

SEGURIDAD EN MICROSERVICIOS

Santiago Monsalve Calderón
Santiago Bellaizan Chaparro

AGENDA

Introduction

Sistemas distribuidos

Autorización / autenticación

OAuth2 + OpenID Connect

TLS/mTLS

**Configuración segura en
entornos distribuidos**

Top 8 ciber ataques

PoC

INTRO- DUCTION

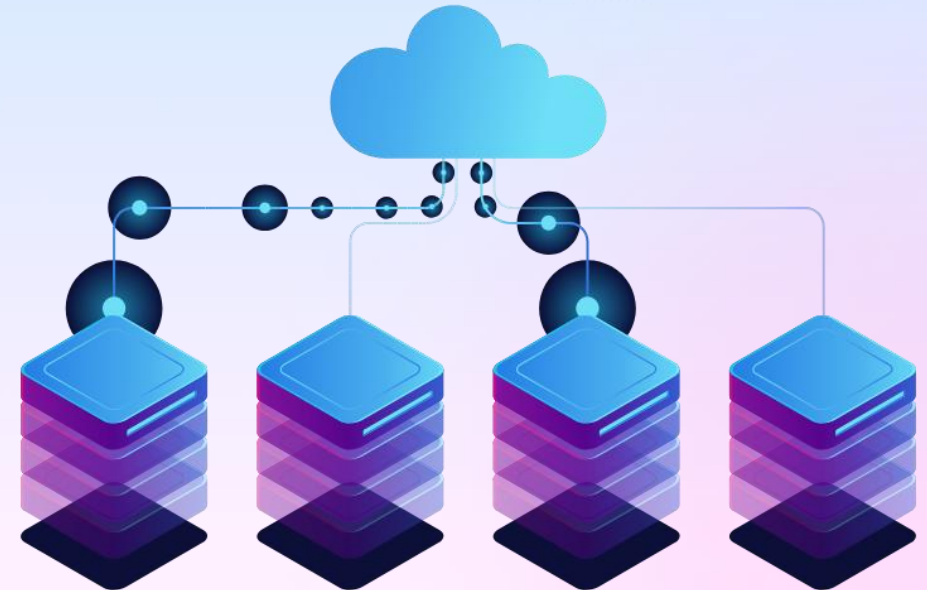
Conjunto de prácticas, herramientas y mecanismos diseñados para proteger cada componente de una arquitectura distribuida. A diferencia de las aplicaciones monolíticas, los microservicios funcionan como piezas independientes que se comunican a través de la red, lo que amplía la superficie de ataque.

SISTEMAS DISTRIBUIDOS

conjunto de computadoras que trabajan juntas, desde distintos lugares, como si fueran un solo equipo.

Aunque están separadas físicamente, estas computadoras se comunican entre sí para cumplir un objetivo común.

Cada una puede encargarse de una parte del trabajo, haciendo que el sistema sea más flexible, escalable y resistente ante fallos.



AUTORIZACIÓN ✨ VS AUTENTICACIÓN

AUTENTICACIÓN AUTORIZACIÓN

AUTENTICACIÓN

- Verifica la identidad de un usuario, sistema o servicio.
- Responde a la pregunta: "¿Quién eres?"
- Usualmente se realiza con usuario y contraseña, pero también puede incluir biometría, tokens o autenticación multifactor (MFA).
- Es el **primer paso** antes de permitir cualquier acceso.

AUTORIZACIÓN

- Define los **permisos** que tiene un usuario o sistema autenticado.
- Responde a la pregunta: "**¿Qué puedes hacer?**"
- Controla el acceso a recursos específicos como datos, funcionalidades o servicios.
- Suele gestionarse con **roles, políticas o reglas de acceso**.

