

Uso de Álgebras Modernas para Seguridad y Criptografía

Implementación de **criptografía** de
clave pública para **protección** de
comunicaciones y **almacenamiento**
de datos con IoT en
entornos de monitoreo
y consumo de energía

} /> [

Equipo

A00830952	Jose Alfredo García Rodríguez
A01570576	Daniel De Zamacona Madero
A00830383	Verónica Victoria García De la Fuente
A00832401	Jose Miguel Perez Flores
A01379097	Karla Susana Olvera Vázquez
A01720932	Eugenio Santisteban Zolezzi

</ Contenidos

{01}

Acerca del Reto

{02}

Solución Propuesta

{03}

Metodología

{04}

Resultados

{05}

Conclusiones y
Trabajo Futuro

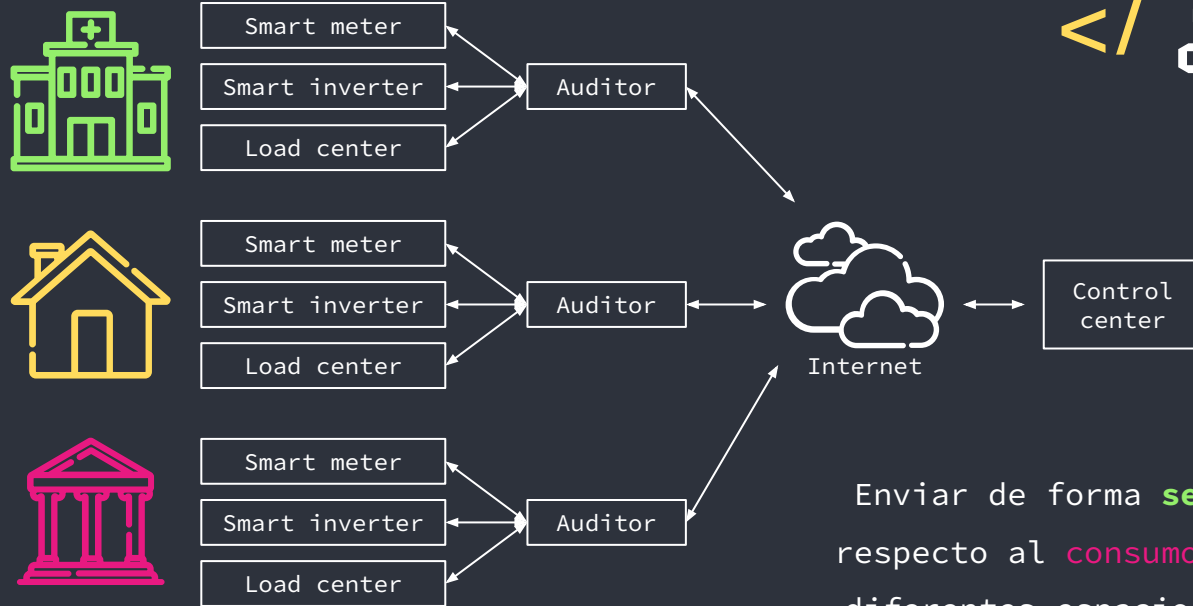
</>

Acerca del Reto

01

} /> [

</ ¿Cuál es el problema?



Enviar de forma **segura** la información con respecto al **consumo de energía** eléctrica en diferentes espacios con el fin de abrir la posibilidad de procesarla, almacenarla y generar **nuevo conocimiento**.

- Mediciones en **tiempo real** del consumo y producción de electricidad
- Estos datos deben ser enviados **encriptados** a un Centro de Control para su análisis
- Centro de Control debe poder **verificar la procedencia** de los datos
- Los datos son encriptados y **guardados en una base de datos**

