobre un campo finito  $F_p$
      - Curvas con propiedades especiales

→  $p$  un número primo  $\geq 2,500$  bits

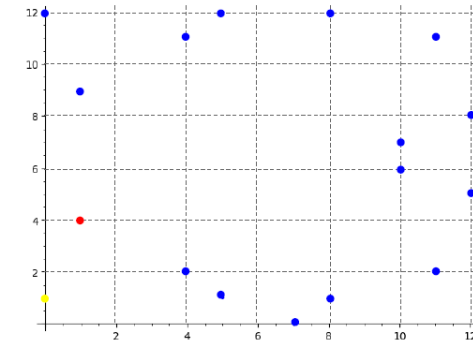
Por ejemplo p2048: 612 dígitos

```
25195908475657893494027183240048398571429282126204032027
77713783604366202077595556264018525880784406918290641249
51508218929855914917618450280848912007284499268739280728
77767359714183472702618963750149718246911650776133798590
95700097330459748808428401797429100642458691817195118746
12151517265463228221686998754918242243363725908514186546
20435767984233871847744479207399342365848238242811981638
15010674810451660377306056201619676256133844143603833904
41495263443219011465754445417842402092461651572335077870
77498171257724679629263863563732899121548314381678998850
40445364023527381951378636564391212010397122822120720357
```

# Seguridad de datos sensibles en la nube: un enfoque criptográfico



- Cifrado basado en atributos (ABE)
  - Cifrado asimétrico, “nuevo” (2005)
    - ...vs cifrado convencional (1976)
  - Fundamentada en la teoría de **emparejamientos bilineales** sobre grupos (*estructuras* algebraicas)
    - Grupo multiplicativo ( $*$  mod  $p$ )
    - Grupo aditivo (**curvas elípticas**)
      - Definido sobre un campo finito  $F_p$
      - Curvas con propiedades especiales



$$y^2 = x^3 + x + 1 \quad (\text{mód } 13).$$



$p$  un número primo  $\geq 224$  bits

# Control de acceso y confidencialidad: un enfoque criptográfico



- Cifrado basado en atributos (ABE)
  - Cifrado **1: M**
    - Cifra para un grupo de potenciales usuarios
    - ... vs criptografía convencional: con cifrado **1:1**  
Para M usuarios se requieren  
**M cifrados y M llaves por administrar.**

# Control de acceso y confidencialidad: un enfoque criptográfico

- Cifrado basado en atributos (ABE)
  - Tecnología relativamente nueva (2005)
    - Cifrado 1: M
  - Cada usuario es identificado por un conjunto de atributos (mapeados a estructuras algebraicas)

