COLOMBIA >

La Fiscalía investiga el ciberataque contra Ecopetrol: se habría infiltrado información sensible

El ente acusador asignó el caso a su dirección de delitos fiscales, que ya recolecta evidencia con peritos forenses, agentes del CTI y dos fiscales, mientras se intenta contener la difusión de archivos reservados

Por **Frank Saavedra**

La Fiscalía General de la Nación abrió una investigación por el ciberataque contra Ecopetrol tras la divulgación ilegal de información sensible de 15 empresas vinculadas a la petrolera estatal - crédito

Colprensa

31 Jul, 2026 09:27 a. m. CO

La Fiscalía General de la Nación abrió una investigación por el ciberataque contra Ecopetrol tras la divulgación ilegal de información sensible de 15 empresas vinculadas con la petrolera estatal, un caso que además activó medidas para frenar la circulación de los datos y advertencias legales para quienes los usen o compartan.

Te puede interesar:
Así reaccionaron varios políticos a la designación de María Carolina Restrepo como directora del Icbf en el gobierno entrante: "Cree que los subsidios son para los ricos"

La pesquisa quedó en manos de la Dirección Especializada para los Delitos Fiscales, que ya recopila evidencia digital con apoyo de peritos forenses, investigadores del CTI y dos fiscales con experiencia en delitos de naturaleza fiscal y tecnológica.

Hasta ahora, **no existen pruebas de un daño esencial o especialmente grave en la operación de la compañía**, aunque esa verificación hace parte del trabajo en curso.

Te puede interesar:
Daniel Briceño le 'cantó la tabla' a Carolina Corcho, que cuestionó la designación de Ana María Vesga como ministra de Salud

El ataque ocurrió el 17 de julio y comprometió información reservada de compañías aliadas de Ecopetrol, divulgada luego por canales no oficiales.

La empresa activó sus protocolos internos para colaborar con las autoridades en la identificación de los responsables y contener la reproducción de los datos en plataformas digitales.

Te puede interesar:

Dos internos habrían fallecido en medio de un encuentro íntimo en la cárcel de Ibagué: los cuerpos fueron encontrados con signos de ahorcamiento

Información relevante

ecopetrol

Ecopetrol informa sobre un incidente cibernético

Bogotá, 17 de julio de 2026

Ecopetrol S.A. (BVC: ECOPETROL; NYSE: EC) informa que ha identificado un acceso no autorizado a ciertos recursos digitales de su propiedad, por parte de un actor externo aún no identificado, así como un intento de ejecución de *Ransomware* (secuestro de información) que fue bloqueado oportunamente por los controles de ciberseguridad implementados al interior del Grupo Empresarial (GE). El acceso no autorizado afectó entornos de almacenamiento de archivos en la nube de aproximadamente 15 compañías del GE lo que resultó en la descarga no autorizada de datos asociados con aproximadamente 3.300 cuentas de usuario. El actor externo comunicó exigencias de extorsión, amenazando con divulgar públicamente la información extraída ilegalmente.

Ante el desarrollo de este incidente Ecopetrol S.A. inició una investigación y activó los protocolos de atención y respuesta a incidentes, además del despliegue de las siguientes actividades, con el propósito de evitar que la información, objeto de extracción ilegal, sea divulgada públicamente por el actor externo, se materialicen afectaciones reputacionales, actuaciones de entidades de supervisión y/o potenciales costos financieros asociados con la investigación, la remediación y el cumplimiento normativo:

a. Revocación inmediata de accesos no autorizados a los activos digitales comprometidos.
b. Bloqueo de mecanismos asociados a descargas masivas de información.
c. Identificación, análisis y contención de las tácticas, técnicas y procedimientos (TTPs) utilizados por el actor malicioso.
d. Formulación de denuncia penal ante la Fiscalía General de la Nación y despliegue de actividades de cooperación con entidades nacionales especializadas.
e. Identificación de infraestructuras externas utilizadas para el almacenamiento o descarga de información con el fin de gestionar acciones de restricción o bloqueo.
f. Activación de mecanismos de acompañamiento con aseguradoras y áreas especializadas de mercado de capitales para la adecuada gestión del evento.
g. Valoración detallada de la información descargada y determinación de su criticidad.
h. Monitoreo intensificado de la infraestructura tecnológica bajo esquemas de alertamiento crítico y validación continua de controles preventivos y detectivos.