TIPOS

AUTENTICACIÓN

- Basada en contraseña
- Basada en certificado
- Biometría
- Basada en tokens
- Contraseña de un solo uso
- Notificaciones push
- Multifactor
- Otros

AUTORIZACIÓN

- Basado en roles (RBAC)
- Basado en atributos (ABAC)
- Basado en políticas (PBAC)
- Control obligatorio (MAC)
- Control discrecional (DAC)

OAuth 2.0

OAuth 2.0, que significa “Open Authorization” (autorización abierta), es un estándar diseñado para permitir que un sitio web o una aplicación accedan a recursos alojados por otras aplicaciones web en nombre de un usuario

TLS(TRANSPORT LAYER SECURITY)

¿QUÉ ES?

- Protocolo de seguridad que cifra la comunicación entre dos dispositivos en una red.
- Su propósito es garantizar la confidencialidad, integridad y autenticidad de los datos transmitidos.
- Evolución desde SSL a TLS (TLS 1.2 y 1.3).

CARACTERÍSTICAS

- **Cifrado:** Protege los datos contra accesos no autorizados.
- **Integridad:** Detecta modificaciones en los datos durante la transmisión.
- **Autenticación:** Verifica la identidad del servidor y, opcionalmente, del cliente.

EJEMPLO

- Abre <https://ejemplo.com>.
- Se inicia el handshake TLS.
- El servidor envía su certificado y se valida.
- Se establece una clave compartida.
- La comunicación está cifrada
- Puedes intercambiar datos sin que nadie los intercepte.

MTLS (MUTUAL TLS)

¿QUÉ ES?

- Es una extensión de **TLS** en la que **tanto el cliente como el servidor se autentican mutuamente** usando certificados digitales. Es decir, no solo el servidor demuestra su identidad (como en TLS estándar), sino que también el cliente debe presentar un certificado válido.

CARACTERÍSTICAS

- Toda la comunicación se cifra con claves seguras generadas en el handshake.
- Útil en banca, salud, IoT y redes empresariales seguras.
- Asegura la comunicación entre servicios en arquitecturas distribuidas.

EJEMPLO

- Cuando un empleado intenta conectarse a la VPN:
- La VPN verifica su certificado.
- Si es válido, se establece una conexión segura.
- Si no, el acceso es rechazado.

GESTIÓN DE SECRETOS Y CONFIGURACIÓN SEGURA EN ENTORNOS DISTRIBUIDOS

- **Menos privilegios:** Solo los servicios y usuarios autorizados deben acceder a secretos específicos.
- **No hardcodear secretos:** Nunca incluir claves en el código fuente o en variables de entorno permanentes.
- **Rotación periódica:** Cambiar las credenciales con regularidad para minimizar riesgos.
- **Encriptación:** Usar cifrado para almacenar y transmitir secretos de forma segura.
- **Auditoría y monitoreo:** Registrar accesos y cambios a los secretos para detectar posibles incidentes.



HERRAMIENTAS PARA GESTIÓN DE SECRETOS

HashiCorp Vault

- Almacena secretos de forma segura.
- Permite acceso basado en políticas con autenticación y autorización.
- Rotación y renovación automática de credenciales.

AWS Secrets Manager

- Almacenamiento cifrado de secretos.
- Integración con IAM y rotación automática.
- Control de acceso granular.

Azure Key Vault

- Protección de secretos y claves criptográficas.
- Control de acceso basado en roles (RBAC).
- Integración con identidades de Azure.

Google Secret Manager

- Gestión de secretos en GCP con control de versiones.
- Auditoría de accesos mediante Cloud Logging.

MÉTODOS DE INYECCIÓN SEGURA DE CONFIGURACIÓN

Variables de Entorno

- Almacenar credenciales en variables de entorno.
- No incluir variables en repositorios.

Configuración Dinámica desde un Gestor de Secretos

- Extraer secretos en tiempo de ejecución en lugar de incluirlos en archivos de configuración.

Montaje de Volúmenes Seguros en Contenedores

- En Docker/Kubernetes, montar secretos desde Secrets en Kubernetes en lugar de incluirlos en imágenes.