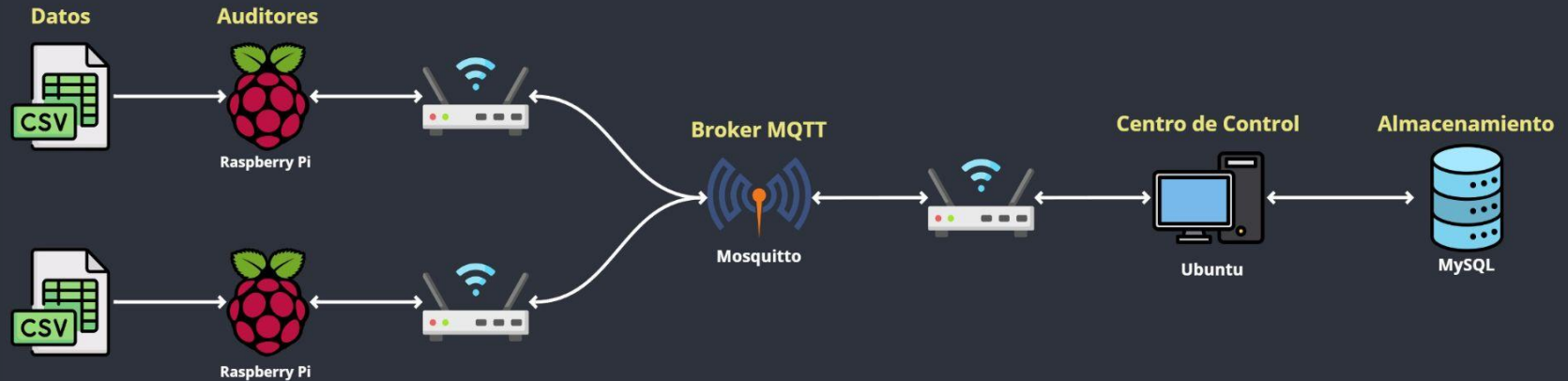
</ Puntos
importantes }

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

02

</ Solución Propuesta />

</ Arquitectura



1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1

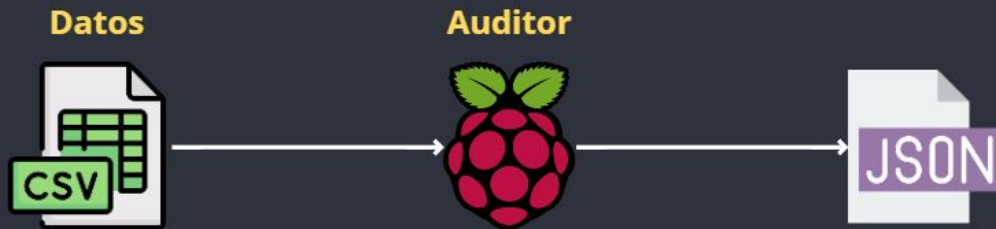
</>

Metodología

03

} /> [

</ Preparación de Datos

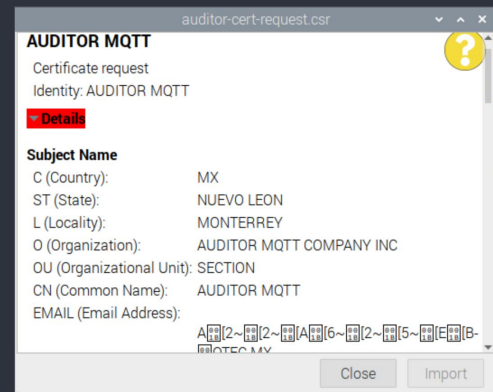
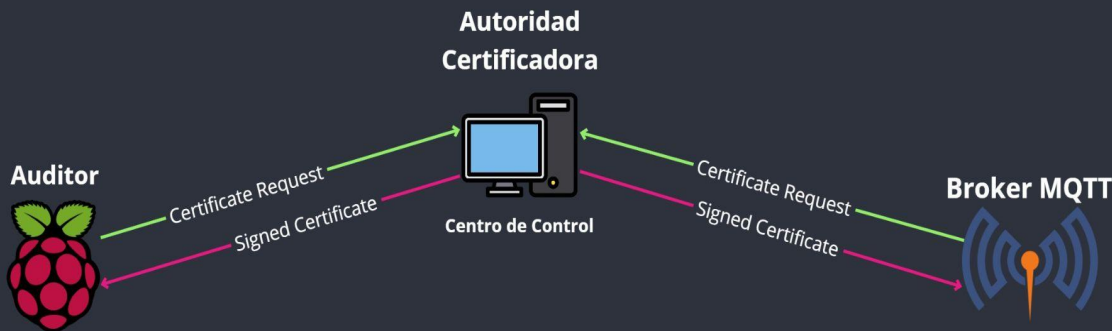


```
{'trace_id': '011',  
'timestamp': '2013-11-02T00:00:00Z',  
'C(0)/P(1)': '0',  
'value': 58.0}
```

</ Certificados

Un certificado **SSL** (Secure Sockets Layer) es un certificado digital que autentica la identidad de un cliente y permite una conexión cifrada. **SSL** es un protocolo de seguridad que crea un enlace encriptado entre un servidor y un cliente.

