Noticias económicas importantes | Noticias empresariales

Ecopetrol reconoce ataque cibernético: datos de usuarios y 15 compañías del grupo impactadas

Ecopetrol reveló que un actor externo robó información de unas 3.300 cuentas de usuario y exigió para evitar su divulgación.

Por: Camilo Jaimes - 2026-07-17

Ecopetrol confirma ciberataque con robo de datos y extorsión a la compañía. Collage Valora Analitik

Ecopetrol confirmó este viernes 17 de julio que fue víctima de un incidente de ciberseguridad que incluyó el acceso no autorizado a parte de su infraestructura digital, la extracción ilegal de información asociada a miles de cuentas de usuario y una posterior exigencia de extorsión por parte de los responsables del ataque.

Lea también: Concepto del Congreso abre la puerta para posesionar a Abelardo de la Espriella fuera de Bogotá

La petrolera, que es emisora de acciones en las bolsas de Bogotá y Nueva York, **informó que detectó un**

La petrolera, que es emisora de acciones en las bolsas de Bogotá y Nueva York, **informó que detectó un acceso no autorizado a recursos digitales de su propiedad por parte de un actor externo que aún no ha sido identificado.** La compañía precisó que, además del robo de información, los atacantes intentaron ejecutar un ataque de ransomware —modalidad de secuestro de información mediante cifrado de sistemas—, el cual fue bloqueado por los controles de ciberseguridad implementados dentro del Grupo Ecopetrol.

El ataque afectó a unas 15 compañías del Grupo Ecopetrol

Según explicó la compañía, **el incidente comprometió entornos de almacenamiento de archivos en la nube correspondientes a aproximadamente 15 compañías del Grupo Empresarial,** lo que permitió la descarga no autorizada de datos relacionados con cerca de 3.300 cuentas de usuario.

Valora te recomienda:

- **Cambios en IVA, renta y 4x1.000: las claves que tendría que tener la reforma tributaria de De la Espriella**
- **Nuevo fallo de la Corte Suprema aclara cuándo algunos trabajadores sí pueden ser despedidos**
- **Ya puede consultar información exógena de la DIAN para declaración de renta 2026: ¿qué es y para qué sirve?**

Tras obtener la información, el actor responsable del ataque contactó a **Ecopetrol para exigir un pago a cambio de no divulgar públicamente los datos extraídos de manera ilegal, configurando un caso de extorsión cibernética.**

Aunque la empresa no detalló el tipo de información comprometida ni el monto exigido por los atacantes, **sí advirtió que continúa evaluando el alcance de la información extraída y los posibles riesgos derivados del incidente.**

El protocolo que activó Ecopetrol tras el ataque

Luego de identificar el ataque, Ecopetrol puso en marcha sus protocolos de respuesta a incidentes informáticos e inició una investigación para contener el riesgo y limitar una eventual divulgación de la

informáticos e inició una investigación para contener el riesgo y limitar una eventual divulgación de la información.

Entre **las medidas adoptadas se encuentra la revocación inmediata de los accesos no autorizados a los activos digitales comprometidos**, el bloqueo de mecanismos utilizados para descargas masivas de información y el análisis de las tácticas empleadas por el actor malicioso para ejecutar el ataque.

Puede interesarle: Yellowstone impulsa un nuevo fondo en EE. UU. tras devolver el 100 % del capital de su Fondo III

La empresa también presentó una denuncia penal ante la **Fiscalía General de la Nación y comenzó a trabajar con entidades especializadas para apoyar la investigación y la respuesta frente al incidente**. Paralelamente, inició acciones para identificar las infraestructuras externas utilizadas para almacenar o descargar la información sustraída, con el objetivo de gestionar su restricción o bloqueo.

Como parte del plan de contingencia, **Ecopetrol activó mecanismos de coordinación con sus aseguradoras y con equipos especializados en mercado de capitales, mientras adelanta una valoración detallada de la información descargada para establecer su nivel de criticidad.**

Pese a la magnitud del incidente, **Ecopetrol aseguró que hasta el momento no ha identificado interrupciones materiales en sus operaciones críticas, ni afectaciones sobre su capacidad** de producción o la prestación de servicios esenciales.

La compañía también indicó que, por ahora, no ha evidenciado un impacto financiero directo que le impida desarrollar normalmente su actividad empresarial ni ha confirmado que la información robada haya sido divulgada públicamente.