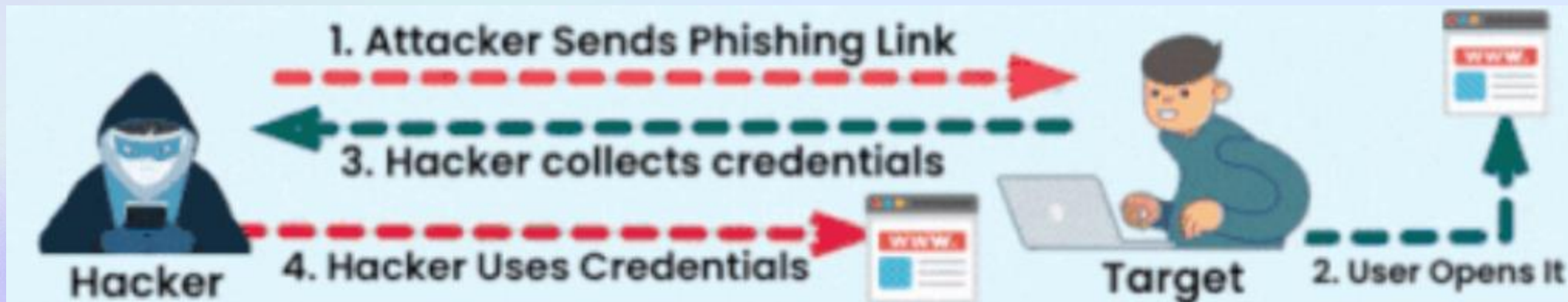
Uso de Identity Provider (IDP)

- Evitar el uso de claves estáticas y autenticar con OAuth2, OpenID Connect o IAM federado.

TOP 8 CIBER ATAQUES

Phishing Attacks – La amenaza cibernética #1

- **Qué es:** Los atacantes utilizan correos electrónicos engañosos para robar credenciales o desplegar malware.
- **Por qué importa:** La automatización mejora la sofisticación del phishing.
- **Cómo prevenirlo:** Seguridad de correo electrónico avanzada, capacitación de usuarios y autenticación multifactor (MFA).



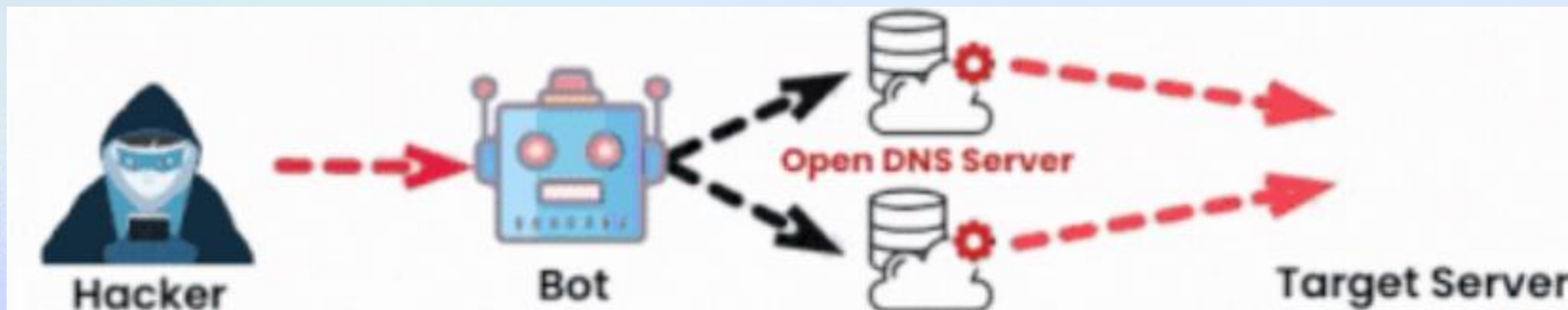
RANSOMWARE – SECUESTRANDO SISTEMAS

- **Qué es:** Malware que cifra archivos o datos críticos, exigiendo un pago.
- **Por qué importa:** Las empresas corren el riesgo de pérdida de datos y daños financieros.
- **Cómo prevenirlo:** Copias de seguridad seguras fuera de línea, protección de endpoints y acceso de confianza cero.



