Ecopetrol confirma ataque digital con acceso a 3.300 cuentas

Ecopetrol detectó un acceso no autorizado a su infraestructura digital, con extracción de datos de 3.300 cuentas de usuario. La empresa bloqueó un intento de ransomware, denunció ante la Fiscalía y activó protocolos de ciberseguridad para contener la amenaza de extorsión.

Redacción Economía
17 de julio de 2026 - 08:13 p. m.

Imagen de referencia.

Foto: Mauricio Alvarado Lozada

Ecopetrol informó este viernes que detectó un acceso no autorizado a parte de su infraestructura digital y confirmó que un actor externo logró extraer información asociada con cerca de 3.300 cuentas de usuario, luego de comprometer entornos de almacenamiento en la nube de aproximadamente 15 compañías del Grupo Ecopetrol.

La empresa precisó que el incidente también incluyó un intento de ejecución de ransomware, una modalidad de secuestro de información que, según la compañía, fue bloqueada oportunamente gracias a los controles de ciberseguridad implementados dentro del grupo empresarial.

“A la fecha, Ecopetrol S.A. no ha identificado ninguna interrupción material de sus operaciones críticas, capacidad de producción o servicios esenciales”, indicó la compañía.

Sin embargo, “el actor externo comunicó exigencias de extorsión, amenazando con

divulgar públicamente la información extraída ilegalmente", señaló la empresa, por lo que activó sus protocolos de atención a incidentes e inició una investigación.

La compañía reconoció que todavía revisa qué tipo de información salió de sus sistemas. Entre los archivos descargados podrían encontrarse documentos corporativos de carácter reservado, información de uso exclusivo de la compañía o incluso datos personales, un análisis que todavía sigue en marcha.

Mientras avanza esa revisión, Ecopetrol revocó los accesos comprometidos, bloqueó mecanismos utilizados para descargas masivas de información y presentó una denuncia penal ante la Fiscalía General de la Nación. También trabaja con autoridades especializadas para rastrear la infraestructura desde la cual se ejecutó el ataque e impedir que la información sea difundida.

La empresa admitió que aún es temprano para medir todas las consecuencias del incidente. Aunque aseguró que no ha identificado un impacto financiero directo, tampoco descartó que el episodio pueda terminar afectando su reputación, sus resultados operacionales o su situación financiera.

Por ahora, mantendrá un monitoreo permanente de la situación y aseguró que divulgará al mercado cualquier hecho relevante que llegue a identificarse durante el desarrollo de la investigación, conforme a las obligaciones previstas para los emisores de valores.

resultados operacionales o su situación financiera.

Por ahora, mantendrá un monitoreo permanente de la situación y aseguró que divulgará al mercado cualquier hecho relevante que llegue a identificarse durante el desarrollo de la investigación, conforme a las obligaciones previstas para los emisores de valores.

Por Redacción Economía

Lo que es tendencia

1 Judicial

Equipo de empalme de De la Espriella denuncia presunta corrupción en entidades del Estado

2 Judicial

Fiscalía ocupa bienes que serían del cantante Charlie Zaa y tendrían relación con las AUC

3 El Magazín Cultural

Paola Holguín llega al Ministerio de Cultura: perfil, trayectoria y controversias

4 Moda e Industria

Abelardo de la Espriella nombra a Silvia Tcherassi como la embajadora ad honorem de la moda