

**XIII
JORNADAS
STIC
CCN-CERT**



La Criptografía por las Nubes

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT



Jorge Dávila Muro

ETSI Informáticos UPM

jdavila@fi.upm.es

Índice

1. ¿Comprar o Alquilar?
2. La Seguridad en la Nube
3. Los Beneficios y Riesgos de las Nubes
4. El cifrado
5. Los HSMs
6. Conclusiones

Modas en la Computación

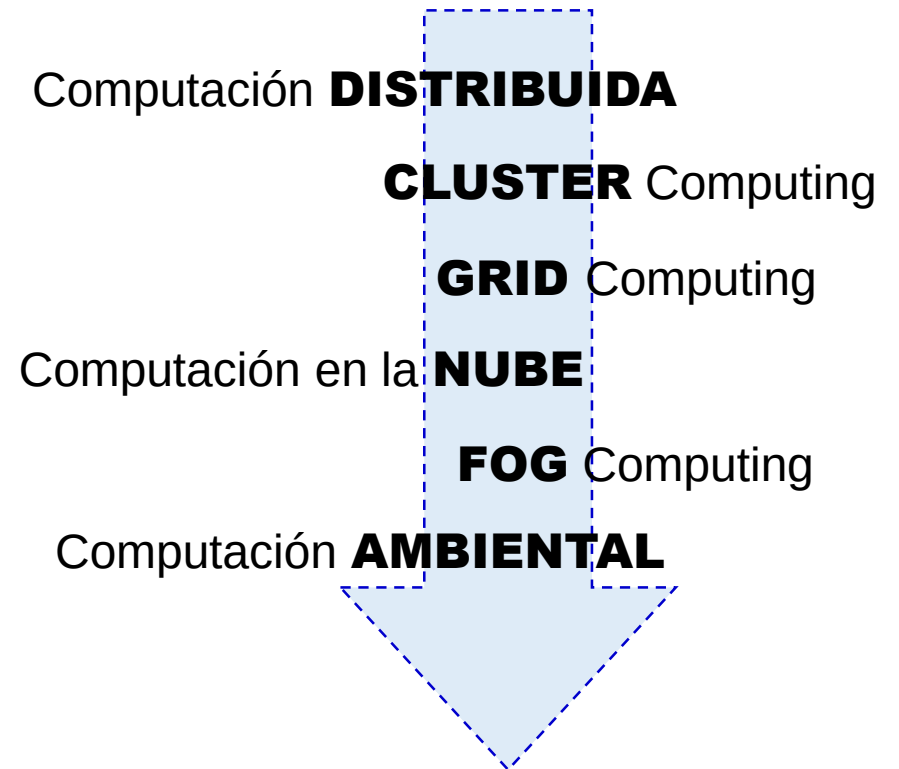
1969: Cuatro nodos ARPANET se conectan en circuitos de 50 kbit/s:

- Universidad de California en Los Ángeles
- Stanford Research Institute
- Universidad de California en Santa Bárbara
- Universidad de Utah.

1996: Un documento interno de **Compaq** acuña la expresión "*cloud computing*".

2006: Amazon.com saca al mercado y populariza su producto **Elastic Compute Cloud (EC2)**.

2013: Google lanza al Mercado su producto **Google Compute Engine**.

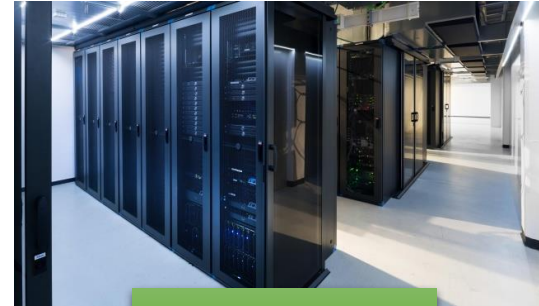


¿Comprar o Alquilar?

La eterna disyuntiva...