$$SK_u \leftarrow \text{KeyGen}(\text{attrs})$$



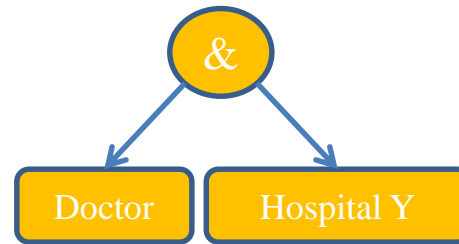
{Doctor, Hospital Y}



{Nurse, Hospital Z}

# Control de acceso y confidencialidad: un enfoque criptográfico

*Política = “doctor” & “Hospital Y”*



$SK_u \leftarrow \text{KeyGen}(\text{attrs})$



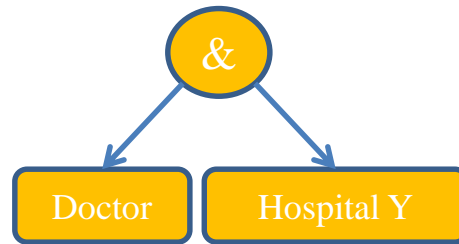
{Doctor, Hospital Y}



{Nurse, Hospital Z}

# Control de acceso y confidencialidad: un enfoque criptográfico

*Política = “doctor” & “Hospital Y”*



$SK_u \leftarrow \text{KeyGen}(\text{attrs})$



{Doctor, Hospital Y}



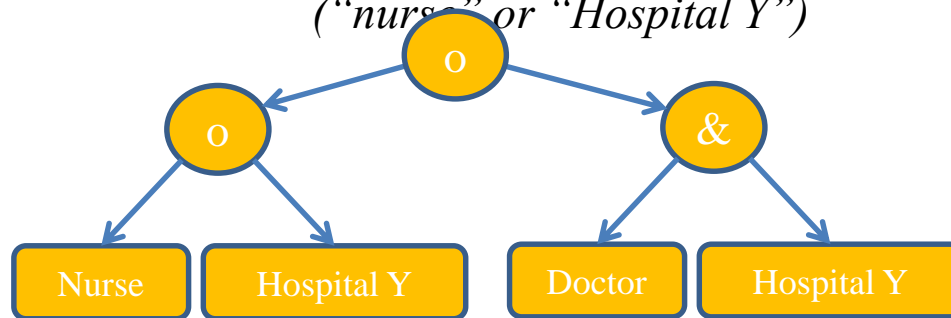
{Nurse, Hospital Z}

# Control de acceso y confidencialidad: un enfoque criptográfico

*Política = (“doctor” & “Hospital Y”)*

*or*

*(“nurse” or “Hospital Y”)*



{Doctor, Hospital Y}

$SK_u \leftarrow \text{KeyGen}(\text{attrs})$



{Nurse, Hospital Z}

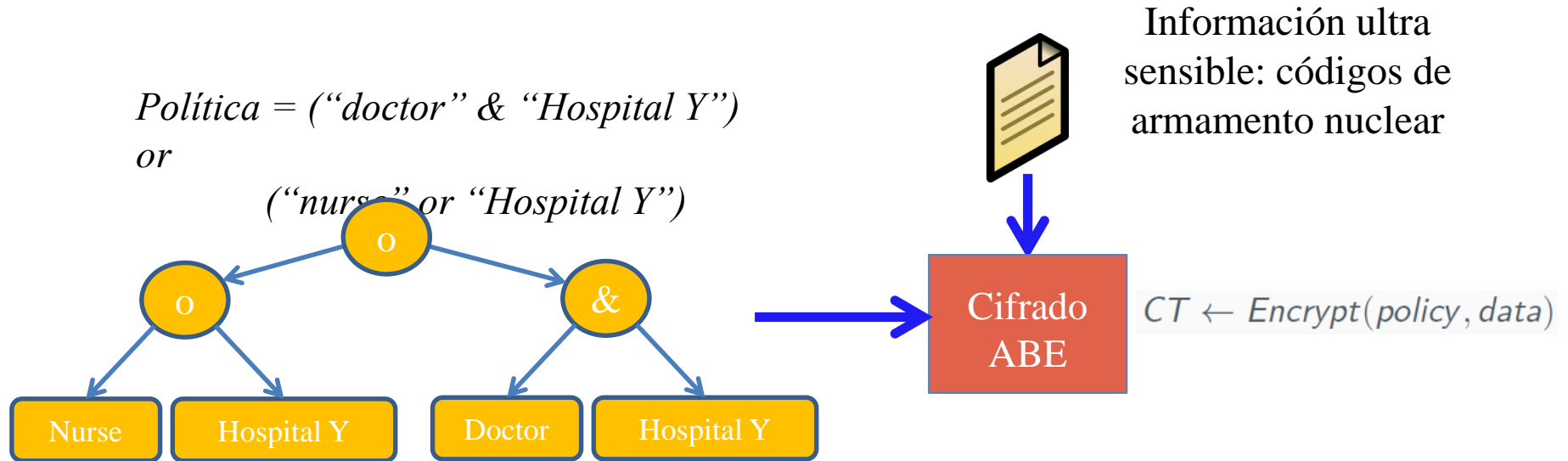


{Hospital Y}





# Control de acceso y confidencialidad: un enfoque criptográfico

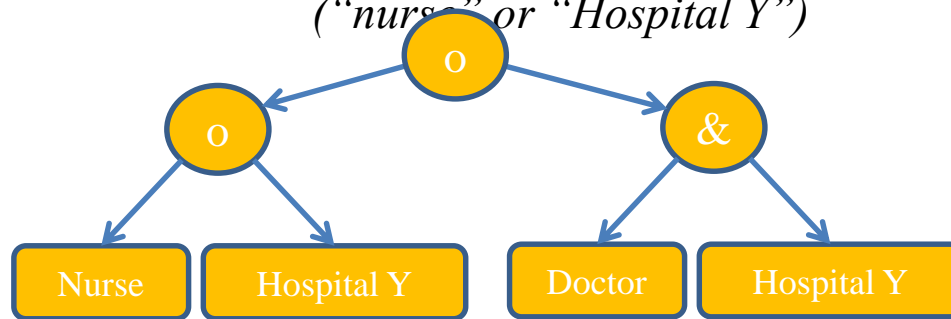


# Control de acceso y confidencialidad: un enfoque criptográfico

*Política = (“doctor” & “Hospital Y”)*

*or*

*(“nurse” or “Hospital Y”)*



Cifrado  
ABE

Datos no mayores al  
tamaño de  $p \approx 2500$  bits  
 $\approx$  **0.0001 Mb/seg**



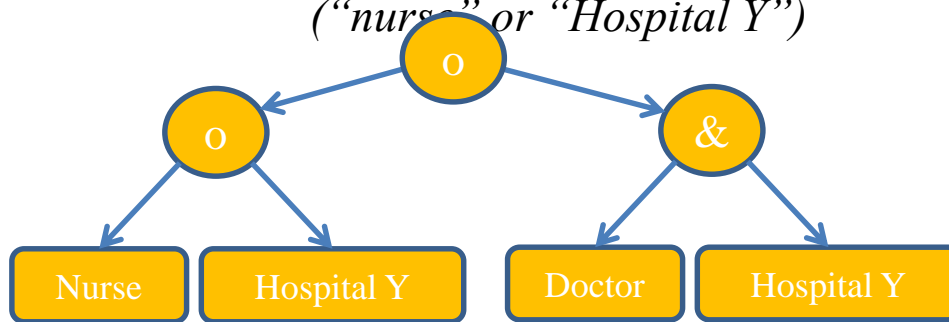
&%\$#’/()&&%%\$#  
”)=?\*i?)(/&%\$#’#%  
”&()/%\$#’!=)(&/(#=  
&%

# Control de acceso y confidencialidad: un enfoque criptográfico

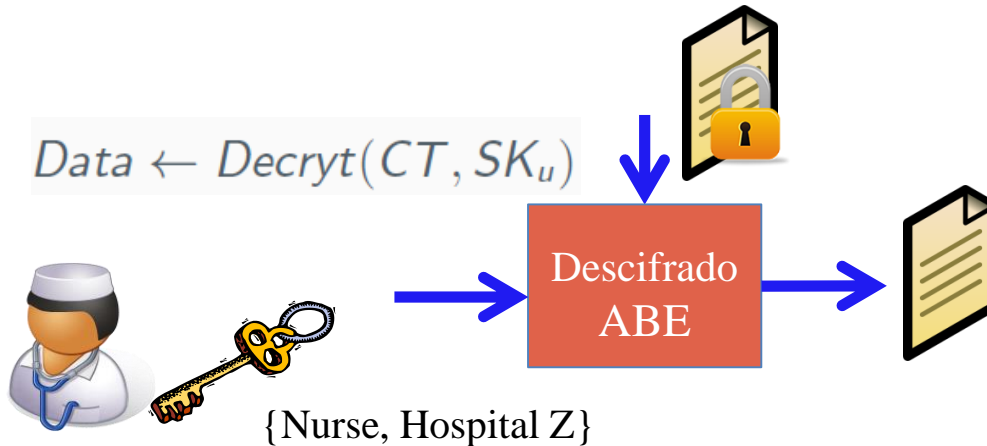
*Política = (“doctor” & “Hospital Y”)*

*or*

*(“nurse” or “Hospital Y”)*



$Data \leftarrow \text{Decrypt}(CT, SK_u)$



# Control de acceso y confidencialidad: un enfoque criptográfico



# Control de acceso y confidencialidad: un enfoque criptográfico



# Sobres digitales: confidencialidad y control de acceso.



El concepto de sobre digital existía en el contexto de cifrado convencional, pero no en el contexto de ABE

