DELL Technologies

# Inyecciones de prompts o SQL: cómo reforzar la ciberseguridad y la resiliencia con Dell Technologies

## La amenaza creciente de los ataques de inyección de prompts o de SQL

Las inyecciones de prompts y SQL han demostrado ser, una y otra vez, uno de los métodos de ciberataque más comunes y perjudiciales. Estos ataques aprovechan vulnerabilidades en los sistemas de bases de datos o las consultas de los usuarios para manipular servidores, apropiarse de datos o sabotear los flujos de trabajo. La confianza generalizada en aplicaciones basadas en datos ha ampliado el alcance de los ataques, de forma que las inyecciones de prompts y SQL se han convertido en una amenaza muy seria en todos los sectores.

Ya sea en plataformas de comercio electrónico o en instituciones financieras, los atacantes aprovechan las brechas de seguridad para conseguir acceso no autorizado a datos confidenciales. Por eso es sumamente urgente poner en marcha contramedidas avanzadas. Dell Technologies es consciente de la gravedad que implican estas amenazas, así que ofrece soluciones innovadoras y adaptables para proteger a las empresas de este tipo de ataques.

## Información sobre inyecciones de prompts o SQL

### ¿Qué son?

- **Los ataques de inyección de prompts** se llevan a cabo manipulando motores de IA o instrucciones automáticas con entradas maliciosas. Estos ataques confunden a sistemas como los chatbots de IA y provocan acciones inesperadas o perjudiciales**.**
- **Los ataques de inyección de SQL** están dirigidos a sistemas de bases de datos en línea. Los atacantes introducen consultas SQL maliciosas en campos de entrada (p. ej., formularios de búsqueda o de inicio de sesión) para manipular y controlar bases de datos back-end.

### Cómo funcionan

#### Procesos de inyección de prompts:

1. Los atacantes manipulan los prompts aprovechando instrucciones ambiguas o mal diseñadas para generar resultados dañinos.
2. Estos ataques suelen ir dirigidos a sistemas de IA pensados para la atención al cliente, la realización de análisis o la toma de decisiones.

#### Procesos de inyección de SQL:

1. Se introduce un código SQL malicioso en los campos de entrada de una aplicación vulnerable.
2. El sistema atacado ejecuta estas instrucciones, con lo que los atacantes consiguen acceso no autorizado a datos y pueden eliminarlos o hacerse con el control del sistema.

### Técnicas comunes

- **Inyecciones de SQL basadas en la unión:** con una combinación de consultas para extraer información de la base de datos.
- **Técnicas basadas en errores:** se utilizan consultas creadas intencionalmente para producir errores que revelan la estructura de la base de datos.
- **Sobrecarga o confusión con prompts:** se envían instrucciones maliciosas que sustituyen a los resultados basados en reglas o IA.

## El impacto en las empresas

Los efectos devastadores de las inyecciones de prompts o SQL van mucho más allá del momento del incidente. Estas son algunas de las consecuencias más graves:

### Costes económicos

Como resultado directo de estos ataques, suelen robarse datos de clientes y registros de transacciones, lo que suele conllevar sanciones económicas. Una institución financiera perdió casi 40 millones de dólares en litigios, compensaciones y nuevas medidas de seguridad tras un ataque con inyección de SQL.

### Interrupción operativa

Las inyecciones de SQL dirigidas a bases de datos back-end pueden desarticular sistemas, paralizar flujos de trabajo e interrumpir la prestación de servicios esenciales. Se calcula que el tiempo de inactividad medio de las empresas afectadas puede ser de entre 18 y 24 horas, lo que genera una gran reducción de la productividad.

### Daños a la reputación

Los ataques de inyección de prompts en plataformas de IA suelen provocar desinformación o una mala toma de decisiones. Si los atacantes acceden a secretos comerciales o ponen en riesgo la prestación de servicios, la confianza de los clientes y la relación con los mismos se ven afectadas.

## Ejemplo real

Una empresa de venta al detalle fue víctima de una inyección de SQL en su plataforma de pago, que expuso datos de las tarjetas de los clientes y obligó a detener el servicio durante varios días. Para solventar el incidente se tuvieron que emitir informes a las autoridades competentes y se perdieron casi **3 millones de dólares** en compensaciones a clientes y litigios.

## Estadísticas alarmantes

Según el informe “State of the Internet” de Akamai (correspondiente a los años 2017-2019), las inyecciones de SQL suponen casi **dos terceras partes (un 65 % aproximadamente)** de todos los ataques a aplicaciones web.

OWASP situó las inyecciones de prompts como el riesgo **número 1 de LLM** en su lista de las 10 principales amenazas en 2025.

Fuente: Principales riesgos de seguridad según OWASP, 2025

## Soluciones de Dell Technologies para afrontar inyecciones de prompts o SQL

Dell Technologies ofrece un ecosistema de herramientas y mecanismos de protección para que las empresas puedan defenderse frente a ataques sofisticados como las inyecciones de prompts y SQL.