DENIAL-OF-SERVICE (DOS) ATTACKS – INTERRUPCIONES EN SERVICIOS

- **Qué es:** Sobrecarga de servidores o redes para provocar fallos en los sistemas.
- **Por qué importa:** Los servicios en tiempo real (finanzas, salud) deben permanecer operativos.
- **Cómo prevenirlo:** Limitación de tasas, protección contra DoS basada en la nube, detección de anomalías.



MAN-IN-THE-MIDDLE (MITM) ATTACKS – MANIPULACIÓN DE DATOS

- **Qué es:** Interceptación de comunicaciones para alterar o robar información.
- **Por qué importa:** La manipulación de datos en sectores como finanzas y salud puede comprometer decisiones críticas.
- **Cómo prevenirlo:** Cifrado de extremo a extremo, TLS 1.3, autenticación robusta, aislar redes corporativas y de visitantes con control de acceso a la red corporativa



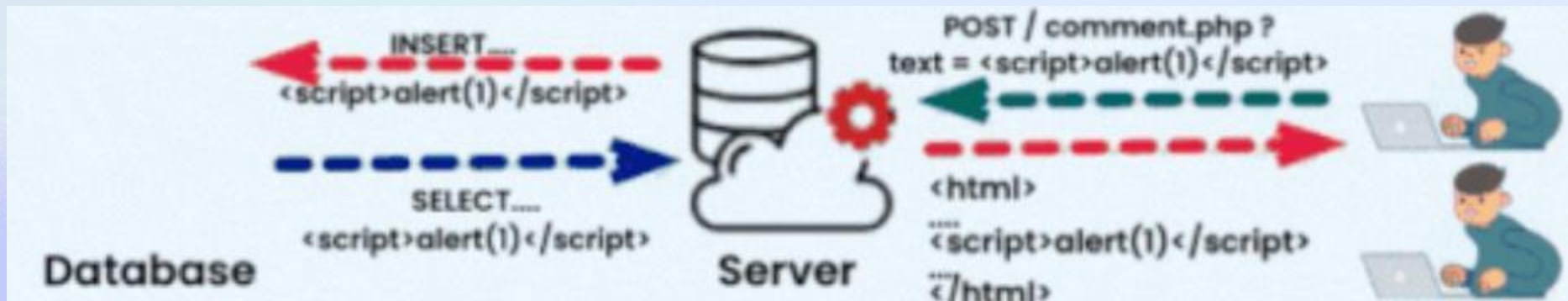
SQL INJECTION – MANIPULACIÓN DE BASES DE DATOS

- **Qué es:** Los atacantes inyectan código malicioso en consultas SQL para acceder o modificar datos.
- **Por qué importa:** Los datos alterados pueden afectar la toma de decisiones y comprometer la seguridad del sistema.
- **Cómo prevenirlo:** Consultas parametrizadas, controles de acceso estrictos en bases de datos.