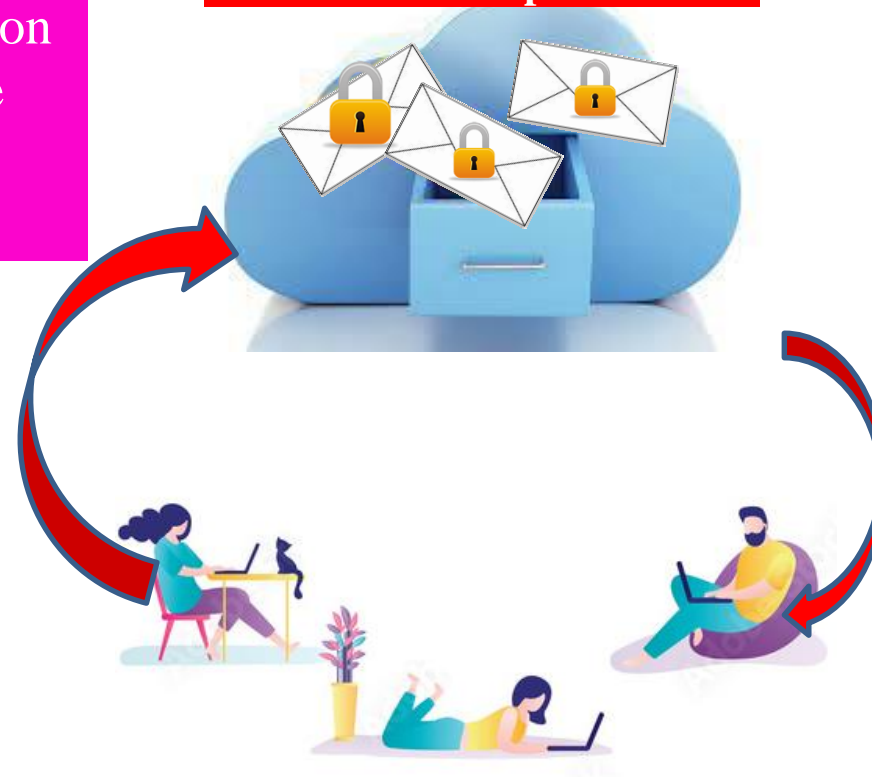
# Sobres digitales: **confidencialidad** y **control de acceso**.



# Sobres digitales: **confidencialidad** y **control de acceso**.

- Datos cifrados con control de acceso embebido

**Servidor honesto pero curioso**





# Sobres digitales: **confidencialidad** y **control de acceso**.

Regular Contribution

## A pairing-based cryptographic approach for data security in the cloud

[Miguel Morales-Sandoval](#) , [Jose Luis Gonzalez-Compean](#), [Arturo Diaz-Perez](#) & [Víctor J. Sosa-Sosa](#)

*International Journal of Information Security* **17**, 441–461 (2018) | [Cite this article](#)

**1020** Accesses | **13** Citations | [Metrics](#)

- Da  
cif  
con  
acc



# Sobres digitales: **confidencialidad y control de acceso.**

Digital Object Identifier 10.1109/ACCESS.2020.DOI

## A Three-Tier Approach for Lightweight Data Security of Body Area Networks in e-Health Applications

MIGUEL MORALES-SANDOVAL<sup>1</sup>, RICARDO DE-LA-PARRA-AGUIRRE<sup>1</sup>, HIRAM GALEANA-ZAPIEN<sup>1</sup>, (MEMBER, IEEE) AND ALEJANDRO GALAVIZ-MOSQUEDA<sup>2</sup>.

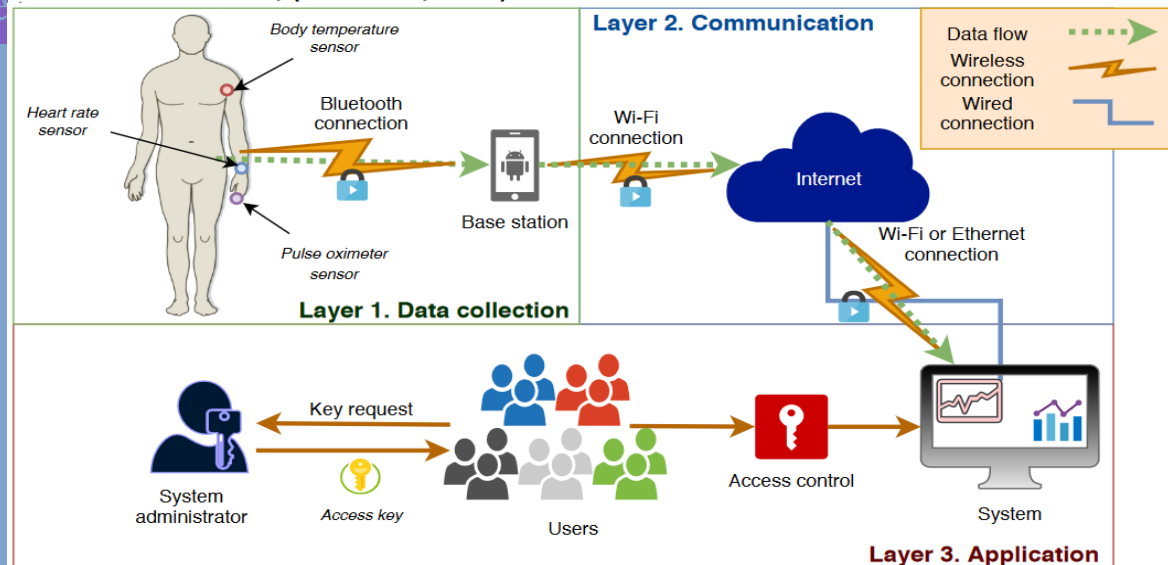


FIGURE 5: WBAN deployment based on the 3-layer model.

