COMUNICACIÓN SOBRE UNA INCIDENCIA DE SEGURIDAD DE DATOS PERSONALES

Información importante para nuestros clientes

Desde **CORREDURÍA DE SEGUROS SUEIRO, S.L.U.** queremos informarte de una incidencia de seguridad que ha afectado a MPM Software, proveedor del tarificador TarifAI utilizado por nuestra correduría para el desarrollo de su actividad profesional.

El pasado 3 de noviembre de 2026, en torno a las 14:00 horas, terceros ajenos a MPM Software accedieron sin autorización a la herramienta de gestión de incidencias (ticketing) que el proveedor pone a disposición de sus clientes y, a través de ella, a la base de datos asociada al tarificador TarifAI, alojada en su plataforma SaaS.

Como consecuencia de este acceso no autorizado, se produjo una exfiltración de datos personales. MPM detectó la actividad anómala aproximadamente a las 16:00 horas del mismo día y adoptó medidas para contener el acceso.

¿Qué información podría haberse visto afectada?

La incidencia podría haber afectado a información personal de las personas que figuran en las pólizas como tomadores, propietarios, conductores o beneficiarios.

Según la información facilitada por MPM Software, entre las categorías de datos personales potencialmente afectadas se encuentran:

- Nombre y apellidos.
- NIF y/o número de pasaporte.
- Fecha de nacimiento.
- Fecha del carné.
- Sexo.
- Idioma.
- Nacionalidad.
- Profesión.
- Estado civil.
- Relación.
- Indicador de privacidad.
- Datos del carné.

- Fórmula de tratamiento.

No todos los registros afectados contienen necesariamente todas las categorías de datos indicadas, por lo que la información potencialmente comprometida puede variar en función de cada persona. MPM ha confirmado que no se extrajeron direcciones, teléfonos, correos electrónicos, números de póliza ni datos bancarios.

¿Qué ha ocurrido con la información?

Según la información facilitada por MPM Software, se ha confirmado una exfiltración de datos personales como consecuencia del acceso no autorizado a la base de datos asociada a TarifAI.

Se trata de una vulneración de la confidencialidad de la información, sin que, hasta el momento, se hayan identificado alteraciones ni pérdidas de datos.

¿Qué riesgos puede implicar esta incidencia?

A partir de la información disponible, los principales riesgos identificados están relacionados con:

- **Posibles intentos de fraude o phishing:** los datos personales podrían utilizarse para realizar comunicaciones fraudulentas mediante correo electrónico, SMS o llamadas telefónicas.
- **Posible suplantación de identidad:** la información identificativa podría utilizarse por terceros para hacerse pasar por las personas afectadas ante otras entidades u organizaciones.

¿Qué medidas se han adoptado?

Desde la detección del incidente, MPM Software ha comunicado la adopción de diversas medidas técnicas y organizativas para contener el acceso no autorizado y reforzar la seguridad de sus sistemas.

Por nuestra parte, desde que hemos tenido conocimiento de los hechos, estamos realizando las actuaciones necesarias para analizar el alcance de la incidencia y valorar sus posibles consecuencias, en coordinación con MPM Software y con nuestro servicio de asesoramiento en protección de datos.

Asimismo, estamos llevando a cabo las actuaciones correspondientes para atender las obligaciones establecidas en la normativa de protección de datos personales.

¿Qué recomendamos a nuestros clientes?

Como medida de precaución, recomendamos prestar especial atención a cualquier comunicación inesperada que pueda recibirse por correo electrónico, SMS o teléfono.

En particular:

- Desconfiar de comunicaciones inesperadas que soliciten información personal, bancaria o credenciales de acceso.
- No facilitar contraseñas, códigos de verificación ni datos bancarios a través de enlaces o comunicaciones cuya autenticidad no se haya podido verificar.
- Evitar abrir enlaces o archivos adjuntos de procedencia sospechosa.
- Prestar especial atención a posibles comunicaciones que suplanten la identidad de nuestra correduría, de compañías aseguradoras u otras organizaciones conocidas.
- Verificar siempre la autenticidad de cualquier solicitud de información o pago antes de facilitar datos o realizar operaciones.

Si recibes alguna comunicación sospechosa o tienes dudas sobre la autenticidad de un mensaje, te recomendamos no responder ni facilitar información y contactar directamente con nosotros a través de nuestros canales habituales.

Para cualquier consulta relacionada con esta incidencia o con el tratamiento de tus datos personales, lopd@suevianet.com

Lamentamos las molestias e inquietudes que esta situación pudiera ocasionarte y agradecemos tu comprensión y colaboración.

Atentamente

La dirección de Correduría de Seguros Sueiro, S.L.U.