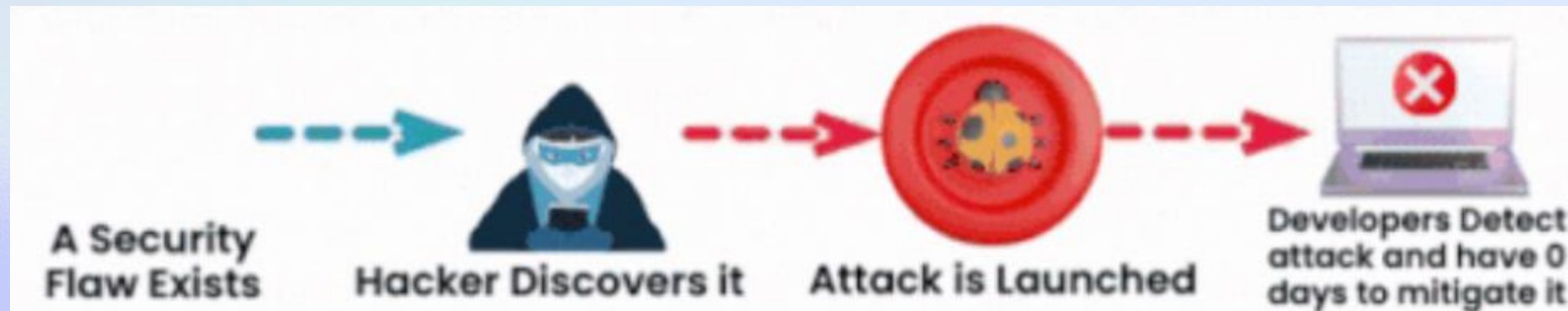
CROSS-SITE SCRIPTING (XSS) – EXPLOTACIÓN DE APLICACIONES WEB

- **Qué es:** Inyección de scripts maliciosos en interfaces web para manipular usuarios o sistemas.
- **Por qué importa:** Puede comprometer la seguridad de plataformas digitales y robar información confidencial.
- **Cómo prevenirlo:** Saneamiento de entradas, Content Security Policy (CSP), detección de anomalías.