A la fecha, Ecopetrol S.A. no ha identificado ninguna interrupción material de sus operaciones críticas, capacidad de producción o servicios esenciales, ningún impacto financiero directo que le impida seguir desarrollando su objeto social o la divulgación efectiva de la información objeto de acceso ilegal. Sin embargo, continúa evaluando la posible exposición de información corporativa que podría incluir datos confidenciales, de carácter reservado, de propiedad exclusiva o datos personales, pues no es posible asegurar que este incidente no vaya a tener algún tipo de efecto adverso material sobre el negocio, la reputación, los resultados operacionales o la situación financiera de la Compañía.

Ecopetrol S.A. continuará monitoreando la evolución de esta situación y, en caso de identificarse hechos o información material que deba ser divulgada al mercado, informará oportunamente de conformidad con la normativa aplicable.

ECP-INFORMACION PUBLICA

Ecopetrol activó sus protocolos internos y colabora con las autoridades para identificar a los responsables del ciberataque y contener la reproducción de los datos - crédito Ecopetrol

En un comunicado, Ecopetrol advirtió que la responsabilidad legal no se limita a quienes ejecutaron el ataque. La petrolera sostuvo: **“Así como la actuación de los agentes externos infringen las regulaciones que protegen el tratamiento de la información de propiedad del Grupo Empresarial, los terceros que accedan a esta información también podrían estar actuando en contravía de las leyes y regulaciones aplicables”**.

La compañía recurrió al mecanismo de *take down* para solicitar el retiro del contenido publicado ilegalmente en internet. Esa estrategia avanza en paralelo con el trabajo del Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) y de la Fiscalía General de la Nación para establecer quiénes estuvieron detrás del ataque.

Según fuentes del ente acusador, citadas por *El Tiempo*, **la investigación ya fue formalmente abierta y tiene un objetivo inmediato doble: establecer el origen del ataque y respaldar a la empresa en las labores de contención**. El equipo asignado trabaja al mismo tiempo sobre la mitigación técnica del episodio y sobre la obtención de pruebas para una eventual atribución penal.

Así mismo, esas mismas fuentes explicaron que **“se apoya la mitigación del ataque y la recolección de evidencia digital**“. Ese material será clave para determinar responsabilidades y reconstruir el recorrido de la información sustraída desde el momento del ataque hasta su publicación en canales no autorizados.

La respuesta oficial, por ahora, combina frentes técnicos y jurídicos. Mientras la autoridad judicial avanza con la pesquisa, Ecopetrol mantiene activas sus medidas de contención para evitar que la información de las 15 empresas afectadas siga circulando en internet.

El grupo The Gentlemen habría amenazado a Ecopetrol con publicar información en siete días

La Fiscalía atribuyó el ataque a The Gentlemen y mantiene la investigación sobre Ecopetrol en etapa de indagación - crédito VisualesIA/Imagen Ilustrativa Infobae

La Fiscalía investiga el ciberataque contra Ecopetrol en el que los responsables se llevaron más de una tera de información, incluidos datos de funcionarios y material vinculado con la Junta Directiva, según revelaron fuentes del organismo a *Caracol Radio*.

El ataque ocurrió hace cerca de un mes y **el equipo de ciberseguridad de la empresa detectó el incidente a tiempo, lo que evitó un daño mayor.**

De acuerdo con esas fuentes, los atacantes advirtieron a la compañía con un mensaje: **“Pórtense bien o en 7 días sacamos la información”.** Una semana después, y tras la falta de respuesta de la empresa, comenzó la exposición de los datos.

Del mismo modo, la reconstrucción del caso señaló que la intrusión se originó en una refinería de Ecopetrol y se concretó a través de un tercero con privilegios de administrador. Tras vulnerar la seguridad, **usaron Kali Linux para ingresar al área de Tecnologías de la Información (TI) y extraer información mediante el directorio activo.**

Según la Fiscalía, entre lo sustraído hay correos y datos asociados a la Junta Directiva, un punto que los investigadores siguen evaluando. Las fuentes atribuyeron el ataque al grupo The Gentlemen y precisaron que la investigación está en etapa de indagación.

The Gentlemen opera con un esquema de ciberdelincuencia basado en ransomware - crédito Visuales IA

El grupo de ciberdelincuencia *The Gentlemen* opera con un esquema de *ransomware*: recluta piratas informáticos para ejecutar ataques y cobra comisiones a cambio de esos servicios. Se presume que sus integrantes son rusos, aunque no hay claridad sobre ese origen.

Su método consiste en robar datos confidenciales de empresas antes de bloquear sus sistemas mediante cifrado. Luego exige un pago para evitar que la información sustraída se filtre de forma pública.

Secciones

América Argentina Colombia España Estados Unidos México Perú Centroamérica

Últimas Noticias RSS

Contáctenos

Redacción Empleo

Contacto comercial

Argentina Colombia España México Perú Media Kit

Legales

Términos y Condiciones Política de Privacidad