- Datos cifrados  
control de acceso

# Sobres digitales: **confidencialidad** y **control de acceso**.



# Sobres digitales buscables: confidencialidad, control de acceso y recuperación de datos.



# Sobres digitales buscables (con capacidades de búsqueda)

Received August 3, 2020, accepted September 2, 2020, date of publication September 16, 2020,  
date of current version September 25, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3023893

## Attribute-Based Encryption Approach for Storage, Sharing and Retrieval of Encrypted Data in the Cloud

MIGUEL MORALES-SANDOVAL<sup>1</sup>, MELISSA HINOJOSA CABELLO<sup>1</sup>,  
HEIDY MARISOL MARIN-CASTRO<sup>1,2</sup>, AND JOSE LUIS GONZALEZ COMPEAN<sup>1</sup>

<sup>1</sup>Center for Research and Advanced Studies of the National Polytechnic Institute (CINVESTAV), Tamaulipas, Ciudad Victoria 87130, Mexico

El proveedor  
del servicio  
no aprende  
nada de la  
consulta ni de  
los resultados

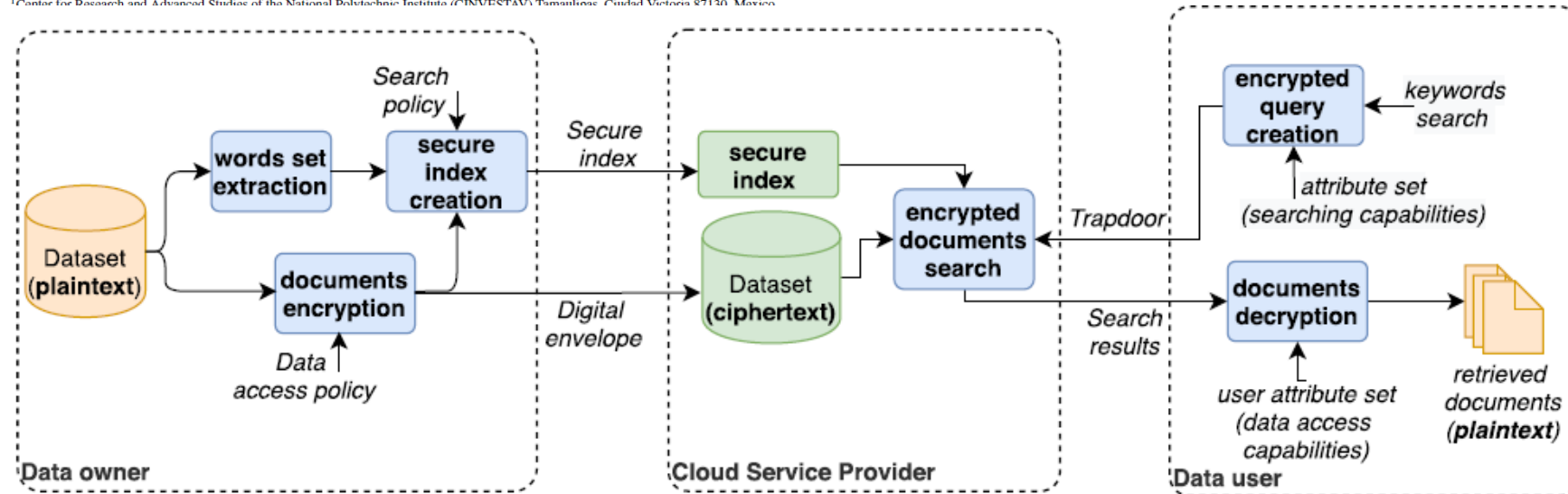


FIGURE 1. System model for document sharing and retrieval in the cloud.

# Sobres digitales con capacidades de búsqueda

TABLE 4. Main components of FABECS construction (Type-III pairing).

	CP-ABSE Type-III	DET-ABE Type-III
A	Matrix, with Linear secret sharing scheme and FBF access policy	
$P_\lambda$	$\{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, \tau\}, H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1, H_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_r$	
$PK_\lambda$	$\{h = g_1^\beta, e(g_1, g_2)^\alpha\}, \{\alpha, \beta\} \in \mathbb{Z}_r^*$ (random)	
$MK_\lambda$	$\{g_1^\alpha\}$	
SK	$SK_u = \{D, D', [d_y]^+\}$ , where $D = g_1^{(\alpha+\beta r)}$ $D' = g_2^r$ $\forall j \in S_u:$ $d_j = H_1(y)^r, r \in \mathbb{Z}_r^*$ (random)	
CT	$CT_w = \{C', C, [C_{y_i}, C'_{y_i}]^+\}$ , where $w$ is a keyword and $C' = e(g_1^{H_2(w)s}, g_2) \times e(g_1, g_2)^{\alpha s}, s \in \mathbb{Z}_r^*$ (random)	$CT_k = \{C', C, [C_{y_i}, C'_{y_i}]^+\}$ , where $k$ is a symmetric key and $C' = k \times e(g_1, g_2)^{\alpha s}, s \in \mathbb{Z}_r^*$ (random)
	$C = g_2^s$ $\forall \rho(i)$ , attribute $y$ at row $\text{Mat}_i$ $C_{y_i} = g_2^{r_i}$ $C'_{y_i} = h^{\lambda_i} \times H_1(\rho(i))^{-r_i}$ $r_i \in \mathbb{Z}_r^*$ (random) $\lambda_i = \mathbf{v} \times \text{Mat}_i$ $\mathbf{v} = \{s, s_1, s_2, \dots, s_{n-1}\}, s_j \in \mathbb{Z}_r^*$ (random)	
$T_u$	$T_u(w_q) = \{T, T', [t_y]^+\}$ , given a query keyword $w_q$ and $SK_u$ , where $T = g_1^{H_2(w_q)} \times D$ $T' = D' \in SK_u$ $t_y = d_y \in SK_u$	Not required
Decrypt or Search	Search, given $CT_w = \{C', C, [C_{y_i}, C'_{y_i}]^+\}$ and $T_u(w_q) = \{T, T', [t_y]^+\}$ $C_w = \frac{e(T, C)}{C_T}$ $\prod ((e(C'_{y_i}, T')e(t_{y_i}, C_{y_i}))^{\omega_i}) = \frac{C_w}{C_T}$ if and only if $C_w \equiv C'$ then $w$ matches $w_q$	Decrypt the symmetric key $k$ , given $CT_k = \{C', C, [C_{y_i}, C'_{y_i}]^+\}$ and $SK_u = \{D, D', [d_y]^+\}$ $C_k = \frac{e(D, C)}{C_T}$ $\prod ((e(C'_{y_i}, D')e(d_{y_i}, C_{y_i}))^{\omega_i}) = \frac{C_k}{C_T}$ $k_1 = \frac{C'}{C_k}$

- Grupos aditivos definidos por una curva elíptica (sobre un campo finito de orden un número primo grande).
- Emparejamientos bilineales asimétricos
- Funciones hash
- Esquemas de repartición de secretos

