Ficha Técnica: Protocolos de Seguridad y Protección de Datos

En **LC Developers**, entendemos que la confianza es la base de cualquier desarrollo tecnológico exitoso. Este documento detalla los estándares de seguridad implementados en nuestros productos de software, diseñados para garantizar la integridad, confidencialidad y disponibilidad de la información de su negocio.

1. Protección contra Vulnerabilidades Comunes

Nuestro ciclo de desarrollo de software (SDLC) integra prácticas de seguridad desde el diseño. Implementamos defensas activas contra las vulnerabilidades más críticas identificadas por OWASP:

> **Protección contra Inyección SQL:**
> Uso estricto de ORM (Object-Relational Mapping) y consultas preparadas para impedir la manipulación de bases de datos.

> **Prevención de XSS (Cross-Site Scripting):**
> Sanitización automática de entradas y salidas de datos para evitar la ejecución de scripts maliciosos en los navegadores de los usuarios.

> **Protección CSRF:**
> Implementación de tokens de verificación en todos los formularios web para asegurar que las solicitudes provengan de fuentes legítimas.

2. Cifrado y Certificados SSL/TLS

La seguridad en el tránsito de datos es innegociable. Todas nuestras plataformas operan bajo protocolos de seguridad estrictos:

> **Certificados SSL/TLS:**
> Implementación obligatoria de HTTPS con certificados de 2048 bits, garantizando que toda comunicación entre el cliente y el servidor esté encriptada y sea ilegible para terceros.

> **Cookies Seguras:**
> Configuración de cookies con atributos `HttpOnly` y `Secure` para prevenir el robo de sesiones.

3. Encriptación de Datos Sensibles

Aplicamos una estrategia de defensa en profundidad para los datos en reposo:

> **Contraseñas:**
>
> Nunca se almacenan en texto plano. Utilizamos algoritmos de hashing robustos (como Bcrypt o Argon2) para asegurar las credenciales de acceso.

> **Información Personal (PII):**
>
> Los datos críticos en la base de datos son encriptados utilizando estándares de la industria (AES-256), asegurando que la información permanezca protegida incluso en caso de acceso físico no autorizado al servidor.

4. Arquitectura de Servicios Web y APIs

Nuestras APIs RESTful están diseñadas con capas de seguridad para proteger la interacción entre sistemas:

> **Autenticación:**
>
> Uso de tokens seguros (como JWT o OAuth2) para validar la identidad de cada solicitud.

> **Rate Limiting:**
>
> Controles de limitación de tasa para prevenir ataques de fuerza bruta y denegación de servicio (DDoS).

Ismael López

Director General

LC Developers México