Ciberataque a Ecopetrol: qué datos quedaron expuestos

Permitió la extracción de archivos vinculados a unas 3.300 cuentas de usuario de 15 empresas del grupo. Parte de la información ya fue publicada y podría incluir datos sensibles de empleados y del negocio petrolero.

Por: Redacción de ITSitio | 10 de agosto 2026

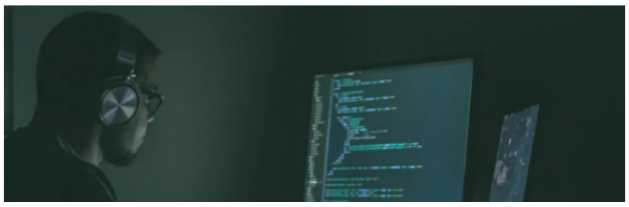
El ciberataque a Ecopetrol expuso información de miles de usuarios.

Seguridad

Un ciberataque a Ecopetrol, la compañía más grande de Colombia y una de las principales empresas energéticas de América Latina, terminó con información corporativa y de empleados publicada ilegalmente en Internet.

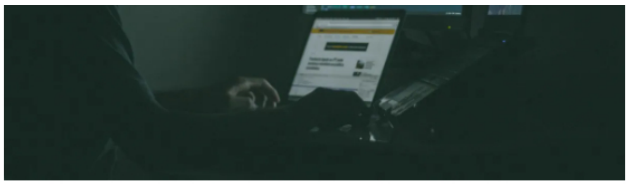
El incidente comenzó a conocerse públicamente el 17 de julio de 2026, cuando la petrolera informó que un actor externo había obtenido acceso no autorizado a recursos digitales de la compañía y de varias de sus subsidiarias. Los atacantes también intentaron ejecutar un ataque de ransomware para cifrar información, pero los sistemas de seguridad lograron bloquear esa etapa de la ofensiva.

Sin embargo, impedir el cifrado no evitó el robo de datos. Ecopetrol confirmó que los responsables consiguieron descargar archivos asociados con aproximadamente 3.300 cuentas de usuario y 15 empresas del Grupo Ecopetrol.



Lo más leído de Seguridad

Los usuarios de Mac reportan más ataques que los de Windows, pero usan menos herramientas de seguridad



Ecopetrol confirmó que un ciberataque permitió descargar archivos asociados con unas 3.300 cuentas de usuario y 15 empresas de su grupo.

Días más tarde llegó una nueva preocupación: el 27 de julio la compañía reconoció oficialmente que parte de la información copiada ilegalmente había sido publicada por los atacantes.

¿Qué pasó en el ciberataque a Ecopetrol?

De acuerdo con la información presentada por Ecopetrol ante la Comisión de Bolsa y Valores de Estados Unidos (SEC), el incidente involucró el acceso no autorizado a entornos de almacenamiento de archivos basados en la nube.

Los atacantes no solamente extrajeron información, sino que **realizaron exigencias de extorsión y amenazaron con divulgar públicamente los datos obtenidos**. Ecopetrol también detectó un intento de ransomware, aunque aseguró que sus controles de ciberseguridad lograron impedir el cifrado de los sistemas.

El 20 de julio, tras realizar nuevos análisis, la compañía señaló que el impacto se había limitado **"exclusivamente a la descarga de archivos"** y que no había identificado alteraciones en la integridad de la información. También sostuvo que las credenciales de acceso asociadas con los usuarios afectados no habían sido capturadas.

Ese escenario cambió parcialmente una semana después, no porque se detectaran problemas operativos, sino porque los atacantes comenzaron a publicar los archivos robados.

Los sistemas de seguridad de la petrolera bloquearon el intento de cifrar información, pero no evitaron la extracción de archivos.

Qué información de Ecopetrol habría quedado expuesta

Determinar exactamente qué datos fueron comprometidos sigue siendo uno de los puntos más sensibles del incidente.

Ecopetrol confirmó la publicación ilegal de información perteneciente a 15 empresas de su grupo, pero hasta el momento no ha detallado públicamente el contenido completo de cada archivo divulgado.

Investigaciones periodísticas realizadas sobre muestras de los documentos publicados señalan que entre la información podrían existir **datos financieros y personales de empleados, documentos internos y datos relacionados con las operaciones petroleras**.

El grupo de ciberdelincuentes que se atribuyó el ataque asegura haber obtenido alrededor de **un terabyte de información y más de 327.000 archivos**. Entre el material que dice poseer aparecen registros vinculados con campos petroleros,

nóminas, información bancaria, datos médicos y biométricos de trabajadores y documentación corporativa. Estas cifras y categorías provienen de los propios atacantes y no han sido confirmadas en su totalidad por Ecopetrol.

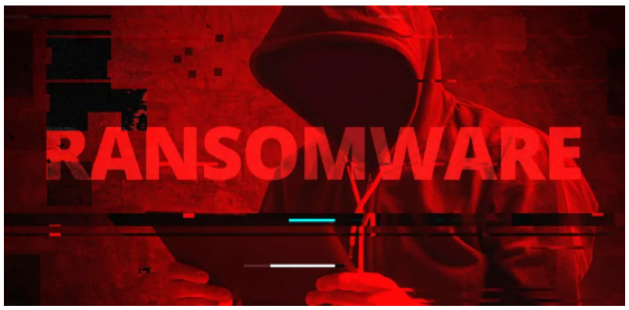
Ecopetrol asegura que sus operaciones no fueron afectadas

Pese al volumen de información extraída, uno de los principales datos comunicados por la petrolera es que el ataque **no provocó una interrupción crítica de sus operaciones**.