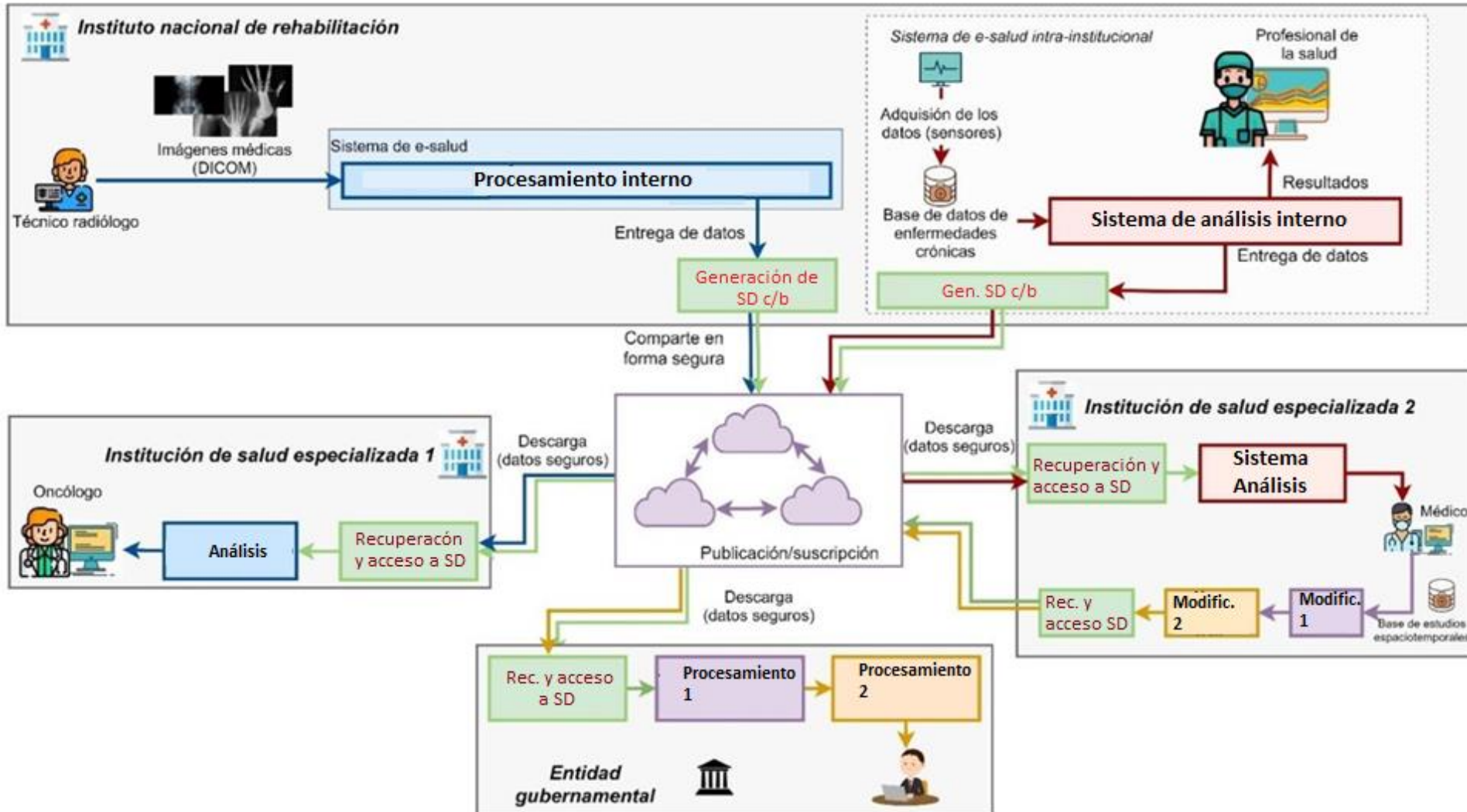
# Caso de aplicación

- FORDECyT Salud 2020 - Proyecto 41756
- Plataforma tecnológica para la gestión, **aseguramiento**, intercambio y preservación de grandes volúmenes de datos en salud y construcción de un repositorio nacional de servicios de análisis de datos de salud.



# Caso de aplicación

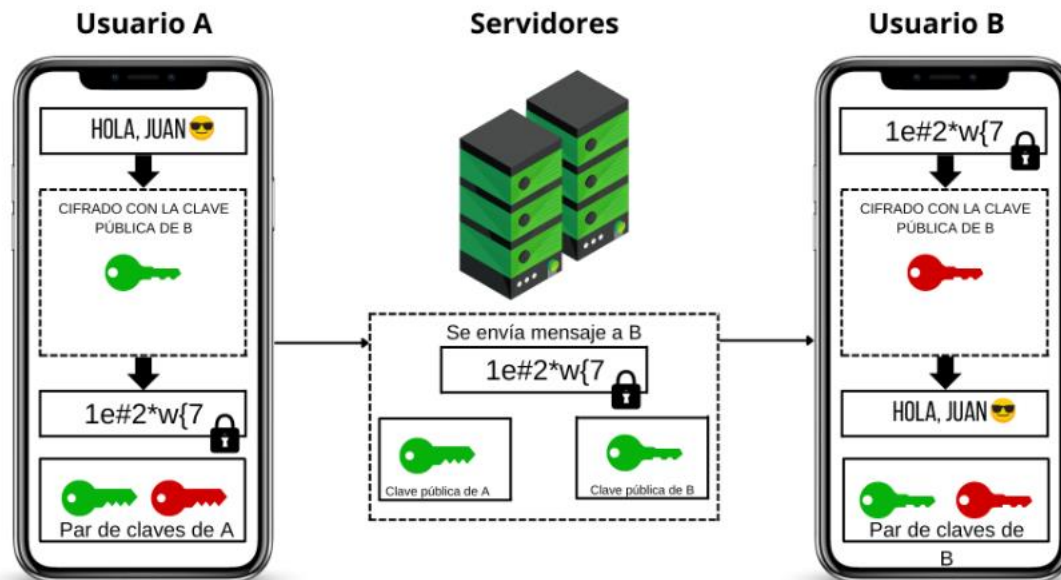
FORDECyT Salud 2020 - Proyecto 41756





## Reto 2: Cómputo cuántico

- En el cifrado asimétrico, parte fundamental en las comunicaciones seguras, cada entidad cuenta con un par de claves:

