Ciberataque contra Ecopetrol: la empresa coordina con la Fiscalía y el MinTIC el retiro de archivos filtrados

La compañía reconoció que aún no está en condiciones de establecer las consecuencias finales del incidente y señaló que los esfuerzos de remediación podrían no evitar divulgaciones adicionales ni procesos regulatorios o judiciales

Por **Frank Saavedra**

Ecopetrol activó acciones para retirar de internet información robada de 15 empresas de su grupo tras el ciberataque de julio de 2026 - crédito VisualesIA/Imagen Ilustrativa Infobae

29 Jul, 2026 07:50 a. m. | Actualizado: 29 Jul, 2026 08:57 a. m. CO

Ecopetrol activó acciones para retirar de internet información robada de 15 empresas de su grupo tras el ciberataque que sufrió la entidad el 17 de julio de 2026, mientras admitió que el impacto total del incidente sigue sin establecerse y que aún no puede descartar nuevas filtraciones, litigios o efectos sobre su operación y su situación financiera.

Te puede interesar:
De una pensión a la Casa de Nariño: así habría llegado Juliana Guerrero a ser una de las personas más influyentes en el gobierno de Gustavo Petro

La compañía informó que trabaja con la Fiscalía General de la Nación y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para **bajar el contenido publicado ilegalmente, restringir su acceso público y avanzar en las investigaciones**. Al mismo tiempo, señaló que el alcance, los efectos y los costos del ataque continúan en evaluación.

La compañía petrolera indicó que, hasta ahora, no ha identificado afectaciones en las soluciones tecnológicas transaccionales de su ecosistema digital ni en las de sus subordinadas o de su red de socios comerciales y financieros, proveedores y clientes. Esa revisión abarca las plataformas que soportan sus operaciones y la infraestructura tecnológica vinculada con terceros.

Te puede interesar:
Investigación periodística reveló que la vocera del Gobierno de De la Espriella no es abogada, pero se presenta como tal

Según la estatal petrolera, **la información divulgada corresponde a datos copiados de manera ilegal durante el incidente de ciberseguridad registrado**.

Información relevante

ecopetrol

Incidente ciberseguridad: Ecopetrol activó nuevos protocolos ante divulgación ilegal de información

Bogotá, 27 de julio de 2026

- **Ecopetrol en colaboración con autoridades realiza las acciones pertinentes para dar de baja la información publicada ilícitamente y restringir su acceso al público.**
- **Ecopetrol continúa adelantando acciones legales correspondientes contra el actor externo responsable.**

Ecopetrol S.A (BVC: ECOPETROL; NYSE: EC) 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. Por lo anterior, en colaboración con la Fiscalía General de la Nación, en particular con la Unidad de Delitos Informáticos, y el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTic), la Compañía está realizando esfuerzos para que la información publicada ilegalmente sea retirada del acceso público (*take down*) y otras acciones para limitar el acceso a dicha información.

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.

Ecopetrol planea continuar con las investigaciones y con los esfuerzos de colaboración con las autoridades competentes con el fin de mitigar y/o atenuar los efectos de las publicaciones ilegales por parte de los agentes externos.

Ecopetrol también confirma que 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.

El alcance total, el impacto y los costos de este incidente de ciberseguridad aún son inciertos. No puede garantizarse que los esfuerzos de remediación de la Compañía sean efectivos, que no se divulgue información adicional o que el incidente no dé lugar a procedimientos regulatorios, iniciación de litigios, daños reputacionales u otros efectos adversos materiales sobre el negocio, la situación financiera y/o los resultados de operación de la Compañía.

Ecopetrol es la compañía más grande de Colombia y una de las principales compañías integradas de energía en el continente americano, con más de 19,000 empleados. En Colombia es responsable de más del 60% de la producción de hidrocarburos, de la mayor parte del sistema de transporte, logística, y refinación de hidrocarburos, y tiene posiciones líderes en petroquímica y distribución de gas. Con la adquisición del 51.4% de las acciones de ISA, participa en la transmisión de energía, la gestión de sistemas en tiempo real (XM) y la concesión vial Costera Barranquilla - Cartagena. A nivel internacional, Ecopetrol tiene presencia en cuencas estratégicas del continente americano, con operaciones de E&P en Estados Unidos (cuenca del Permian y Golfo de México), Brasil y México, y a través de ISA y sus filiales tiene posiciones líderes en el negocio de transmisión de energía en Brasil, Chile, Perú y Bolivia, de concesiones viales en Chile y de telecomunicaciones

ECP-INFORMACION PUBLICA

La compañía coordina con la Fiscalía General de la Nación y el MinTIC el retiro de contenido ilegal y la investigación del ciberataque - crédito @ECOPETROL_SA/X

Las gestiones se realizan con la Unidad de Delitos Informáticos de la Fiscalía General de la Nación y con el MinTIC, **mediante procedimientos de retiro de contenido en internet conocidos como *take down* y otras medidas para limitar el acceso de terceros**.

