

# CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**DEEPSEEK EN LA MIRA: FILTRACIÓN MASIVA  
OTORGA CONTROL TOTAL SOBRE SU BASE DE  
DATOS EN UNA GRAVE BRECHA DE SEGURIDAD**

31 / 01 / 2025

## CONTENIDO

INTRODUCCIÓN .....	3
RESUMEN .....	5
NOTICIA COMPLETA .....	7
CONTACTOS DE SOPORTE .....	8

## INTRODUCCIÓN

DeepSeek, una empresa reconocida en el ámbito de la inteligencia artificial se encuentra en el centro de una controversia tras una filtración masiva que expuso información altamente sensible, incluyendo claves secretas, registros internos y el historial de conversaciones de los usuarios. Esta grave brecha de seguridad ha despertado preocupaciones sobre la vulnerabilidad de sus sistemas y la capacidad de la compañía para proteger los datos de sus clientes. A medida que la noticia se difunde, expertos en ciberseguridad analizan el impacto de este incidente, mientras que los usuarios y la comunidad tecnológica exigen respuestas y medidas concretas para mitigar los riesgos.

## DEEPSEEK EN LA MIRA: FILTRACIÓN MASIVA OTORGA CONTROL TOTAL SOBRE SU BASE DE DATOS EN UNA GRAVE BRECHA DE SEGURIDAD

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_01_31_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	<b>CLEAR</b>
Fecha de publicación:	31/01/2025
Es día cero (0 day):	No

## RESUMEN

### ¿Qué sucedió?

En los últimos días, DeepSeek, una influyente empresa de inteligencia artificial enfrenta una grave crisis tras la exposición de su base de datos. La filtración dejó accesibles claves secretas, registros internos y el historial de chat de los usuarios, generando serias preocupaciones sobre la seguridad de la plataforma.

El incidente tomó mayor relevancia cuando se reveló que Microsoft y OpenAI investigan si un grupo vinculado a DeepSeek obtuvo datos de OpenAI sin autorización. Esta situación ha encendido alarmas en la industria tecnológica y ha puesto en entredicho las prácticas de seguridad de la empresa.

Mientras tanto, la falta de una respuesta oficial detallada ha incrementado la incertidumbre, dejando a expertos en ciberseguridad preocupados por el riesgo que esta filtración representa para los usuarios y el ecosistema de inteligencia artificial.

### ¿Cómo pasó?

#### El origen de la filtración

La filtración de la base de datos de DeepSeek fue detectada por investigadores, quienes encontraron una base de datos de código abierto utilizada comúnmente en el análisis de servidores. En esta base de datos, los archivos de registros contenían las rutas tomadas por los usuarios dentro de los sistemas de la plataforma. Lo más alarmante fue que la base de datos era accesible públicamente sin ningún tipo de autenticación o medidas de seguridad, lo que permitió el acceso sin restricciones y el control total sobre su contenido. Esto significaba que cualquier persona con los conocimientos adecuados podía ingresar y extraer información sin restricciones.

#### Datos expuestos

Más de un millón de registros fueron comprometidos, incluyendo datos sensibles como claves secretas, historial de chats y detalles internos del sistema. Esta exposición no solo comprometió la seguridad de los datos, sino que también permitió una escalada de privilegios, brindando a los atacantes acceso completo a la infraestructura de DeepSeek. La falta de mecanismos de autenticación facilitó el acceso sin restricciones, abriendo la puerta a ataques cibernéticos dirigidos, robo de identidad o la explotación de vulnerabilidades en los sistemas de inteligencia artificial.

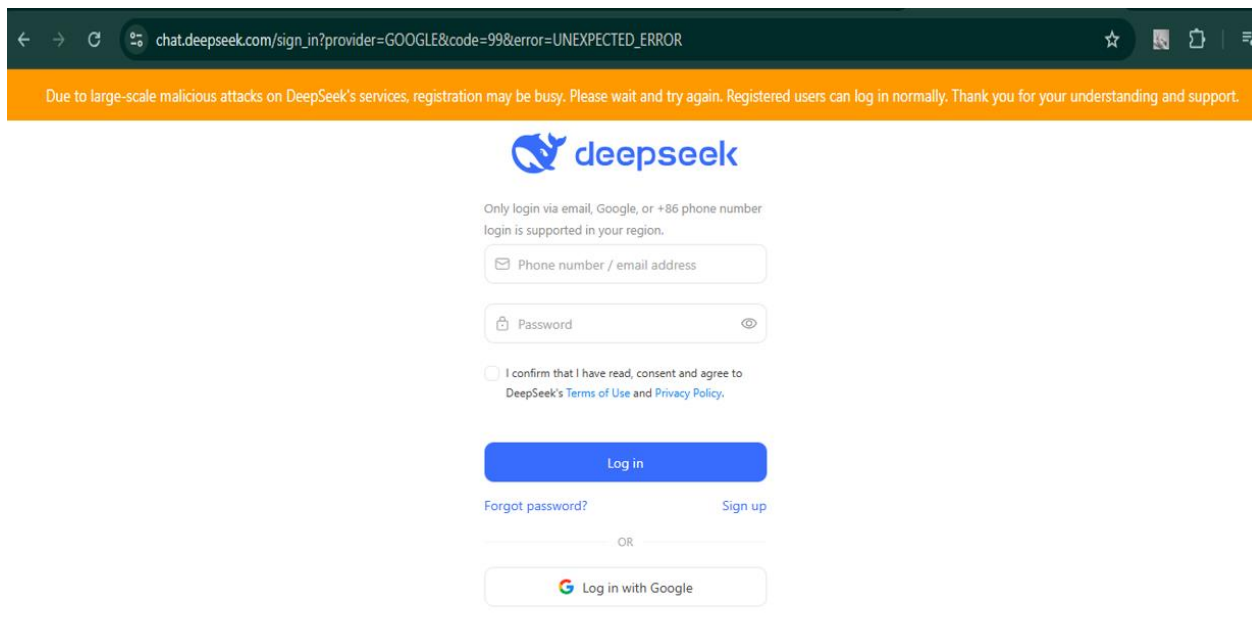
La filtración de estos datos representa un peligro crítico, ya que podrían ser utilizados para llevar a cabo ciberataques más avanzados, poner en riesgo identidades personales o aprovechar fallas en la inteligencia artificial para fines maliciosos.

#### Falta de respuesta oficial

Hasta el momento, DeepSeek no ha proporcionado explicaciones claras sobre cómo ocurrió la filtración ni qué medidas se han implementado para mitigar el impacto. Esta falta de transparencia ha generado aún más dudas sobre la capacidad de la empresa para proteger la información de sus usuarios y clientes.

Sin embargo, el equipo de DeepSeek dio un mensaje para los nuevos usuarios que se quieren registrar:

*“Debido a los ataques maliciosos a gran escala contra los servicios de DeepSeek, el proceso de registro puede estar ocupado. Espere e intente nuevamente. Los usuarios registrados pueden iniciar sesión normalmente. Gracias por su comprensión y apoyo.”*



The screenshot shows a web browser window with the URL `chat.deepseek.com/sign_in?provider=GOOGLE&code=99&error=UNEXPECTED_ERROR`. An orange banner at the top contains the message: "Due to large-scale malicious attacks on DeepSeek's services, registration may be busy. Please wait and try again. Registered users can log in normally. Thank you for your understanding and support." Below the banner is the DeepSeek logo and a login form. The form includes the text "Only login via email, Google, or +86 phone number login is supported in your region." and fields for "Phone number / email address" and "Password". There is a checkbox for "I confirm that I have read, consent and agree to DeepSeek's Terms of Use and Privacy Policy." and a blue "Log in" button. Links for "Forgot password?" and "Sign up" are also present. Below these is an "OR" separator and a "Log in with Google" button.

Este comunicado sugiere que la plataforma enfrenta problemas derivados de ataques dirigidos, lo que podría estar vinculado con el incidente de filtración. No obstante, sigue sin haber detalles claros sobre las acciones específicas que la empresa está tomando para solucionar la situación.

### Conclusión y lecciones aprendidas

Este incidente ha puesto de manifiesto la vulnerabilidad de las plataformas de inteligencia artificial, especialmente cuando se gestionan grandes cantidades de datos sensibles sin las medidas adecuadas de seguridad. La exposición de la base de datos de DeepSeek es una lección clara de que las organizaciones deben priorizar la protección de datos y establecer sistemas de autenticación robustos para prevenir accesos no autorizados. La falta de una respuesta inmediata por parte de la empresa también resalta la importancia de contar con un protocolo de respuesta ante incidentes de seguridad, el cual permita mitigar rápidamente los daños y mantener la confianza de los usuarios.

Una de las lecciones clave que deja este incidente es la importancia de la capacitación continua sobre ciberseguridad. Los equipos de desarrollo y seguridad deben mantenerse constantemente actualizados sobre las últimas amenazas cibernéticas y las mejores prácticas para proteger los datos sensibles. Además, la concientización sobre la seguridad debe ser parte integral de la cultura organizacional, asegurando que todos los empleados comprendan la importancia de proteger los datos.

### Recomendaciones

1. **Cambiar contraseñas de inmediato:** Si tienes una cuenta en DeepSeek, es fundamental que cambies tu contraseña lo antes posible. Utiliza una clave única, larga y compleja que combine



letras, números y caracteres especiales. Evita reutilizar contraseñas anteriores o similares a las de otros servicios, ya que podrían estar comprometidas.

2. **Habilitar autenticación en dos pasos (2FA):** Activa la autenticación en dos factores en tu cuenta para agregar una capa extra de seguridad. Este método requiere no solo la contraseña, sino también un código de verificación enviado a tu teléfono o correo electrónico, lo que dificulta el acceso no autorizado, incluso si alguien obtiene tus credenciales.
3. **Evitar compartir información sensible:** Dado el riesgo de futuras filtraciones, es recomendable no almacenar información personal o datos sensibles dentro de la plataforma de DeepSeek hasta que se garanticen mejores medidas de seguridad.
4. **Monitorear cuentas y actividad inusual:** Revisa regularmente el historial de accesos de tu cuenta para identificar cualquier actividad sospechosa. Si notas intentos de inicio de sesión desde ubicaciones desconocidas o dispositivos no autorizados, cambia tu contraseña de inmediato y revisa la configuración de seguridad de tu cuenta.
5. **Mantenerse informado:** Sigue los comunicados oficiales de DeepSeek y de expertos en ciberseguridad para conocer las actualizaciones sobre la filtración y las medidas que la empresa está tomando para mitigar los daños.

## NOTICIA COMPLETA

<https://devel.group/blog/deepseek-en-la-mira-filtracion-masiva-otorga-control-total-sobre-su-base-de-datos-en-una-grave-brecha-de-seguridad/>

## CONTACTOS DE SOPORTE



Correo electrónico: [info@develsecurity.com](mailto:info@develsecurity.com)

### Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://www.devel.group/>