La compañía informó que no identificó afectaciones en las soluciones tecnológicas transaccionales de Ecopetrol, sus subsidiarias ni en las utilizadas por su red de socios comerciales, entidades financieras, proveedores y clientes.

Tampoco se informaron alteraciones significativas en la producción de hidrocarburos o en los servicios esenciales.

El punto resulta especialmente relevante por el peso estratégico de la compañía. Ecopetrol tiene más de **19.000 empleados** y es responsable de más del **60% de la producción de hidrocarburos de Colombia**, además de tener presencia en transporte, refinación, petroquímica, gas, transmisión eléctrica y otros negocios energéticos.



Los atacantes combinaron la extracción de información con amenazas de extorsión y un intento de ransomware que no logró cifrar los sistemas.

The Gentlemen, el grupo que se atribuyó el ataque

Aunque Ecopetrol inicialmente informó que el responsable era un actor externo todavía no identificado, el grupo de ransomware **The Gentlemen** se atribuyó posteriormente el ciberataque y publicó información presuntamente extraída de la compañía.

The Gentlemen es una operación de **ransomware como servicio o RaaS**, un modelo en el que los desarrolladores de herramientas maliciosas trabajan con afiliados encargados de infiltrarse en organizaciones y ejecutar los ataques.

Según Check Point Research, el grupo apareció a mediados de 2025 y experimentó un rápido crecimiento durante 2026. Para abril ya había publicado más de 320 víctimas y se había convertido en uno de los grupos de ransomware más activos a nivel mundial.

Una investigación posterior de la compañía de ciberseguridad indicó que la organización superó las 400 víctimas públicas y que suele obtener el acceso inicial mediante **dispositivos perimetrales sin actualizar o credenciales previamente comprometidas o adquiridas**.

Cómo habrían conseguido acceder a Ecopetrol

La investigación sobre el punto de entrada sigue abierta.

El acceso habría comenzado a través de **un tercero que poseía privilegios de administrador**. Una vez dentro del entorno, los atacantes habrían utilizado herramientas de seguridad y análisis como Kali Linux para avanzar sobre

sistemas de tecnología de la información y obtener datos de funcionarios.

Esta información todavía forma parte de una investigación en etapa de indagación y no constituye una conclusión definitiva sobre cómo comenzó el ataque.

El caso vuelve a poner en primer plano un desafío creciente para las grandes organizaciones: la seguridad ya no depende únicamente de proteger los sistemas propios, sino también de controlar los accesos privilegiados otorgados a proveedores, contratistas y otros integrantes de la cadena tecnológica.

El caso evidencia los riesgos que representan los accesos privilegiados de proveedores, contratistas y otros terceros para las grandes organizaciones.

Qué está haciendo Ecopetrol tras el ciberataque

Tras confirmarse la divulgación de los archivos, Ecopetrol activó nuevos protocolos y comenzó a trabajar junto con la **Fiscalía General de la Nación y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)** para intentar retirar el contenido publicado y restringir su acceso.

La compañía también inició acciones legales contra los responsables y mantiene las tareas de investigación y monitoreo de sus sistemas.

El alcance total del **ciberataque a Ecopetrol**, sus costos y las consecuencias de la exposición de información todavía no están definidos. Lo que sí está confirmado es que los atacantes consiguieron superar una primera barrera de seguridad, descargar miles de archivos y convertir un intento fallido de ransomware en un incidente de exposición de datos que continúa generando riesgos semanas después del acceso inicial.

Preguntas frecuentes

1. **¿Cuántas cuentas fueron afectadas por el ciberataque a Ecopetrol?** Ecopetrol informó que los atacantes descargaron ilegalmente archivos asociados con aproximadamente **3.300 cuentas de usuario** pertenecientes a 15 empresas del grupo.
2. **¿Qué información fue filtrada de Ecopetrol?** La empresa confirmó la publicación de información robada, aunque no detalló todo su contenido. Investigaciones sobre muestras filtradas identificaron documentos corporativos, datos financieros y personales de empleados e información vinculada con operaciones petroleras.
3. **¿Quién está detrás del ataque a Ecopetrol?** El grupo de ransomware **The Gentlemen** se atribuyó públicamente el ataque. Sin embargo, las investigaciones oficiales sobre los responsables y sobre la forma exacta en que se produjo la intrusión continúan abiertas.

Redacción de ITSitio

Ver Publicaciones

Ecopetrol

Publicaciones Relacionadas

Los usuarios de Mac reportan más ataques que los de Windows, pero usan menos herramientas de seguridad

Redacción de ITSitio | 29 julio, 2026

Colombia, entre los países afectados por la campaña de ciberataques StrikeShark

Redacción de ITSitio | 29 julio, 2026

WhatsApp ya es uno de los canales favoritos para distribuir malware: alertan por una campaña que simula facturas y pagos

Redacción de ITSitio | 21 julio, 2026

WhatsApp ya es uno de los canales favoritos para distribuir malware: alertan por una campaña que simula facturas y pagos

Tener un backup ya no alcanza: el dato que define si una empresa sobrevive a un ciberataque

10,9 billones de intentos de ataque: por qué las cifras de ciberseguridad pueden confundir a las empresas colombianas

ANTERIOR
Trendline Technology integra NetApp y refuerza su ecosistema de solucio...

SIGUIENTE
Colombia alcanza 10 millones de accesos 5G y acelera su conectividad