NACIÓN

Ecopetrol confirma publicación de información robada de 15 empresas tras ciberataque

Julio 28, 2026

0

Facebook | X | WhatsApp

Ecopetrol confirmó la filtración de información de 15 empresas del Grupo tras un ciberataque y aseguró que sus plataformas siguen operando con normalidad.

La petrolera informó que, tras el incidente de ciberseguridad divulgado en días pasados, los actores externos responsables del ataque difundieron información obtenida de manera ilegal de 15 compañías del Grupo Ecopetrol.

Ante esta situación, la empresa señaló que trabaja de manera conjunta con la Fiscalía General de la Nación, a través de la Unidad de Delitos Informáticos, y con el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con el propósito de lograr el retiro de la información publicada de forma ilegal y limitar el acceso a ese contenido.

«Ecopetrol S.A. informa que, a propósito del incidente de ciberseguridad divulgado en días pasados de julio de 2026, los actores externos han publicado la información que fue copiada ilegalmente de 15 empresas del Grupo Ecopetrol», indicó la compañía.

Ecopetrol advierte posibles implicaciones legales por acceder a la información filtrada

La empresa también advirtió que el acceso por parte de terceros a esa información podría implicar el incumplimiento de las normas que regulan la protección y el tratamiento de la información de propiedad del Grupo Empresarial.

«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

ULTIMOS ARTICULOS


CIUDAD
Córdoba, Capitana Nacional del Mar 2026


JUDICIAL
Atacaron a bala almacén de repuestos para motos en Fundación


CIUDAD
SANTA MARTA: 501 AÑOS RECIBIENDO AL MUNDO Historia del Puerto que impulsó el desarrollo y progreso de la ciudad


NACIÓN
Gobierno radica proyecto de ley minera para modernizar el sector


MAGDALENA
Más de 105.000 adultos recibirán el pago de

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», señaló.

Ecopetrol aseguró que continuará adelantando las investigaciones y mantendrá la cooperación con las autoridades competentes para mitigar los efectos derivados de la publicación de la información.

La compañía afirma que no hay afectaciones en sus sistemas transaccionales

La compañía también informó que, hasta el momento, no ha identificado afectaciones en sus plataformas transaccionales ni en las soluciones tecnológicas de sus empresas subordinadas, así como tampoco en la infraestructura digital de sus socios comerciales y financieros, proveedores o clientes.

«No se ha identificado ningún compromiso o afectación de las soluciones tecnológicas transaccionales dentro de su ecosistema digital, ni de las de sus subordinadas o de su red de socios comerciales y financieros, proveedores y clientes», afirmó.

No obstante, Ecopetrol advirtió que el alcance total del incidente, su impacto y los costos asociados aún son inciertos. En ese sentido, indicó que no puede garantizar que las medidas de remediación sean completamente efectivas ni descartar la divulgación de información adicional o la eventual apertura de procesos regulatorios, litigios, afectaciones reputacionales u otros efectos sobre la operación y la situación financiera de la empresa.

The Gentlemen se atribuyó el ataque contra Ecopetrol

El ataque cibernético contra Ecopetrol ocurrió el pasado 17 de julio, cuando un actor externo intentó sustraer información de la compañía. Días después se conoció que el responsable sería «The Gentlemen», un grupo de ransomware como servicio (RaaS) que acumula más de 250 víctimas en distintos países.

Antes de que el grupo The Gentlemen se atribuyera el ataque contra Ecopetrol, las autoridades colombianas ya lo tenían identificado como una de las organizaciones de ransomware con mayor actividad a nivel internacional. Según el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), hasta abril de 2026 esta estructura había sido relacionada con más de 200 ataques en 50 países, dirigidos principalmente contra empresas de los sectores de manufactura, construcción, salud, finanzas y energía.

De acuerdo con los reportes oficiales, The Gentlemen concentra cerca del 10 % de los ataques de ransomware registrados en el mundo, lo que lo ubica como el segundo actor con mayor capacidad de afectación, solo por detrás de Qilin.

Así opera el grupo de ransomware señalado del ataque

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia advirtió que «el grupo mantiene actividad de intrusión activa y confirmada, con capacidad demostrada de comprometer el dominio completo de una organización y desplegar el cifrado en cuestión de minutos una vez alcanzados privilegios de administrador de dominio».