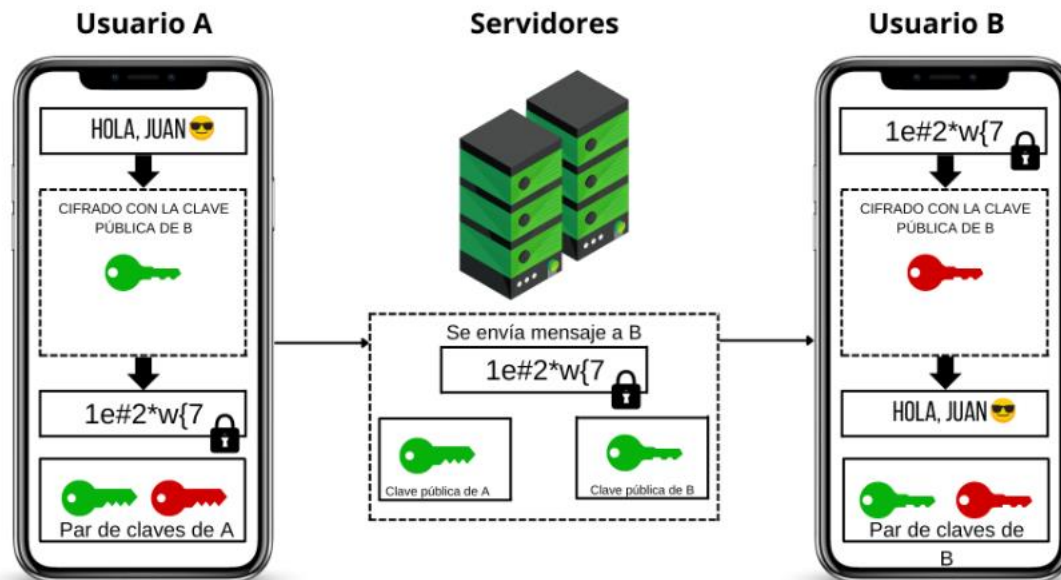


Cualquiera puede cifrar datos, con la **llave pública** del destinatario.

Solo el destinatario, con su **llave privada**, puede descifrar los mensajes.

# Reto 2: Cómputo cuántico

- En el cifrado asimétrico, parte fundamental en las comunicaciones seguras, cada entidad cuenta con un par de claves:



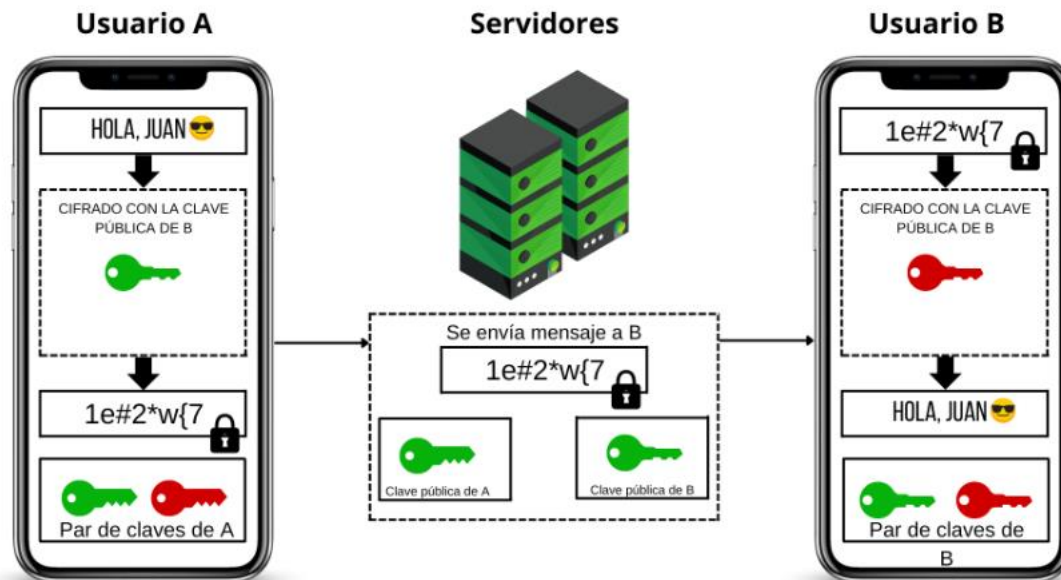
Cualquiera puede cifrar datos, con la **llave pública** del destinatario.

Solo el destinatario, con su **llave privada**, puede descifrar los mensajes.

$$\text{Llave pública} = f(\text{llave privada})$$

## Reto 2: Cómputo cuántico

- En el cifrado asimétrico, parte fundamental en las comunicaciones seguras, cada entidad cuenta con un par de claves:



Cualquiera puede cifrar datos, con la **llave pública** del destinatario.

Solo el destinatario, con su **llave privada**, puede descifrar los mensajes.

$$\text{Llave pública} = f(\text{llave privada})$$

La seguridad del cifrado depende de la dificultad para calcular  $f^{-1}$

## Reto 2: Cómputo cuántico

- En 1994, Peter Shor descubrió que, si alguna vez se inventaran las computadoras cuánticas, se contarían con algoritmos de complejidad polinomial que pudieran resolver problemas para los que ahora solo se cuentan con algoritmos no polinomiales.
  - Incluidos los algoritmos para calcular  $f^{-1}$

$$\text{Llave pública} = f(\text{llave privada})$$

La seguridad del cifrado  
depende de la dificultad para  
calcular  $f^{-1}$

## Reto 2: Cómputo cuántico

- En 1994, Peter Shor descubrió que, si alguna vez se inventaran las computadoras cuánticas, se contarían con algoritmos de complejidad polinomial que pudieran resolver problemas para los que ahora solo se cuentan con algoritmos no polinomiales.
  - Incluidos los algoritmos para calcular  $f^{-1}$
- Esa posibilidad ha hecho que se desarrolle una nueva LGAC
  - Criptografía post-cuántica
  - Algoritmos criptográficos que resistan a estos ataques, es decir, que sean “quantum safe”
  - Se estima que en 2030 se contará con una computadora cuántica con suficiente poder de cómputo para atacar a los actuales cifradores.

