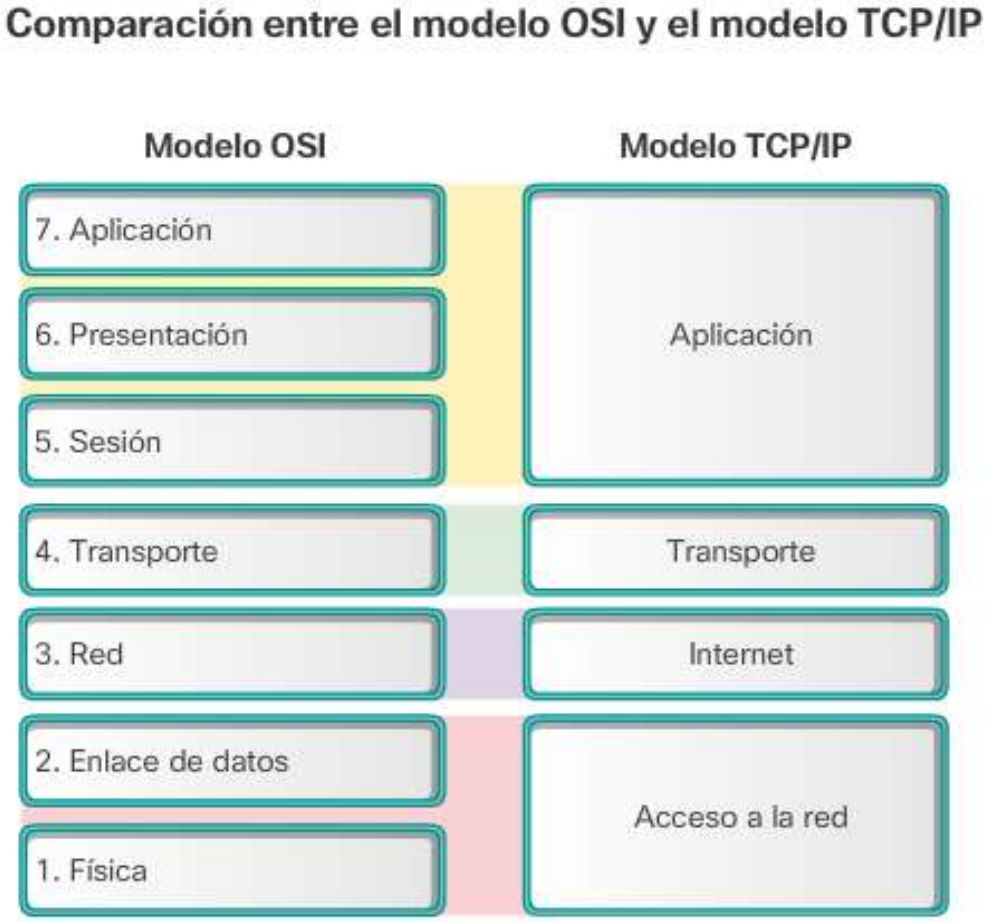
INSTITUTO SUPERIOR TECNOLÓGICO QUITO

Seguridad Web

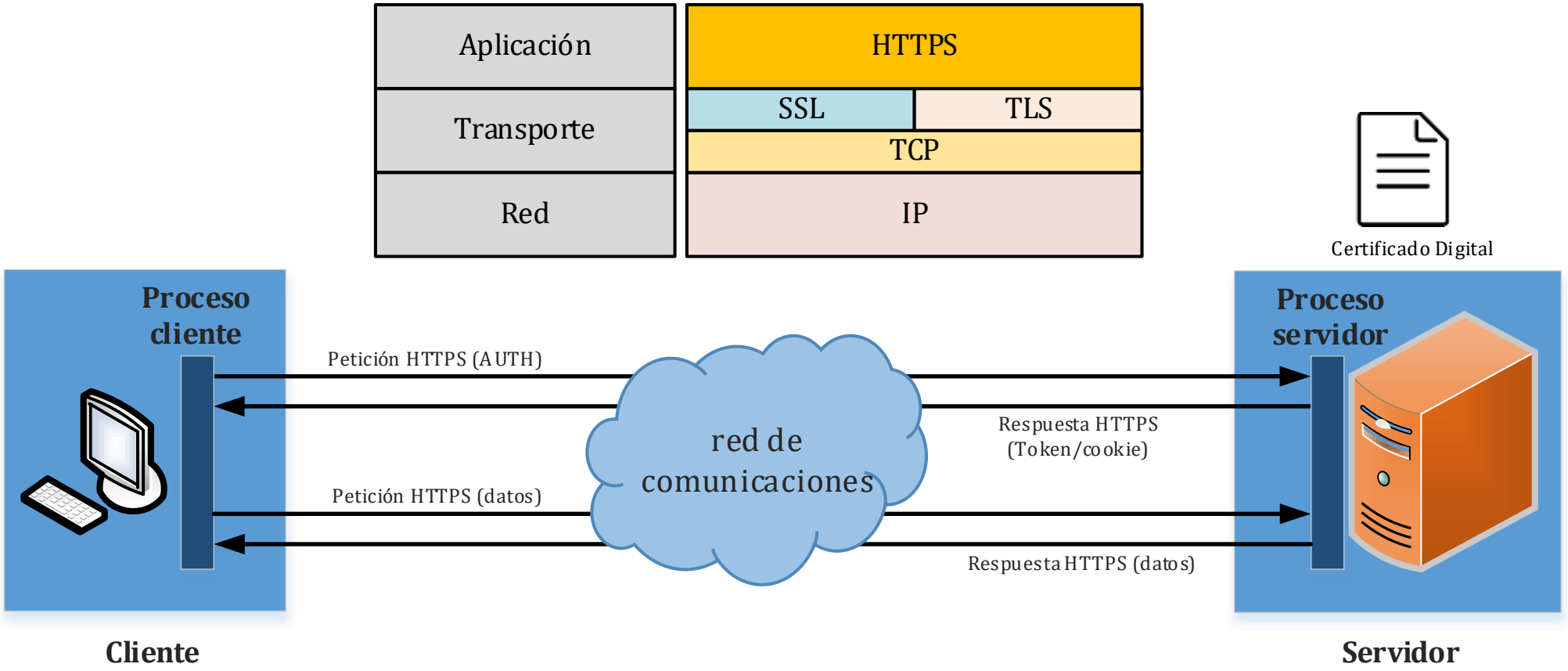
Unidad III

3.1 Modelo OSI de la ISO

- **ISO** (*International Organization for Standardizatior*
- **OSI** (*Open System Interconnection*).
- Modelo para analizar comunicaciones.
- La idea es que cada capa brinda un servicio a la capa superior.



Las similitudes clave se encuentran en la capa de transporte y en la capa de red. Sin embargo, los dos modelos se diferencian en el modo en que se relacionan con las capas que están por encima y por debajo de cada capa.



SSL y TLS son vulnerables sobre todo
a ataques man-in-the-middle

3.2 Capa Aplicación y Protocolo HTTP

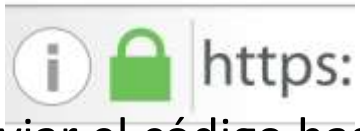
- **HTTP** (Hypertext Transfer Protocol).
- Protocolo **NO seguro** de capa aplicación.
- Protocolo de tipo **petición-respuesta sin estado**.

