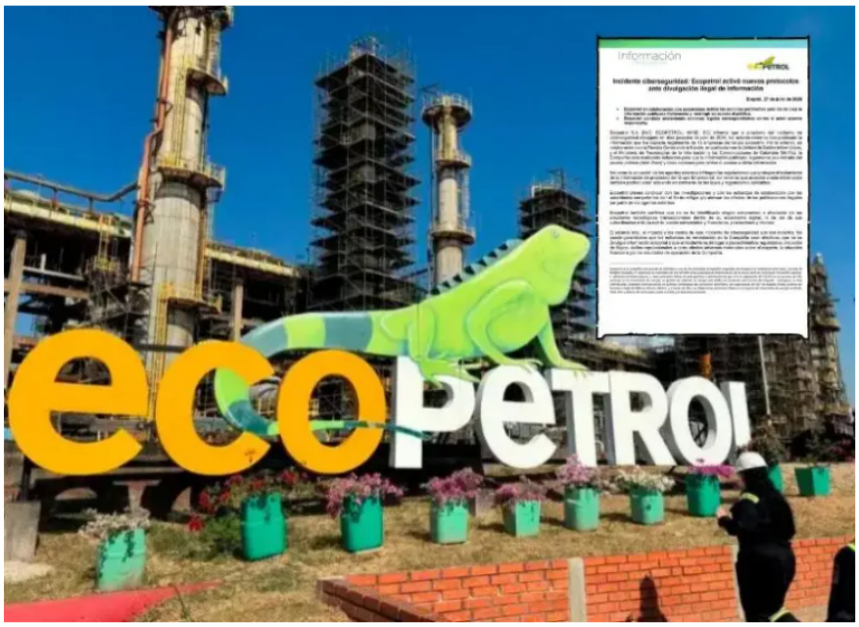
¿Ciberataque a Ecopetrol? Publican información de 15 empresas del grupo y la compañía pide intervención de las autoridades

La petrolera informó que trabaja con la Fiscalía y el MinTIC para retirar los archivos divulgados ilegalmente y limitar su acceso, mientras evalúa el alcance del incidente ocurrido en julio de 2026.



La compañía trabaja con Fiscalía y MinTIC para retirar archivos filtrados y limitar su acceso público. FOTO: Cortesía / Tomado de X: @ECOPETROL_SA

ESCUCHA EL RESUMEN
00:00 powerbeans 00:46

María Camila Salas Valencia hace 8 horas

Ecopetrol confirmó este 27 de julio de 2026 que **actores externos publicaron información copiada ilegalmente de 15 empresas pertenecientes al Grupo Ecopetrol**, luego del incidente de ciberseguridad reportado días atrás.

La compañía, desde Bogotá, informó que adelanta acciones junto con la Fiscalía General de la Nación y el Ministerio de Tecnologías de la Información y las

Las más leídas


En La Bastilla harán "gran trueque literario" de más de 5.500 libros
hace 30 minutos


De la Espriella designó a Carolina Bazurdo como secretaria privada de Presidencia; esta será su función
hace 56 minutos


Atención: Murió el reconocido escritor y periodista Plinio Apuleyo Mendoza
hace 2 horas

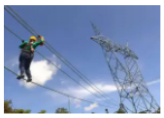

La Eurocopa 2028 no tiene ningún clasificado, pero ya conoce las ocho ciudades que serán sede en cuatro países
hace 2 horas


Traslado de planta enfrenta a Essity y al sindicato de Familia
hace 2 horas

Te recomendamos


Todo lo que hay que saber

General de la Nación y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para retirar el contenido del acceso público, limitar su difusión y avanzar en las investigaciones sobre el ataque.



Economía

Precio de la energía en bolsa se disparó casi 400% en junio, impulsado por mayor uso de plantas térmicas

La empresa indicó que continúa con las acciones legales correspondientes contra el actor externo señalado como responsable del incidente y que mantiene activos sus protocolos de respuesta para mitigar los efectos derivados de la publicación no autorizada de información.

Ecopetrol busca retirar la información divulgada ilegalmente

A través de un comunicado, Ecopetrol S.A. explicó que la publicación de los archivos corresponde a **información que fue extraída de manera ilegal durante el incidente de ciberseguridad registrado en julio de 2026.**

La compañía señaló que, en coordinación con la Unidad de Delitos Informáticos de la Fiscalía General de la Nación y el MinTIC, desarrolla acciones para lograr el retiro del contenido publicado mediante procesos de eliminación de información de internet, conocidos como *take down*, además de implementar medidas orientadas a restringir el acceso de terceros.

Ecopetrol indicó que continuará con las investigaciones y con el trabajo conjunto con las autoridades competentes para establecer el alcance del incidente y reducir los efectos asociados a la divulgación de los archivos.