Sin embargo, advirtió que las investigaciones siguen en curso y que todavía no es posible descartar consecuencias futuras para la organización.

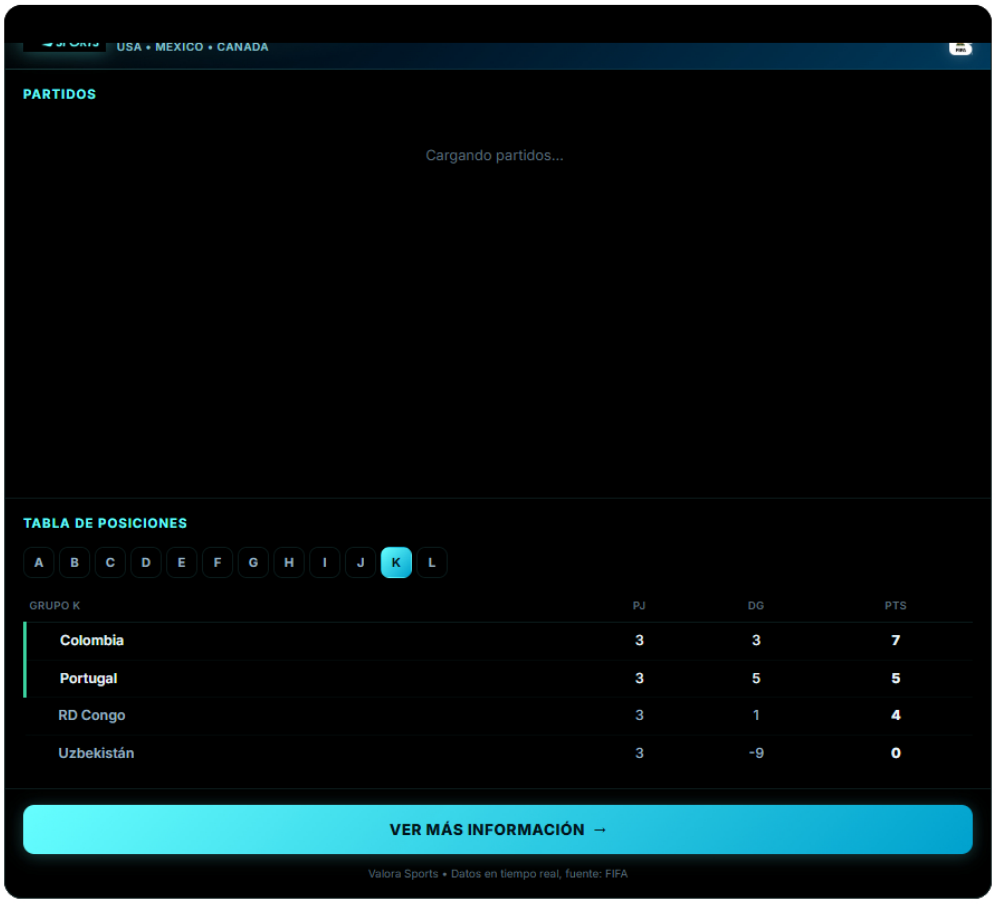
Ecopetrol explicó que continúa revisando la posible exposición de información corporativa obtenida por los atacantes, la cual podría incluir datos confidenciales, información reservada, activos de propiedad exclusiva o datos personales.

La petrolera señaló que, debido a la naturaleza del incidente, aún no puede asegurar que el ataque no genere efectos materiales sobre el negocio, su reputación, los resultados operacionales o incluso su situación financiera.

También puede leer: Terminó la ventana pensional: menos del 15 % de los colombianos habilitados se cambió de régimen

Precisó además que **mantendrá un monitoreo permanente sobre la evolución del caso y que informará oportunamente al mercado si identifica hechos relevantes que deban ser divulgados conforme a la**

regulación aplicable.



Ver más

Tags: ecopetrol

También te puede interesar:

Gobierno De la Espriella refuerza acciones con FMI, Banco Mundial y Departamento del Tesoro de EE. UU: estos son los planes

Nueva MinTransporte arranca plan para destrabar megaobras en Colombia

Yellowstone impulsa un nuevo fondo en EE. UU. tras devolver el 100 % del capital de su Fondo III