### Seguridad de puntos finales con Dell Trusted Devices

Los puntos finales son las principales vías de acceso a las redes de las empresas. Dell Trusted Devices integra soluciones de seguridad a nivel de hardware y firmware para una protección sólida y resistente.

- **Dell SafeID** protege las credenciales de usuarios con un sistema de autenticación mejorado basado en hardware.
- **SafeData** cifra los datos confidenciales tanto en tránsito como en reposo para protegerlos en caso de ataque con inyección de SQL.

### Detección preventiva de amenazas con CrowdStrike

Las herramientas de detección preventiva de Dell con tecnología de CrowdStrike utilizan IA para identificar y neutralizar actividades sospechosas.

- **Supervisión en tiempo real:** las posibles inyecciones de prompts o SQL en entornos híbridos se detectan inmediatamente.
- **Contención de amenazas:** los algoritmos basados en IA aíslan los nodos afectados de la red para evitar que el ataque se propague a todo el sistema.

Una empresa multinacional de fabricación que usaba herramientas de detección preventiva de amenazas consiguió detener un intento de inyección de SQL dirigido a sus bases de datos. Si no lo hubiera detectado, habría perdido millones de dólares en tiempo inoperativo.

### Seguridad de servidores y almacenamiento con Dell

- **Servidores de confianza:** proteja las aplicaciones de bases de datos reforzando los servidores contra intentos de vulneración.
- **Seguridad adaptable en las cargas de trabajo:** evite la ejecución no autorizada de inyecciones o códigos maliciosos.

### Dell PowerProtect protege la integridad de los datos

- **Copias de seguridad inmutables:** un sistema resiliente garantiza una recuperación rápida aunque las bases de datos o los prompts se hayan dañado.
- **Almacenamiento con sistema de cámara de aire:** aísla los puntos de recuperación de forma física y lógica, de forma que se mitigan los efectos negativos de la inyección de SQL.

Por ejemplo, durante un ataque de ransomware mediante una inyección de SQL, un proveedor de telecomunicaciones logró restablecer sus operaciones en menos de 48 horas gracias a las soluciones de copias de seguridad aisladas de Dell PowerProtect, lo que le ahorró una gran pérdida económica.

### Seguridad de red avanzada y microsegmentación con las redes de Dell PowerSwitch y SmartFabric OS

La segmentación de red avanzada, los controles de acceso estrictos y los análisis de tráfico en tiempo real en toda la infraestructura fortalecen las defensas contra ataques de día cero.

## Colaboraciones estratégicas

- **Microsoft:** defensas integradas contra inyecciones basadas en consultas en plataformas de uso común como Azure y SQL Server**.**
- **CrowdStrike y Secureworks:** la inteligencia avanzada contra amenazas y las respuestas adaptadas a incidentes, junto con la infraestructura de Dell, impulsan la resiliencia.

## Creación de una estrategia de seguridad multicapa

### Acciones clave que deberían emprender las empresas

- **Principios de confianza cero:** implemente una estructura de validación integral para todos los usuarios y los comandos del sistema.
- **Prácticas de codificación seguras:** los programadores deben borrar las entradas de los usuarios e implementar soluciones resistentes a inyecciones de SQL.
- **Protocolos de cifrado:** proteja las transmisiones y el almacenamiento de datos con algoritmos de cifrado avanzado.
- **Formación de empleados:** proporcione formación a su personal para que pueda identificar anomalías en entradas, intentos de phishing y la manipulación maliciosa de prompts.
- **Auditorías y pruebas del sistema:** realice pruebas regulares de vulnerabilidad para comprobar que sus defensas contra inyecciones de prompts y SQL están actualizadas.

La arquitectura de Dell aplica todos estos principios al mismo tiempo para crear plataformas con la máxima seguridad para todos sus clientes.

## Sacar el máximo partido a Dell Professional Services

Dell Professional Services ayuda a las empresas con un enfoque personalizado, desde la respuesta a incidentes hasta la supervisión diaria. Nuestros equipos cualificados evalúan los riesgos, implementan defensas sólidas y ofrecen una corrección inmediata en caso de amenazas.

## Proteger lo más importante con Dell Technologies

Para afrontar las sofisticadas inyecciones de prompts y SQL se requiere un enfoque preventivo. Dell Technologies, su aliado de confianza, le ofrece herramientas de última generación, colaboraciones estratégicas y servicios de expertos.

Las soluciones preventivas son el primer paso hacia el futuro de la integridad operativa y la confianza de los clientes. Póngase en contacto con Dell Technologies hoy mismo para proteger sus datos, aumentar la resiliencia y seguir creciendo en el mundo digital actual.

Juntos, protegemos lo más importante.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **Dell.com/SecuritySolutions**

Más información acerca de las soluciones Dell

Póngase en contacto con un experto de Dell Technologies

Consulte más recursos.

Únase a la conversación con #HashTag.



DELL Technologies