Las autoridades explicaron que esta organización apareció a mediados de 2025 y adoptó una identidad inspirada en la película The Gentlemen, del director Guy Ritchie. Además, mantiene un sitio propio en la dark web, desde donde publica información sobre sus operaciones y sus víctimas.

A diferencia de otros grupos de ransomware, The Gentlemen realiza un reconocimiento detallado de la infraestructura tecnológica de sus objetivos antes de ejecutar el ataque. Para ello utiliza herramientas como Advanced IP Scanner y Nmap, con las que identifica los equipos conectados, las cuentas con mayores privilegios y los puntos más vulnerables de la red.

Los análisis de su forma de operar indican que los ataques suelen comenzar mediante accesos de administración expuestos en internet o a través de credenciales robadas. Una vez dentro del sistema, los atacantes exploran la red interna, identifican los usuarios con mayor nivel de acceso y, posteriormente, extraen información sensible hacia servidores externos utilizando canales cifrados.

Como parte de la etapa final del ataque, eliminan registros de actividad y otras evidencias con el propósito de dificultar la investigación forense antes de activar el ransomware.

Según la información recopilada por las autoridades, el grupo supera las 250 víctimas en distintos países. La mayor parte de los casos se ha registrado en Estados Unidos y Tailandia, aunque también

hay ataques reportados en India, México, España, Francia y Colombia. En su propio portal de la dark web, The Gentlemen también se ha atribuido ataques contra BCN Medical y Canal Capital.

1. **¿Qué pasó con Ecopetrol tras el ciberataque de julio de 2026?**

Ecopetrol confirmó que los responsables del ciberataque publicaron información obtenida ilegalmente de 15 empresas del Grupo. La compañía informó que trabaja con la Fiscalía General de la Nación y el MinTIC para retirar el contenido difundido y limitar su acceso, mientras avanza la investigación sobre el incidente.

2. **¿Qué consecuencias advirtió Ecopetrol por la información filtrada?**

Ecopetrol señaló que las personas que accedan a la información publicada ilegalmente podrían incumplir las normas sobre protección y tratamiento de datos del Grupo Empresarial. Además, indicó que el alcance total del incidente, sus costos y posibles efectos regulatorios, judiciales, operativos y financieros aún no pueden determinarse.

3. **¿Qué afectaciones ha identificado Ecopetrol en sus sistemas tras el ataque?**

Ecopetrol aseguró que, hasta el momento, no ha identificado compromisos en sus plataformas transaccionales ni en las soluciones tecnológicas de sus empresas subordinadas, socios comerciales, proveedores o clientes. Sin embargo, precisó que continúa evaluando el impacto del incidente de ciberseguridad.

4. **¿Quién es The Gentlemen, el grupo señalado del ataque contra Ecopetrol?**

The Gentlemen es un grupo de ransomware como servicio (RaaS) al que se atribuye el ataque contra Ecopetrol. Según las autoridades, ha sido relacionado con más de 250 víctimas en distintos países y concentra cerca del 10 % de los ataques de ransomware registrados en el mundo, afectando principalmente a empresas de sectores como energía, salud, finanzas, manufactura y construcción.

ID: 16

ARTÍCULO ANTERIOR
Posesión de Abelardo De La Espriella: congresistas dicen que hay mayorías para autorizarla en Cali

ARTÍCULO SIGUIENTE
José Manuel Restrepo, el rey Felipe VI, Noboa, Milei y el resto de mandatarios que acompañarán a Keiko Fujimori en su posesión

ARTICULOS RELACIONADOS

DEJA UNA RESPUESTA

Comentario:

Nombre:*

Correo electrónico:*

Sitio web:

Guarde mi nombre, correo electrónico y sitio web en este navegador para la próxima vez que comente.

PUBLICAR COMENTARIO

el sector

MAGDALENA

Más de 105.000 adultos recibirán el pago de Colombia Mayor en el Magdalena

Cargar más >

RADIO HOY

(Lunes a Viernes 8:00 AM-12:00 M y 2:00–7:00 PM, Sábados 8:00 a 12:00 M)

DATOS DE CONTACTO

estudios@radiohoy.com

REDES SOCIALES

MARCAS ALIADAS

UBICACIÓN