Lea más: **Corte cambia importante requisito para recibir subsidio en cajas de compensación, ¿de qué se trata?**

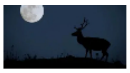
Posibles implicaciones legales por acceso a la información filtrada

La compañía advirtió que tanto la extracción como la difusión de información perteneciente al Grupo Empresarial pueden representar incumplimientos frente a las normas que regulan la protección y tratamiento de datos.

Además, señaló que las personas que accedan al contenido publicado por los atacantes podrían enfrentar consecuencias legales si actúan en contra de las disposiciones vigentes.

“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”, señaló Ecopetrol.

La petrolera afirmó que mantendrá las acciones legales y técnicas necesarias mientras avanza la investigación sobre el origen y las consecuencias del ataque.


sobre la Luna del Ciervo: fecha, hora y cómo verla desde Colombia

hace 4 horas


Las veces que Petro ha defendido a cercanos untados de corrupción

hace 13 horas

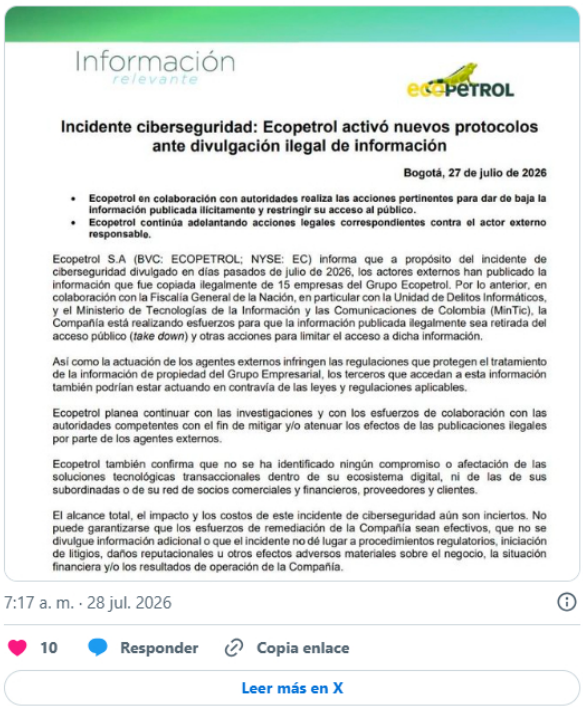

Nueva pelea entre Petro y Angie Rodríguez: la echó y reveló su historia clínica por negarse a mover $1 billón para El Niño

hace 13 horas


Doña María Antonia llegará a los 125 años y desde Cali contó el secreto de su larga vida

#InformaciónRelevante | Incidente ciberseguridad: Ecopetrol activó nuevos protocolos ante divulgación ilegal de información.

Lee más aquí 👇



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.

7:17 a. m. · 28 jul. 2026

10 Responder Copia enlace

Leer más en X

Le puede interesar: **A Antioquia le llega el 51% de la inversión social de las empresas del país**

No se identifican afectaciones en sistemas transaccionales

Ecopetrol informó que, hasta el momento, **no ha identificado compromisos ni afectaciones en las soluciones tecnológicas transaccionales** que hacen parte de su ecosistema digital.

La compañía también señaló que las revisiones realizadas no evidencian impactos en las plataformas tecnológicas de sus empresas subordinadas ni en los sistemas utilizados por su red de socios comerciales y financieros, proveedores y clientes.

“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”, indicó.

La empresa explicó que las medidas actuales están enfocadas en contener la divulgación de la información, fortalecer los controles de seguridad y continuar con el análisis técnico del incidente.

Siga leyendo: **Cargar carro eléctrico en Colombia será más fácil: nueva regulación simplifica reglas para instalar electrolineras**

Impacto económico y alcance del incidente permanecen en evaluación

La compañía informó que todavía no es posible establecer el alcance total del ataque, sus impactos o los costos asociados al incidente de ciberseguridad.

Ecopetrol señaló que no puede garantizar que las medidas de remediación sean completamente efectivas, que no se presenten nuevas publicaciones de información o que el caso no genere procesos administrativos, judiciales o efectos sobre la operación y los resultados financieros de la empresa.

“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”.

No se pierda: **BACU acelera su expansión en Medellín: superó 40.000 órdenes y proyecta abrir 10 nuevos restaurantes**

The Gentlemen se atribuyó el ataque contra Ecopetrol

El incidente de ciberseguridad contra Ecopetrol **ocurrió el 17 de julio de 2026**, cuando un actor externo intentó sustraer información de la compañía. Posteriormente, el grupo de ransomware The Gentlemen se atribuyó la responsabilidad del ataque y publicó información relacionada con sus víctimas.

Según el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), esta organización había sido identificada como una estructura con actividad internacional y relacionada con más de 200 ataques en 50 países hasta abril de 2026.

Los reportes oficiales señalan que **The Gentlemen concentra cerca del 10 % de los ataques de ransomware registrados en el mundo** y se encuentra entre los grupos con mayor actividad, después de Qilin.