- Mantener el **control** requiere algo más que dinero (*know how*).
- El **control** de lo que se calcula y con qué se calcula, **se pierde en las nubes**.
- La **responsabilidad** siempre se mantiene.

¿Tiene sentido asumir una responsabilidad sin tener control real sobre ella?



in House

COMPRAR

INSIDER RISK

- Electricidad
- Mantenimiento
- Personal
- Seguridad
- Auditoria
- Controles

Control y

Responsabilidad
TOTAL



in Cloud

ALQUILAR

PROVIDER RISK

- Utilizar
- Pagar

INSIDER RISK

Responsabilidad
TOTAL

Medidas de seguridad en la Nube

Desde el punto de vista del **proveedor**:

Objetivo: Ofrecer una experiencia de espacio **privado** en unas instalaciones **publicas**.

- Aislamiento de Redes
- Aislamiento de Aplicaciones
- Micro segmentación
- Cifrado de los datos
- Actualizaciones y Parches
- Herramientas Dev Ops
- Monitorización continua
- Defensas tradicionales

INSIDER RISK

Virtualización = Abstracción:

De los detalles de implementación
(hardware y SO)

De los detalles de ejecución
(multitarea, multiusuario)



Modelos disponibles

- **Hipervisor** + SO propio + Aplicaciones
- SO común + **Docker**+ Aplicaciones
- **Docker** empaqueta una aplicación y sus dependencias en un contenedor virtual que puede correr en cualquier servidor Linux.
- Permite ejecutarse **en varias ubicaciones** (on-premises, public cloud, o private cloud).

Beneficios de trabajar en la Nube

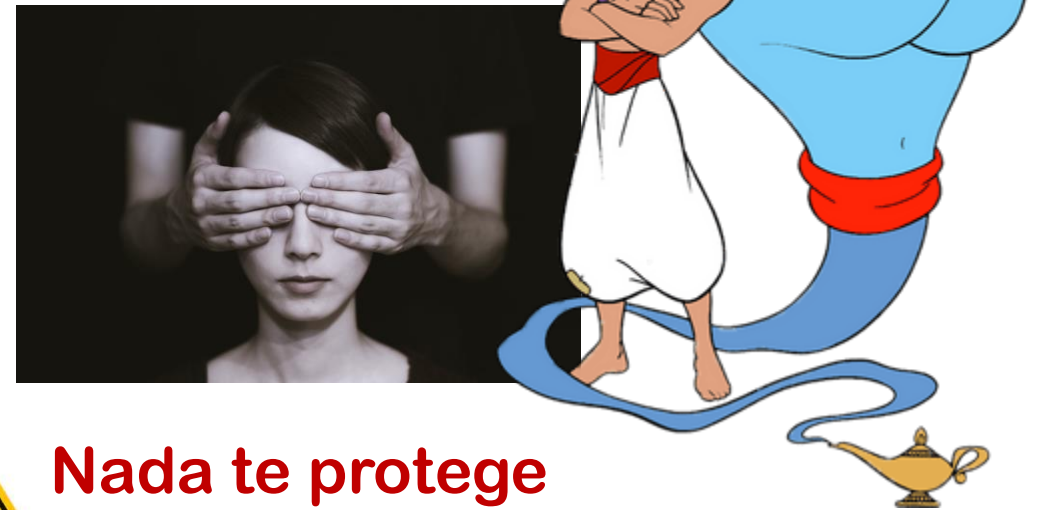
- Pago por uso.
- Ajuste dinámico y puntual con la demanda.
- Entorno abstracto y muy simplificado.
- No hay inversión inicial ni mantenimiento de instalaciones.
- Uso colectivo de instalaciones y personal especializado.
- Seguridad comunitaria.
- Actualizaciones automáticas.
- Disponibilidad inmediata en plataformas, software y servicios.
- Acceso desde cualquier parte de Internet.
- **Despreocupación.**



Riesgos de trabajar en la Nube

No podía ser todo tan bonito...