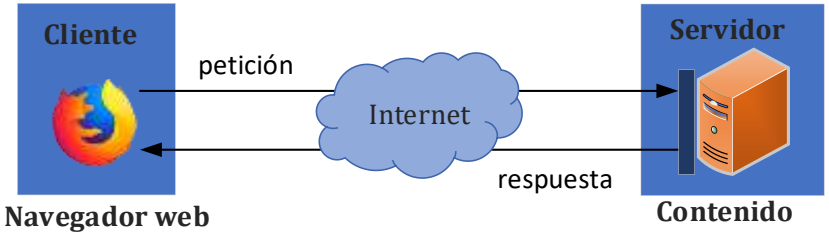
3.3 Capa Transporte y protocolos SSL y TLS

- **SSL** (*Secure Sockets Layer*): Antiguo protocolo para brindar seguridad a HTTP.
- **TLS** (*Transport Layer Security*): Protocolo mucho más robusto que SSL.
- Proveen de seguridad al protocolo HTTP.

3.3 Capa Transporte y protocolos SSL y TLS

1. Cliente solicita página web a servidor.
2. Servidor responde con firma digital de un mensaje randómico. Si es la primera vez también con el certificado digital del servidor.
3. Cliente descifra firma digital y recalcula el hash sobre el mensaje recibido. Si el hash descifrado coincide con el recalculado el proceso es exitoso y se autentica el servidor.
4. Cliente y servidor crean una clave privada (Diffie-Hellman).
5. Se logra un canal cifrado simétrico con servidor autenticado.
6. En la transmisión de datos subsequentes se debe entonces enviar el código hash (precautelar integridad).





3.4 Formatos de datos

- JSON (*JavaScript Object Notation*): Comprende otra manera de expresar un mensaje.

Texto plano

4000 habitantes de la parroquia Cotocollao de la ciudad de Quito se quedaron sin energía eléctrica desde las 16.00 hasta las 18.00 del martes 31 de octubre de 2023

JavaScript Object Notation (JSON)

```
informacion = {
        "ciudad": "Quito",
        "cantidad": 4000,
        "parroquia": "Cotocollao",
        "recurso": "energía eléctrica",
        "horaInicio": "16",
        "horaFin": "18",
        "dia": 31,
        "mes": 10,
        "anio": 2023,
        "dia_semana": "martes"
}
```

Postman

File Edit View Help

New Import Runner My Workspace Invite Upgrade

Filter

History Collections APIs BETA

Save Responses Clear all

Today

GET http://localhost:50858/api/values/5

GET http://localhost:50858/api/values/5

GET https://www.gob.ec/api/v1/instituciones/212

GET https://www.gob.ec/api/v1/

August 19

POST http://localhost:54827/itsqm/operaciones

POST http://localhost:54827/itsqm/operaciones

POST http://localhost:54827/itsqm/operaciones

GET http://localhost:54827/itsqm/operaciones

August 18

GET http://localhost:59234/itsqm/values?numero=3

GET http://localhost:59234/itsqm/values?numero=3

GET http://localhost:59234/itsqm/values?numero=3

GET Untitled Requ... GET http://localhost... GET http://localhost... POST http://localho... GET https://www.go... GET http://localhost...

No Environment

Untitled Request

GET http://localhost:50858/api/values/5 Send Save

Params Authorization Headers (7) Body Pre-request Script Tests Cookies Code Comments (0)

Query Params

KEY	VALUE	DESCRIPTION	••• Bulk Edit
Key	Value	Description	

Body Cookies Headers (10) Test Results Status: 200 OK Time: 159ms Size: 600 B Save Response

Pretty Raw Preview JSON


```
{
    "nombre": "David",
    "apellido": "Cevallos",
    "cedula": "123456789",
    "edad": 28,
    "sexo": "masculino",
    "direccion": "Buenaventura 123 y Oviedo",
    "telefono": "2845147"
}
```


Bootcamp Build Browse

ESP 20:47 23/12/2019

3.5 Mecanismos de evasión

- **Cifrado:** Cifrar malware para evitar mecanismos de detección (antivirus, firewalls, otros).
- **Segmentación:** Hacer el mensaje más pequeño y reconstruirlo en el destino.
- **Temporización (Timing):** Añadir tiempos de espera para evitar detecciones.


Yo soy ITQ
www.itq.edu.ec