FRACASO ESTATAL

Ecopetrol confirmó un ciberataque: Petro queda otra vez bajo la lupa en Colombia

20/07/2026 | El robo de datos expone una empresa estratégica debilitada por la politización del Gobierno.

Petro debe responder por la fragilidad de la mayor empresa de Colombia.

Anderson Riverol

Ecopetrol confirmó que un atacante externo ingresó en sus recursos digitales, extrajo información asociada con unas 3.300 cuentas y alcanzó entornos utilizados por 15 empresas del grupo. El responsable intentó desplegar un programa de secuestro informático, formuló exigencias

Leé también:

Ecopetrol apartó a Ricardo Roa y ahora Colombia mira lo que puede pasar

La petrolera destaca que sus sistemas bloquearon el ransomware y que no se detectaron interrupciones en la producción. Sin embargo, evitar el cifrado de los servidores no equivale a impedir el ataque: la extracción de datos ocurrió y la propia empresa admite que todavía no puede descartar consecuencias adversas sobre sus finanzas, sus operaciones o su reputación. Presentar como éxito una defensa que permitió el robo de información demuestra hasta qué punto el Gobierno intenta administrar el daño antes que explicar el fracaso.

Colombia es un país del extremo norte de Sudamérica. Su paisaje cuenta con bosques tropicales, las montañas de los Andes y varias plantaciones de café.

Politización costosa

El gobierno de Gustavo Petro no puede tratar el incidente como un problema técnico ajeno a su responsabilidad. El Estado controla el 88,49 % de las acciones de Ecopetrol y, por tanto, ejerce una influencia determinante sobre su orientación y su gobierno corporativo. La seguridad de sus activos

ideológica.

La empresa llegó al ciberataque después de años de tensiones internas, renuncias en la junta directiva, controversias contractuales y cuestionamientos alrededor de Ricardo Roa, exgerente de la campaña presidencial de Petro. La Fiscalía anunció que formularía cargos contra el directivo por presuntas irregularidades electorales y tráfico de influencias, acusaciones que Roa niega, pero el presidente mantuvo públicamente su respaldo. Petro privilegió la lealtad política incluso cuando la conducción de Ecopetrol necesitaba recuperar independencia, estabilidad y credibilidad.

El ataque agrava el deterioro institucional de Ecopetrol bajo Petro.

Responsabilidad presidencial

El ataque no demuestra por sí mismo que Petro haya causado una falla informática concreta, pero sí expone el resultado de una conducción que debilitó los controles institucionales alrededor de la empresa más importante del país. En una infraestructura estratégica, la ciberseguridad depende de inversión sostenida, supervisión profesional, cadenas claras de responsabilidad y una dirección concentrada en proteger los activos. Cuando la administración se organiza alrededor de afinidades políticas y disputas ideológicas, esas prioridades terminan perdiendo espacio.

La politización dejó a la petrolera expuesta a una crisis de confianza.

Petro debe entregar una explicación completa sobre el origen de la intrusión, la información comprometida, el tiempo durante el cual permaneció abierto el acceso y las decisiones de seguridad adoptadas antes del incidente. También corresponde una auditoría independiente que determine responsabilidades y evite que el Gobierno oculte el problema detrás de comunicados tranquilizadores. El ciberataque no es solamente una crisis tecnológica: es otra señal del deterioro institucional que Petro deja en Ecopetrol.

TEMAS DE ESTA NOTA:

RELACIONADAS

PETRÓLEO ESTATAL

La frase de Gustavo Petro que sacudió a Ecopetrol: ¿qué hay detrás?

CONFLICTO LABORAL

Petrobras respira aliviada tras la huelga: qué cedió a los petroleros de Brasil

ENERGÍA OFFSHORE

Petrobras y Equinor dominan subasta en Brasil: ¿qué significa para el futuro?

MÁS NOTICIAS