$$\text{Llave pública} = f(\text{llave privada})$$

La seguridad del cifrado depende de la dificultad para calcular  $f^{-1}$

## Reto 2: Cómputo cuántico

- El pasado mes de septiembre, se publicaron nuevos algoritmos recomendados para PQC (NIST)
  - Basado en una competencia, iniciada en 2016

Llave pública =  $f$  (llave privada)

La seguridad del cifrado  
depende de la dificultad para  
calcular  $f^{-1}$

## Reto 2: Cómputo cuántico

- Los algoritmos criptográficos actuales que garantizan la CIA, y esquemas como los que se han usado para sobres digitales en la seguridad de Big data, deberán migrar a construcciones “quantum safe”
  - Antes de Y2Q (2030)
  - EEUU, China y Rusia, a la cabeza en la migración

$$\text{Llave pública} = f(\text{llave privada})$$

La seguridad del cifrado  
depende de la dificultad para  
calcular  $f^{-1}$

# Reto 2: Cómputo cuántico

INNOVATION

## Why Companies Must Act Now To Prepare For Post-Quantum Cryptography



Ted Shorter Forbes Councils Member

Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

Feb 11, 2022, 07:45am EST

Llave pública =  $f$  (llave privada)

La seguridad del cifrado depende de la dificultad para calcular  $f^{-1}$



# Reto 2: Cómputo cuántico



$$\text{Llave pública} = f(\text{lave privada})$$

La seguridad del cifrado  
depende de la dificultad para  
calcular  $f^{-1}$

# Reto 2: Cómputo cuántico

INNOVATION

Why Companies Must Act Now  
To Prepare for the Post-Quantum Cryptography  
Transition

NATIONAL  
CYBERSECURITY

Forbes  
Technology  
Council

## Data security: post-quantum cryptography transition underway

[uaga, Olivier](#)

Security experts are helping organizations to phase in solutions for protecting communications data in a post-quantum world.

7 October 2022

Llave pública =  $f$  (llave privada)

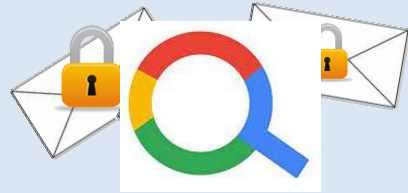
La seguridad del cifrado  
depende de la dificultad para  
calcular  $f^{-1}$

# Líneas de trabajo actuales

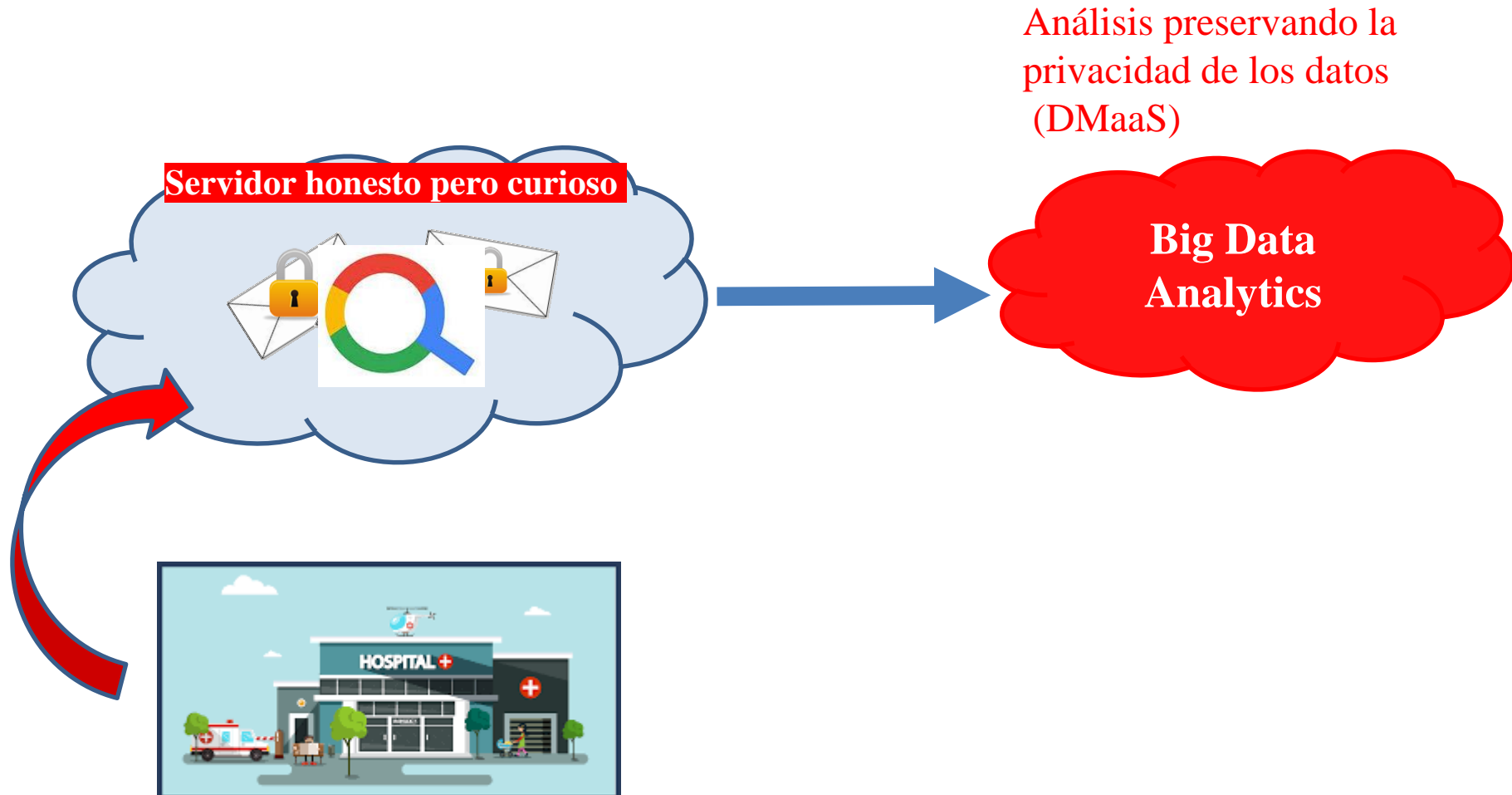
- PQC en dispositivos con pocos recursos de cómputo
  - Basado en látrices (retículas)
  - Para dispositivos con pocos recursos computacionales
    - En el Internet de las Cosas (nodos sensores)
      - Internet de las cosas médicas
      - Internet de las cosas industriales
  - Compartición de secretos
  - Firmas digitales