De interés: **¿Usaría el cupo de su tarjeta de crédito para pagar por Bre-B? Nu Colombia ya lo permite, esto es lo que debe saber**

Así opera el grupo de ransomware señalado

Las autoridades han explicado que The Gentlemen utiliza métodos de reconocimiento previo de las redes objetivo antes de ejecutar sus ataques. Para identificar vulnerabilidades y equipos conectados, emplea herramientas como Advanced IP Scanner y Nmap.

De acuerdo con los análisis realizados, la operación del grupo incluye las siguientes fases:

-Identificación de sistemas, dispositivos y cuentas con altos privilegios dentro de la infraestructura tecnológica.

-Acceso inicial mediante servicios de administración expuestos en internet o credenciales obtenidas de manera ilícita.

-Exploración de la red interna para ubicar información de interés y ampliar los permisos de acceso.

-Extracción de datos hacia servidores externos mediante canales cifrados.

-Eliminación de registros y evidencias digitales antes de ejecutar el cifrado de información.

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 indicaron que la organización apareció a mediados de 2025 y que mantiene un sitio en la dark web donde publica información sobre sus operaciones y las empresas afectadas.

De acuerdo con los registros disponibles, **The Gentlemen supera las 250 víctimas en diferentes 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 aseguró que continuará trabajando con las autoridades para retirar la información publicada ilegalmente, restringir su acceso y avanzar en las investigaciones relacionadas con el incidente de ciberseguridad registrado en julio de 2026.

Bloque de preguntas y respuestas:

¿Qué empresas del Grupo Ecopetrol fueron afectadas por la publicación ilegal de información?

Ecopetrol informó que la información divulgada ilegalmente corresponde a archivos copiados de 15 empresas que hacen parte del Grupo Ecopetrol. La compañía no detalló públicamente cuáles fueron esas empresas afectadas.

¿Cuándo ocurrió el ciberataque contra Ecopetrol?

El incidente de ciberseguridad contra Ecopetrol ocurrió el 17 de julio de 2026, cuando actores externos intentaron extraer información de la compañía. La publicación de los archivos obtenidos ilegalmente fue confirmada posteriormente por la empresa.

¿Qué está haciendo Ecopetrol para retirar la información filtrada de internet?

Ecopetrol trabaja 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) para solicitar el retiro del contenido publicado ilegalmente y limitar su acceso público.

¿Quién fue el responsable del ciberataque contra Ecopetrol?

El grupo de ransomware The Gentlemen se atribuyó el ataque contra Ecopetrol. Las autoridades colombianas habían identificado previamente a esta organización como un actor con actividad internacional relacionado con múltiples ataques de ransomware.

Temas recomendados | Economía | Empresas | Ecopetrol | Ciberataque | Ministerio TIC | Informe | Comunicado | intervención | Fiscalía | Autoridades

Para seguir leyendo

Economía

¿Quién es Joaquín Gutiérrez? La mano derecha de De la Espriella que suena para presidir Ecopetrol pero no tiene experiencia en hidrocarburos

hace 2 horas

Economía

Apple desbanca a Nvidia tras acercarse a los US$5 billones en bolsa

hace 11 minutos

Economía

En casi la mitad de los países donde se cerrarán embajadas hay déficit comercial

hace 7 horas

Economía

Usuarios han transferido $97,1 billones a las generadoras de energía, pero la capacidad no ha mejorado: Superservicios

hace 4 horas

Traslado de planta enfrenta a Essity y al sindicato de Familia

Trabajadores señalan presiones por el traslado de la planta de Medellín a Cajicá. Essity afirma que la transición es gradual.

La transición de la planta de Essity (antes Grupo Familia) en Medellín hacia Cajicá generó un conflicto laboral: el sindicato denuncia presiones y la empresa asegura que el proceso será gradual. FOTO **CORTESÍA SINALTRAFAMILIA**

El Colombiano hace 3 horas

La **decisión de Essity de trasladar gradualmente la producción de su planta de Medellín hacia Cajicá mantiene abierto un conflicto laboral** con el sindicato Sinaltrafamilia. Mientras los trabajadores denuncian presiones para aceptar el traslado o acuerdos de retiro, la compañía sostiene que el proceso busca fortalecer la competitividad y garantizar la sostenibilidad del negocio.

Según Essity (antes Grupo Familia), la reconfiguración hace parte de una evaluación de su red de manufactura de productos de papel de consumo en Colombia. La empresa indicó que las líneas de producción serán trasladadas por etapas a Cajicá, pero aclaró que mantendrá sus operaciones en el país y garantizará el abastecimiento de sus productos y el cumplimiento de sus compromisos comerciales.

Sindicato denuncia presiones

Los trabajadores sindicalizados mantienen un cese de actividades desde el 17 de julio y permanecen en una carpa instalada en la portería de la planta de Medellín,