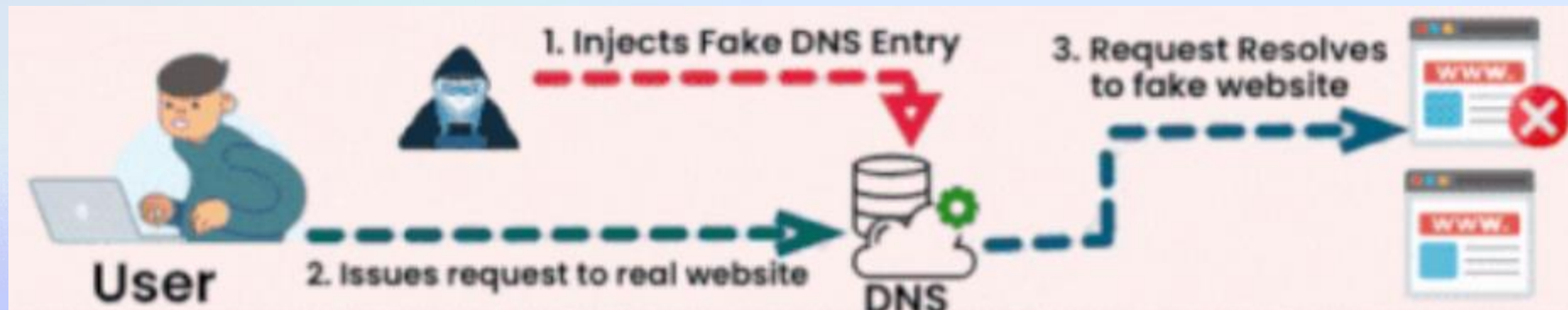
ZERO-DAY EXPLOITS – ATAQUES ANTES DE QUE EXISTAN SOLUCIONES

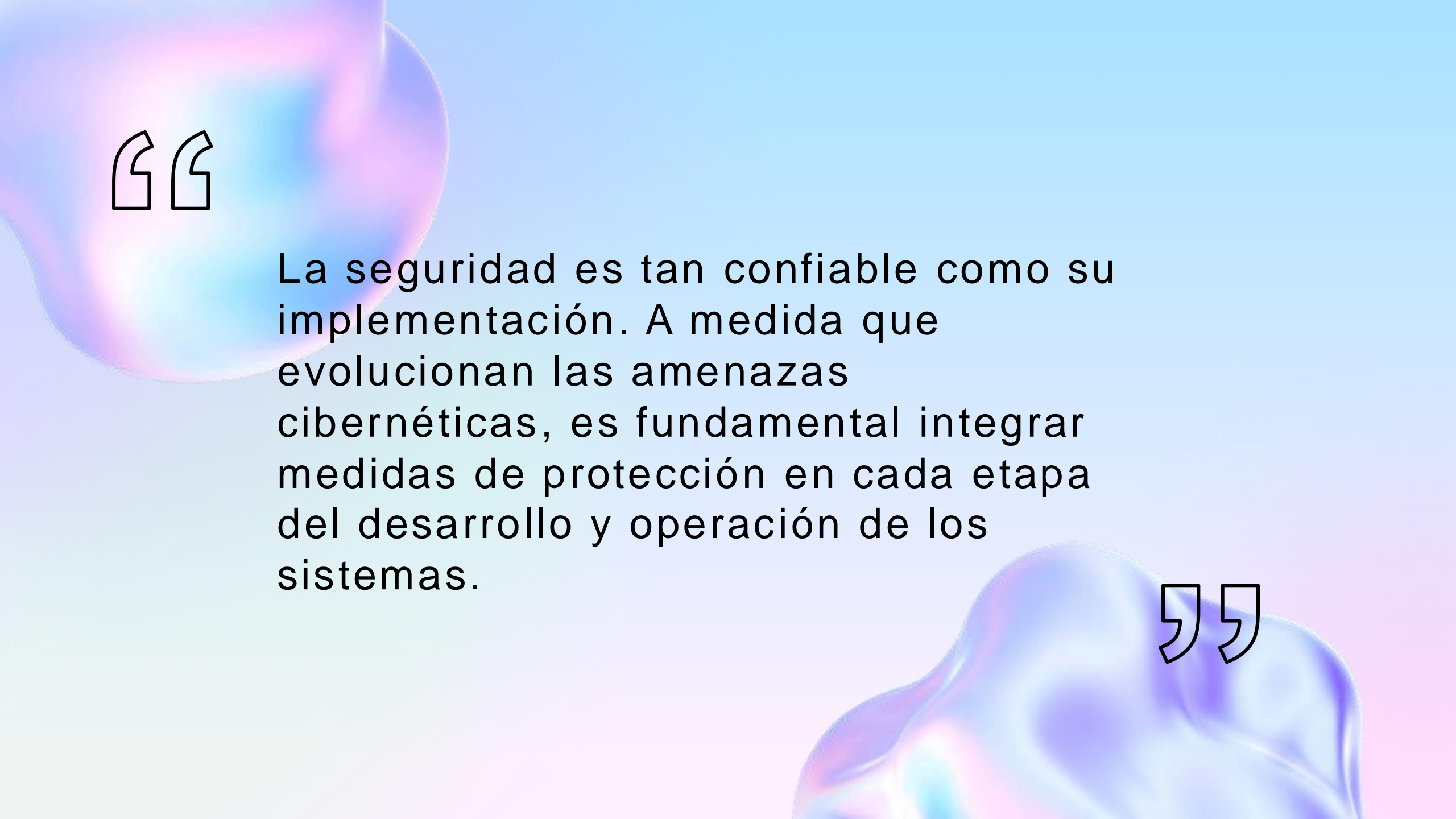
- **Qué es:** Explotación de vulnerabilidades desconocidas antes de que sean corregidas.
- **Por qué importa:** Pueden provocar filtraciones de datos, fraudes o fallos en infraestructuras críticas.
- **Cómo prevenirlo:** Herramientas de inteligencia de amenazas, parches de seguridad, simulaciones de ataques.



DNS SPOOFING – REDIRECCIÓN DE SERVICIOS

- **Qué es:** Manipulación de registros DNS para redirigir usuarios a plataformas falsas.
- **Por qué importa:** Los atacantes pueden robar credenciales o inyectar datos maliciosos en sistemas.
- **Cómo prevenirlo:** DNSSEC, monitoreo de DNS, verificación de endpoints.





“

La seguridad es tan confiable como su implementación. A medida que evolucionan las amenazas cibernéticas, es fundamental integrar medidas de protección en cada etapa del desarrollo y operación de los sistemas.

”

PRUEBA DE CONCEPTO