# Líneas de trabajo actuales

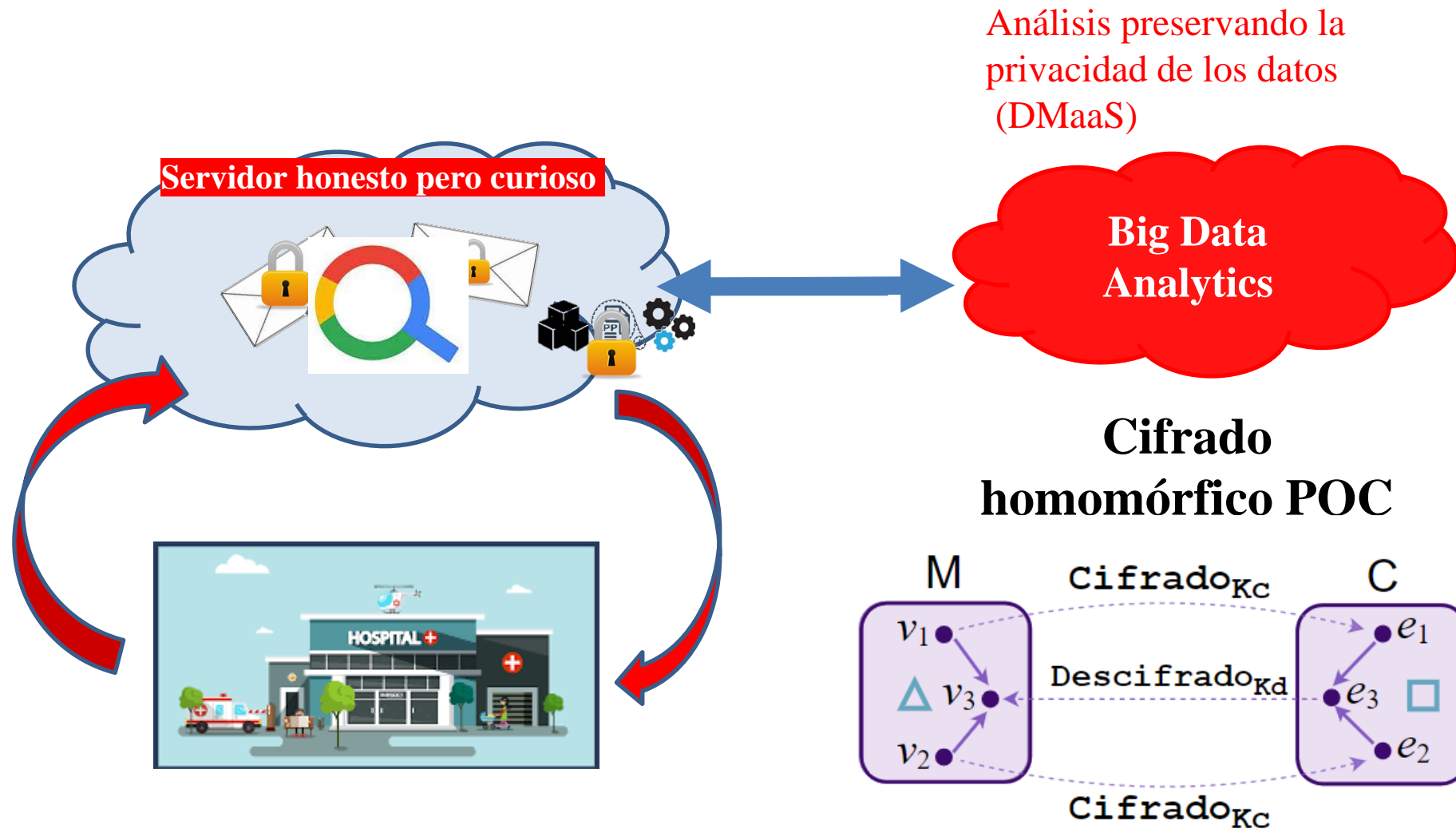
**Servidor honesto pero curioso**



# Líneas de trabajo actuales



# Líneas de trabajo actuales



# Comentarios finales



- El cifrado sigue siendo una tecnología vigente, que permite proveer servicios de seguridad en entornos donde los datos (manejo y procesamiento) son sensibles.
  - Incluso por regulaciones, los datos deben mantenerse privados.
- El cifrado convencional no es adecuado en datos en salud
  - Se requiere cifrado 1:M
- El cifrado, debe ser seguro y eficiente. De lo contrario, no es viable en un sistema de ciencia de datos.

# Comentarios finales



- La seguridad de datos es la última línea de defensa
  - Si el atacante irrumpe en un sistema, los datos, si están cifrados, son inutilizables
- El Big data impone retos relacionadas con la eficiencia, la seguridad y el acceso a datos a gran escala, las soluciones tradicionales no son suficientes
  - Privacidad bajo el control del propietario de datos
- El cómputo cuántico permitirá resolver problemas de alto impacto, pero también atacar a la mayoría de los criptosistemas de clave pública
  - La transición a PQC es necesaria



**¡Gracias!**

Miguel Morales Sandoval  
[miguel.morales@cinvestav.mx](mailto:miguel.morales@cinvestav.mx)





**ECORFAN®**

© ECORFAN-Mexico, S.C.

No part of this document covered by the Federal Copyright Law may be reproduced, transmitted or used in any form or medium, whether graphic, electronic or mechanical, including but not limited to the following: Citations in articles and comments Bibliographical, compilation of radio or electronic journalistic data. For the effects of articles 13, 162,163 fraction I, 164 fraction I, 168, 169,209 fraction III and other relative of the Federal Law of Copyright. Violations: Be forced to prosecute under Mexican copyright law. The use of general descriptive names, registered names, trademarks, in this publication do not imply, uniformly in the absence of a specific statement, that such names are exempt from the relevant protector in laws and regulations of Mexico and therefore free for General use of the international scientific community. BIMES is part of the media of ECORFAN-Mexico, S.C., E: 94-443.F: 008- ([www.ecorfan.org/booklets](http://www.ecorfan.org/booklets))