Certificados **autofirmados** Creados usando **openSSL**,
firmados con **ECDSA**



1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 1 1 1 0 1

</ Encriptado de los datos



Boot-up

El CC genera un par de claves RSA por cada auditor

Envía la clave pública al auditor, que usa para encriptar una clave que envía de regreso

Estas claves serán utilizadas para el encriptado con AES-128

AES-128

Algoritmo simétrico de encriptado

Utiliza una clave de 128 bits y un vector de inicialización para el encriptado y desencriptado.

```
{'encrypted_data':  
  '*%Óé\x02t1n\x1e)...etc,  
  'iv':  
  '\x8e\x1f\x88!\x82òGa\x9e`\x1eV....etc'}
```



</ Encriptado de los datos



Boot-up

El CC genera un par de claves RSA por cada auditor

Estas claves serán utilizadas para el encriptado con AES-128

AES-128

Algoritmo simétrico de encriptado

Utiliza una clave de 128 bits y un vector de inicialización para el encriptado y desencriptado.

```
{'trace_id': '011',  
'timestamp': '2013-11-02T00:00:00Z',  
'C(0)/P(1)': '0',  
'value': 58.0}
```



AES-128

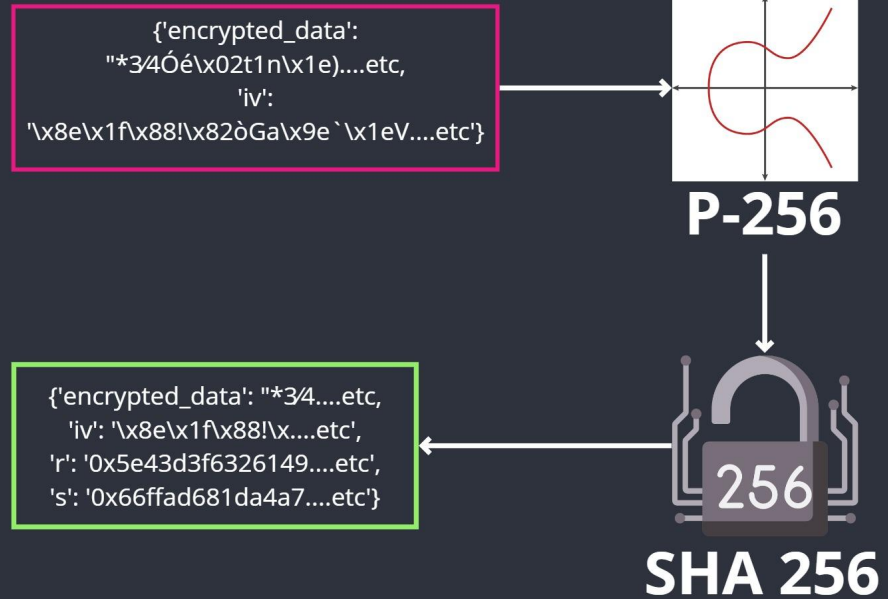
RSA

```
{'encrypted_data':  
  "**34Ôé\x02t1n\x1e)...etc,  
  'iv':  
  '\x8e\x1f\x88!\x82ôGa\x9e`\x1eV....etc'}
```

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 1 1 1 0 1

</ Firmado de los datos

- Se firma los datos usando el algoritmo **ECDSA**
- Se utilizó la curva **P-256**
- La firma se aplica a **cada trama** enviada
- El **Centro de Control** almacena todas las firmas **válidas**



</ Comunicación MQTT

- **MQTT** es un protocolo de mensajería **ligero**, usado en redes con **recursos limitados**
- Las tramas son encriptadas por el protocolo **TLS** cuando se encuentran en tráfico
- Levantamos un Broker con **Mosquitto**

Auditor



Broker MQTT



Centro de Control



← Subscribe

→ Publish

← Publish

→ Subscribe

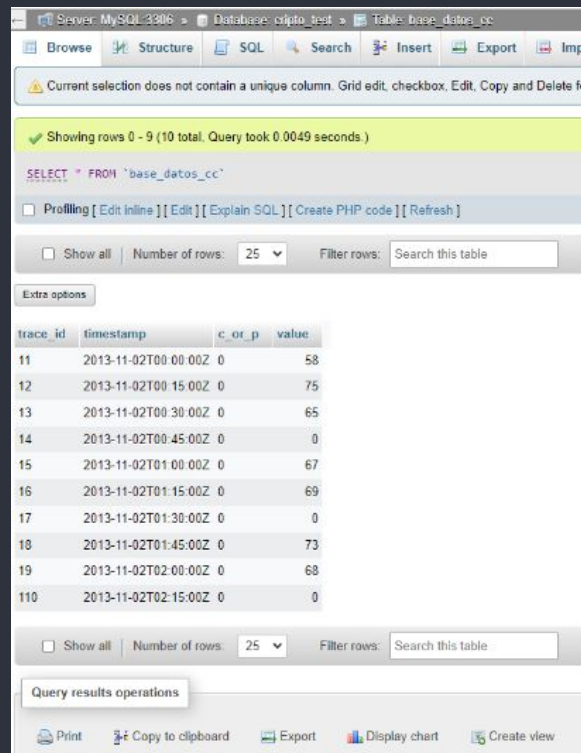
Tópico: Actualizaciones

Tópico: Datos

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

</ Base de Datos

- Utilizamos **MySQL** para el manejo de la base de datos relacionales
- Se encuentra montado en un **servidor Apache**
- La información almacenada se encuentra encriptada con **AES-256**
- Para acceder se requiere de **Autenticación** con usuario y contraseña autorizados