- Se adquieren **dependencias estratégicas**.
- Fuerte asimetría en el **reparto de los riesgos y consecuencias**.
- Dependencia permanente de la conectividad y las redes.
- Te sometes a **soberanías ajenas** al aceptar de facto la deslocalización (*gag orders*).
- “*Lo que se da no se quita*”.
- No sabes realmente lo que ocurre.
- **Confianza ciega** en los proveedores.



**Nada te protege
del Proveedor.**

La esencia del Cifrado

Ocultar en el caos lo que importa ...

Cifrado;

Transformación **reversible** de **algo que contiene Información** en **algo que carece de ella**,...

para quien no conozca la **Clave** criptográfica correcta.

Un criptograma seguro tiene que ser **indistinguible** de una secuencia **Aleatoria Uniformemente Distribuida**.



Sistemas de Cifrado

A la búsqueda de un buen algoritmo...

- Familia de funciones que relacionan mensajes en claro y criptogramas.

Cifrado $c = E(k_e, m)$

Descifrado $m = D(k_d, c)$

- Es seguro si el único modo de encontrar la clave utilizada es probar todos sus posibles valores (**Ataque por Fuerza Bruta**).
- La seguridad del sistema de cifrado emana de que:
 - El número de posibles claves sea **inabarcable**.
 - Que la clave se genere en **Secreto**, de forma **Uniforme** y completamente al **Azar**.
 - Que la clave opere y se destruya siempre en el más absoluto secreto.**



Auguste Kerckhoffs

La seguridad del sistema recae exclusivamente en la seguridad de la clave, debiéndose suponer conocidos por todos el resto de los parámetros del sistema criptográfico.

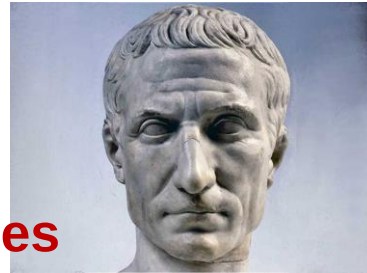
Implementación del Cifrado

¿Cómo lo hago?

- Método de Cesar

$$c = (m + \mathbf{b}) \bmod |A|$$

$$|A| = \mathbf{27 \text{ posibilidades}}$$



- Cifrado Afín

$$C = (\mathbf{a} \cdot m + \mathbf{b}) \bmod |A|$$

18 valores de a y 27 valores de b,

$$18 \times 27 = \mathbf{486 \text{ posibilidades}}$$

$$\mathbf{27! =}$$

$$10.888.869.450.418.352.160.768.000.000$$

$$\approx \mathbf{10^{28}}$$

- Cifrado Vigenere y clave de 20 letras

$$C = (m + \mathbf{k}_i) \bmod |A|$$

$$27^{20} \sim 4 \times \mathbf{10^{28} \text{ posibilidades}}$$

moléculas en 1,25 Toneladas de agua



- La maquina ENIGMA de la WW II tenía una complejidad de

$$2^{25} \sim 3 \times \mathbf{10^7 \text{ posibilidades}}$$



- Mínima seguridad actual es de 112 bits

$$2^{112} \sim 5 \times \mathbf{10^{33} \text{ posibilidades}}$$

5.192,3 Quintillones europeos

Cifradores Modernos

Hay donde elegir...

Algoritmos comunes:

AES, Blowfish, Triple DES, Serpent, Twofish

Algoritmos menos comunes:

Camellia, CAST-128, GOST, IDEA, RC2, RC5, RC6, SEED, ARIA, Skipjack, TEA, XTEA

Cajón de sastre:

3-Way Akelarre Anubis BaseKing BassOmatic BATON BEAR and LION CAST-256 Chiasmus CIKS-1 CIPHERUNICORN-A CIPHERUNICORN-E CLEFIA CMEA Cobra COCONUT98 Crab Cryptomeria/C2 CRYPTON CS-Cipher DEAL DES-X DFC E2 FEAL FEA-M FROG G-DES Grand Cru Hasty Pudding cipher Hierocrypt ICE IDEA NXT Intel Cascade Cipher Iraqi Kalyna KASUMI KeeLoq KHAZAD Khufu and Khafre KN-Cipher Kuznyechik Ladder-DES Libelle LOKI (97, 89/91) Lucifer M6 M8 MacGuffin Madryga MAGENTA MARS Mercy MESH MISTY1 MMB MULTI2 MultiSwap New Data Seal NewDES Nimbus NOEKEON NUSH PRESENT Prince Q RC6 REDOC Red Pike S-1 SAFER SAVILLE SC2000 SHACAL SHARK Simon SM4 Speck Spectr-H64 Square SXAL/MBAL Threefish Treyfer UES xmx XXTEA Zodiac



Bloque de datos: **128 bits**

Longitud de las Claves: **128, 192 y 256 bits**

Velocidad de operación: **2,5 Gbs⁻¹ (335 MBs⁻¹)**



$$2^{128} \approx 10^{38}$$

$$2^{192} \approx 10^{57}$$

$$2^{256} \approx 10^{77}$$

$$2^{384} \approx 10^{115}$$

$$2^{512} \approx 10^{154}$$

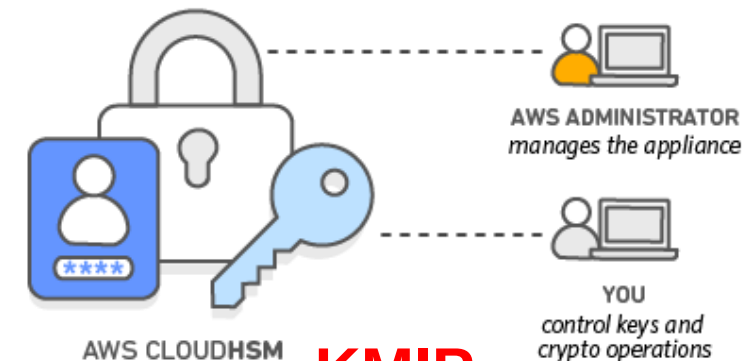
Hardware Security Modules

El bastionado hardware en una era global, etérea e intangible

- Son vestigios caros de un pasado físico y material.
- Dispositivo que salvaguarda y maneja claves.
- Aporta autenticación fuerte y cierta capacidad de proceso.
- Contienen varios chips criptoprocesadores con mecanismos Tamper Resistant.
- Gestionan el ciclo completo de la vida de las claves.



cloudHSM



AWS CLOUDHSM

KMIP

¿Es realmente segura su gestión?

NO si las claves pueden salir y operar fuera de sus límites físicos y lógicos.

Por qué no se debe hacer criptografía en la nube

- Todo lo digital se **copia sin dejar rastros**.
- **Imposible control** del número de copias que hay de las claves y de quién las tiene.
- Una vez se hace algo público, es **imposible convertirlo en privado**.
- La mala criptografía da una **falsa sensación de seguridad**.
- ¿Para qué cifrar si se les da la información en claro?



En las nubes depositar sólo objetos cifrados que nunca se descifran en ellas (Almacenamiento, Transporte, Intercambio).

Conclusiones

- El procesamiento de los datos tiene que hacerse con sus versiones en claro.
- Si el cifrado y descifrado se hace en la nube, entonces la nube tiene que conocer las claves.
- Lo etéreo y dinámico de la nube anula la cualidad esencial de los HSM (Perímetros HW bastionados)
- Hay que **cambiar los modos de calcular** e incluir una **Anonimización** robusta.
- El almacenamiento en la nube **sólo es seguro si está cifrado por uno mismo**.



La Criptografía
sobra

Contradicción
in terminis

La profesión de fe
ciega en una
teoría no es una
virtud sino un
crimen intelectual

Imre Lakatos



CRIPTOGRÁFICA

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional