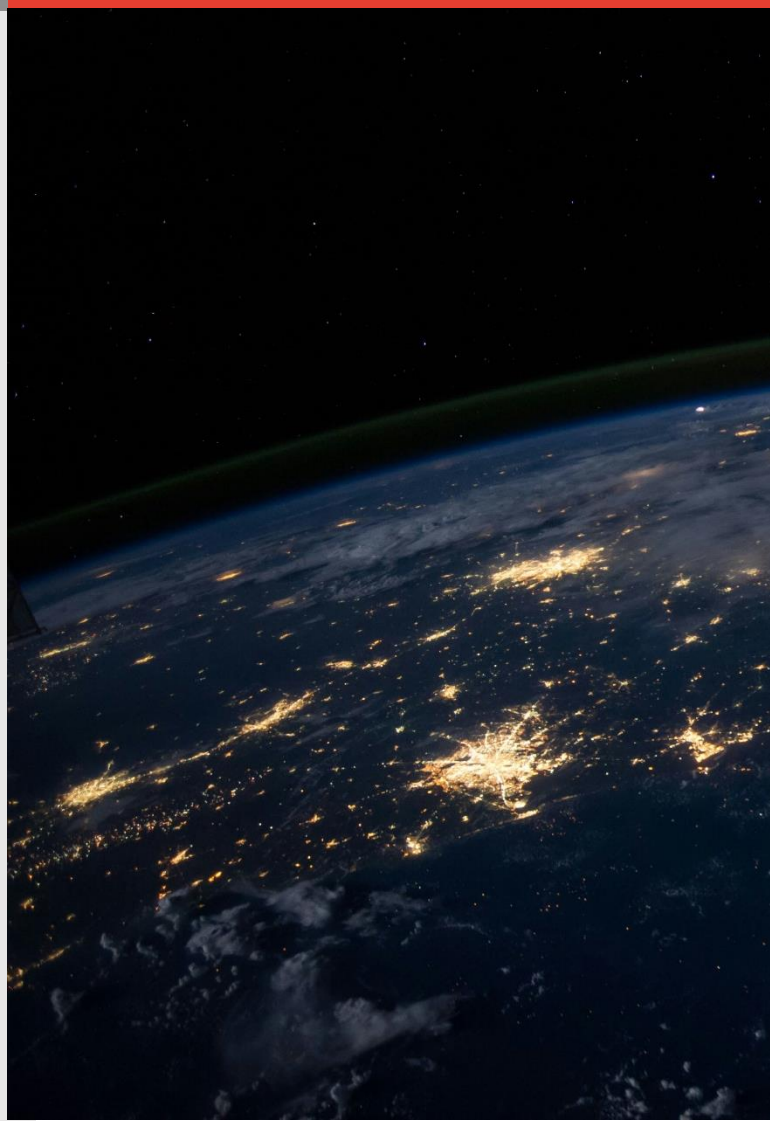
NOTA INFORMATIVA

Sanción millonaria a Meta por deficiente gestión de contraseñas

Meta es sancionada con 91 millones de euros por no implementar medidas de seguridad adecuadas en el almacenamiento de contraseñas.



Lo que necesitas saber

- Meta es sancionada con 91 millones de euros por no implementar medidas de seguridad adecuadas para proteger las contraseñas de los usuarios, almacenándolas en texto plano sin cifrado.

- La investigación reveló que Meta violó varios artículos del Reglamento General de Protección de Datos (RGPD), incluyendo la notificación y documentación de violaciones de seguridad.

- Al no proteger las contraseñas, Meta expuso a los usuarios a riesgos significativos de acceso no autorizado a sus cuentas personales.

- Este caso subraya la necesidad de que las empresas implementen medidas de seguridad robustas para proteger la información sensible y cumplir con las normativas de protección de datos.

En marzo de 2019, *Meta Platforms Ireland Limited* ("**Meta**") informó a la Comisión de Protección de Datos de Irlanda ("**DPC**") que, por error, había almacenado contraseñas de usuarios de sus redes sociales en "texto plano" dentro de sus sistemas internos, es decir, sin aplicar ninguna protección criptográfica ni cifrado.

Este incidente dio lugar a una investigación que se prolongó durante cinco años, culminando en una Decisión notificada a Meta este 26 de septiembre. Como resultado, Meta ha recibido **una sanción de 91 millones de euros** por no haber implementado las medidas de seguridad necesarias para proteger las contraseñas de los usuarios.

La investigación de la DPC reveló que Meta había incumplido varios artículos del Reglamento General de Protección de Datos ("**RGPD**"). La DPC determinó que Meta no había protegido correctamente las contraseñas de sus usuarios, exponiéndolas a accesos no autorizados y vulnerando sus derechos de privacidad. Este nuevo revés para Meta refuerza la preocupación en Europa sobre el cumplimiento de las normativas de protección de datos y la responsabilidad proactiva de las grandes tecnológicas en la gestión de la privacidad de los usuarios.

La decisión de la DPC detalla las infracciones del RGPD cometidas por Meta, fundamentadas en diversas disposiciones de dicha normativa:

- **Notificación de violaciones de seguridad (artículo 33, apartado 1 del RGPD)**: Las empresas, como responsables del tratamiento, deben informar a las autoridades de protección de datos sobre cualquier violación de datos personales. Meta no cumplió con esta norma, ya que no notificó en un plazo adecuado a la DPC sobre la filtración de contraseñas almacenadas en texto sin formato.
- **Documentación de incidentes (artículo 33, apartado 5 del RGPD)**: Además de notificar, las empresas deben mantener un registro detallado de las violaciones de datos personales. Meta tampoco documentó correctamente estas violaciones, lo que dificulta la trazabilidad y la mejora de las medidas de seguridad.
- **Medidas de seguridad (artículo 5, apartado 1, letra f y artículo 32, apartado 1 del RGPD)**: Las empresas deben garantizar la seguridad de los datos personales mediante medidas técnicas y organizativas adecuadas, que aseguren su confidencialidad continua y los protejan contra accesos no autorizados. Meta incumplió estos requisitos al no implementar ninguna técnica de cifrado ni protección adecuada para las contraseñas, exponiéndolas a riesgos de procesamiento no autorizado.

Este caso destaca la exigencia del RGPD a los responsables del tratamiento de datos, de **implementar medidas de seguridad robustas**, teniendo en cuenta los riesgos para los usuarios y la naturaleza del tratamiento. Esto requiere una evaluación continua de los riesgos inherentes al tratamiento y las medidas adecuadas para mitigarlos, especialmente en el almacenamiento de contraseñas de usuarios.

Resulta esencial garantizar que las contraseñas de los usuarios nunca se almacenen en "texto plano", dado el alto riesgo de abuso asociado con el acceso no autorizado a dicha información. Las **contraseñas son datos extremadamente sensibles**, ya que su compromiso podría permitir el acceso a cuentas personales, como es el caso de las de redes sociales.

En resumen, entre las medidas proactivas a implementar incluyen:

- Evaluación de impacto y análisis del tratamiento de datos personales.
- Implementar medidas de seguridad como el cifrado de contraseñas y datos sensibles.
- Capacitar a los empleados en protección de datos y mejores prácticas.
- Establecer protocolos eficientes de notificación de incidentes de seguridad.
- Realizar auditorías regulares y supervisión continua de los sistemas de protección de datos.

La multa impuesta a Meta es un recordatorio para todas las empresas: la protección de la información no es opcional, es un deber legal. Una gestión proactiva del cumplimiento normativo en materia de protección de datos no solo ayuda a **evitar sanciones millonarias**, sino que también es fundamental para **mantener la confianza de los clientes y usuarios**.

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60