The screenshot shows a MySQL database management interface. At the top, there's a navigation bar with tabs for 'Browse', 'Structure', 'SQL', 'Search', 'Insert', 'Export', and 'Import'. Below this, a message states: 'Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are disabled.' A green banner indicates 'Showing rows 0 - 9 (10 total. Query took 0.0049 seconds)'. The SQL query entered is 'SELECT * FROM `base_datos_cc`'. Below the query, there are links for 'Profiling', 'Edit inline', 'Edit', 'Explain SQL', 'Create PHP code', and 'Refresh'. A section for 'Extra options' includes a 'Show all' checkbox, a 'Number of rows' dropdown set to 25, and a 'Filter rows' search box. The main area displays a table with 10 rows and 4 columns: 'trace_id', 'timestamp', 'c_or_p', and 'value'. The data is as follows:

trace_id	timestamp	c_or_p	value
11	2013-11-02T00:00:00Z	0	58
12	2013-11-02T00:15:00Z	0	75
13	2013-11-02T00:30:00Z	0	65
14	2013-11-02T00:45:00Z	0	0
15	2013-11-02T01:00:00Z	0	67
16	2013-11-02T01:15:00Z	0	69
17	2013-11-02T01:30:00Z	0	0
18	2013-11-02T01:45:00Z	0	73
19	2013-11-02T02:00:00Z	0	68
110	2013-11-02T02:15:00Z	0	0

At the bottom, there's a 'Query results operations' section with icons for 'Print', 'Copy to clipboard', 'Export', 'Display chart', and 'Create view'.

04

</ Resultados
obtenidos />

</ Resultados



Envío

```
kali@raspberrypi: ~/Downloads
File Edit Tabs Help
kali@raspberrypi:~/Downloads$ python3 publisher.py
Connected to MQTT Broker!
Published message 1 of 10
Published message 2 of 10
Published message 3 of 10
Published message 4 of 10
Published message 5 of 10
Published message 6 of 10
Published message 7 of 10
Published message 8 of 10
Published message 9 of 10
Published message 10 of 10
kali@raspberrypi:~/Downloads$
```



Recepción

```
alfa@alfa-VirtualBox: ~/mosquitto
alfa@alfa-VirtualBox:~/mosquitto$ python3 subscriber.py
Traceback (most recent call last):
  File "subscriber.py", line 43, in <module>
    client = connect_mqtt()
  File "subscriber.py", line 24, in connect_mqtt
    client.tls_set(ca_certs="/home/alfa/mosquitto/certs/ca.crt",
  File "/home/alfa/.local/lib/python3.8/site-packages/paho/mqtt/client.py", line
796, in tls_set
    context.load_cert_chain(certfile, keyfile, keyfile_password)
ssl.SSLError: [SSL] PEM lib (_ssl.c:4046)
alfa@alfa-VirtualBox:~/mosquitto$ python3 subscriber.py
Connected to MQTT Broker!
Received '{"trace_id": "1", "timestamp": "2013-11-02T00:00:00Z", "C(0)/P(1)": "0
", "value": 58.0}' from 'python/mqtt/cripto_test' topic
Received '{"trace_id": "2", "timestamp": "2013-11-02T00:15:00Z", "C(0)/P(1)": "0
", "value": 75.0}' from 'python/mqtt/cripto_test' topic
Received '{"trace_id": "3", "timestamp": "2013-11-02T00:30:00Z", "C(0)/P(1)": "0
", "value": 65.0}' from 'python/mqtt/cripto_test' topic
Received '{"trace_id": "4", "timestamp": "2013-11-02T00:45:00Z", "C(0)/P(1)": "0
", "value": 0.08}' from 'python/mqtt/cripto_test' topic
Received '{"trace_id": "5", "timestamp": "2013-11-02T01:00:00Z", "C(0)/P(1)": "0
", "value": 67.0}' from 'python/mqtt/cripto_test' topic
```



Conclusiones y trabajo futuro

05

</ Trabajo a futuro

Seguridad Física

Implementar **medidas de seguridad específicas** para el **espacio físico** a utilizar por la OSF

Virtualización

Entornos virtuales separados para **facilitar el mantenimiento y gestión** de la propuesta, aislar servicios y así **prevenir la propagación de malware.**

</ Gracias!

Alguna pregunta?

A00830952@tec.mx
A01570576@tec.mx
A00830383@tec.mx
A00832401@tec.mx
A01379097@tec.mx
A01720932@tec.mx

/>

} /> [

CREDITS: This presentation template was created by Slidesgo, and includes icons by Flaticon, and infographics & images by Freepik

Please keep this slide for attribution