Te puede interesar:
Paloma Valencia celebró la condena de nueve años de prisión contra Carlos Caicedo y lanzó duro mensaje al Pacto Histórico

La petrolera sostuvo que la extracción, publicación y uso indebido de información de propiedad del grupo empresarial vulneran las normas sobre protección y tratamiento de esa información.

En esa línea, advirtió: "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 respuesta de la empresa incluye la continuidad de las acciones legales contra el actor externo que señala como responsable del incidente. **También mantendrá activos sus protocolos de respuesta para contener la difusión de los archivos y reducir los efectos derivados de su publicación no autorizada.**

TIC | COLCERT

Comunicado a la Opinión Pública

Bogotá, julio 18 de 2026 (@Ministerio_TIC) – Frente al incidente cibernético reportado por Ecopetrol en las últimas horas, el Ministerio TIC se permite informar a la ciudadanía que:

- El Grupo de Respuestas a Emergencias Cibernéticas de Colombia (ColCERT) recibió el reporte correspondiente de parte de Ecopetrol el día de ayer. Desde ese momento se iniciaron las actividades de coordinación con los organismos pertinentes para entender lo sucedido y plantear líneas de defensa y atención.

- En el marco de esa coordinación, los grupos de defensa de Ecopetrol confirmaron la contención de los ataques recibidos.

- Como parte de esas acciones, el ColCERT mantiene canales de coordinación directa con la Dirección Especializada contra los Delitos Informáticos de la Fiscalía General de la Nación, con el propósito de apoyar la gestión de incidentes y fortalecer la respuesta institucional. También se mantiene contacto con los equipos de investigación judicial de la DIJIN de la Policía Nacional y el CTI de la Fiscalía.

- Además, continúa el acompañamiento diario a la gestión y definiendo necesidades de apoyo e intercambio de información directa con los equipos especializados de respuesta de Ecopetrol

- El ColCERT, como instancia nacional de coordinación para la gestión de incidentes de seguridad digital, articula esfuerzos con las capacidades del Estado y con actores especializados del ecosistema de ciberseguridad.

- El ColCERT seguirá acompañando a Ecopetrol durante este proceso. El Ministerio TIC informará oportunamente sobre las acciones que se desarrollen en el marco de esta gestión.

Consulte las publicaciones técnicas del ColCERT
Acceda a alertas, advertencias, informes, y demás publicaciones técnicas para fortalecer la prevención, identificar riesgos y mantenerse informado sobre las principales amenazas de seguridad digital.
https://www.colcert.gov.co/800/w3-propertyvalue-412601.html

Canales oficiales del ColCERT:
Sitio web: www.colcert.gov.co
Correo: contacto@colcert.gov.co
Línea telefónica Bogotá: +57 601 344 22 22
X: @colCERT

Pública

Ecopetrol confirmó que el incidente ocurrió el 17 de julio de 2026, cuando un actor externo intentó sustraer información de la compañía. Después, el grupo de *ransomware The Gentlemen* se atribuyó el ataque y publicó información relacionada con sus víctimas.

De acuerdo con el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, ColCERT, **esa estructura tenía actividad internacional y estaba vinculada con más de 200 ataques en 50 países hasta abril de 2026**. Los reportes oficiales también le atribuyen cerca del 10% de los ataques de *ransomware* registrados en el mundo y la ubican entre los grupos con mayor actividad, después de Qilin.

Las autoridades explicaron que el grupo realiza tareas de reconocimiento previo de las redes objetivo, identifica vulnerabilidades y equipos conectados, accede mediante servicios de administración expuestos en internet o credenciales obtenidas ilícitamente, explora la red interna, extrae datos hacia servidores externos por canales cifrados y elimina registros antes de ejecutar el cifrado de la información.

ColCERT 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**".

Los registros disponibles indican que la organización apareció a mediados de 2025, opera un sitio en la *dark web* y supera las 250 víctimas en distintos países, con casos reportados principalmente en Estados Unidos y Tailandia, además de India, México, España, Francia y Colombia. **El grupo también se ha atribuido ataques contra BCN Medical y Canal Capital**.

Ecopetrol no descartó nuevas filtraciones, litigios, procesos regulatorios y efectos sobre su operación y su situación financiera por el ciberataque - crédito Luisa González/Reuters

La empresa afirmó de forma expresa que todavía no puede determinar las consecuencias finales del incidente. En su actualización más reciente señaló: "**No puede garantizarse que los esfuerzos de remediación de la Compañía sean efectivos**, que no se divulgue información adicional o que el incidente no dé lugar a procedimientos regulatorios, iniciación de litigios, daños reputacionales u otros efectos adversos materiales sobre el negocio, la situación financiera y/o los resultados de operación de la Compañía".

Ese reconocimiento dejó abierta la posibilidad de nuevas publicaciones de información y de actuaciones administrativas o judiciales derivadas del caso. Mientras tanto, Ecopetrol mantendrá la coordinación con las autoridades para retirar el material divulgado ilegalmente, restringir su acceso y avanzar en las investigaciones sobre el ciberataque.