



6AM W

Justicia

“La información ya se encuentra en la dark web”: experto sobre ciberataque a Ecopetrol

Yefrin Garavito, director de la Unidad de Investigación de la Defensa, explicó el ABC completo del ciberataque del que fue víctima la estatal Ecopetrol.



O. Pérez ✕ | J. Esteban ✕ @
29/07/2026 - 06:33 GMT-5



Añadir Caracol Radio en Google

El ciberataque contra Ecopetrol continúa revelando detalles sobre la información que fue extraída por los delincuentes informáticos y los riesgos que representa su publicación. Un análisis conocido por 6AM W de Caracol Radio señala que los atacantes habrían obtenido cerca de un terabyte de información, **equivalente a 327.095 archivos, de los cuales 11 fueron clasificados como críticos y tres como de alto riesgo.**

De acuerdo con el documento, entre la información comprometida hay **429 archivos relacionados con credenciales y controles de acceso.** También se habrían llevado cerca de 64 gigabytes de información correspondiente a operaciones financieras y del tesoro, además de 584 archivos relacionados con pagos realizados por la petrolera.

En entrevista con 6AM W de Caracol Radio, Yefrin Garavito, investigador forense de la Unidad de Investigación de la Defensa y colaborador de la Fiscalía y la Policía Nacional, explicó que detrás del ataque estaría el grupo de ciberdelincuentes conocido como Gentleman, especializado en ataques de ransomware dirigidos contra

Lo más leído

Fueron encontrados los cuatro policías que estaban desaparecidos en Cerro Santana, Cauca

28/07/2026

Tabla horas extra para 2026 Colombia: Valores y recargos actualizados tras reducción jornada laboral

27/07/2026

Transportadores evidencian la afectación ante la contingencia en la vía La Línea por un derrumbe

28/07/2026

Arena USC de Cali será el escenario de la posesión presidencial de Abelardo de la Espriella

28/07/2026

Detenidas más de 400 personas por posesión de drogas en el festival de música Tomorrowland

28/07/2026

Últimas Noticias

Legalizan captura de excandidato al Senado que habría favorecido a 'Papá Pitufo'

Angie Rodríguez pide protección tras denunciar intimidaciones de funcionarios del DNI y criminales

Defensa del alcalde de Villa de Leyva denuncia presunta persecución judicial

Se formaliza la primera Área Especial de Manejo de Residuos Sólidos de

empresas de alto valor.

“Es un grupo de ciberdelincuentes que se ha especializado en desarrollar ransomware focalizado para empresas de alto flujo. **Han atacado más de 300 empresas en todo el mundo, incluyendo organizaciones en Latinoamérica y Colombia**”, explicó.

Garavito señaló que el ataque tuvo dos fases. La primera consistió en el robo de información mediante el acceso a credenciales y servicios en la nube. La segunda buscaba cifrar los sistemas de Ecopetrol para impedir el acceso a la información y exigir el pago de un rescate. Sin embargo, aseguró que esa etapa fue bloqueada por los mecanismos de ciberseguridad de la compañía.

Lea más: [Así se orquestó el ciberataque a Ecopetrol: Fiscalía investiga](#)

“Obtuvieron credenciales e información de la nube de varios usuarios de Ecopetrol, pero cuando intentaron activar el ransomware, los sistemas de la empresa generaron las alertas y bloquearon el ataque. Por eso no llegó a mayores”, afirmó.

El experto confirmó que **la información robada ya fue publicada en la dark web** luego de que, presuntamente, Ecopetrol no accediera a negociar con los responsables del ataque.

“Esa información ya se encuentra en la dark web. Los atacantes intentaron realizar una negociación, publicaron un cronómetro para que fueran contactados y, al no lograrlo, decidieron divulgar la información para generar un daño reputacional”, indicó.

Aunque explicó que una persona del común difícilmente accederá a esos archivos, advirtió que sí representan un riesgo para otros actores especializados en ataques informáticos.

“Quienes buscan este tipo de información saben cómo ingresar a la dark web. Allí pueden encontrar documentación que incluso incluye planos de infraestructura crítica, lo que podría facilitar la planeación de nuevos ataques. Ecopetrol tendrá que fortalecer no solo la ciberseguridad, sino también la seguridad física de sus instalaciones”, sostuvo.

Garavito añadió que, una vez la información es publicada en la dark web, resulta muy difícil eliminarla completamente.

“Quien descargue esa información puede volver a publicarla en otros sitios, como ha ocurrido con otras grandes filtraciones internacionales. Es muy difícil recuperarla o impedir que siga circulando”, explicó.

Sobre la forma en que se produjo el ataque, el investigador aseguró que una de las hipótesis que deberán verificar las autoridades es si **existió el uso indebido de credenciales de un usuario con altos privilegios**, lo que incluso podría abrir la puerta a investigar una posible participación interna.

“Para acceder a los servidores y a los servicios en la nube tuvieron que utilizar una credencial de usuario. El análisis forense permitirá identificar cuál fue la cuenta utilizada para el escalamiento de privilegios y establecer **si se trató de un descuido o si hubo una entrega deliberada de esa información**”, señaló.

Consultado sobre el monto que habría exigido el grupo criminal, Garavito indicó que no fue posible establecer una cifra porque

de reincorporación colectiva del país

“Volver a jugar bajo la luna”, el informe de mujeres afro que retrata el impacto de la guerra

“Es el triunfo de la voz de las víctimas”: Norma Vera tras la nueva condena contra Hernán Giraldo

Caracas, mayo 2020. ¿Por qué no se puede establecer una tregua porque Ecopetrol nunca inició conversaciones con los atacantes.

“Empresas como Ecopetrol no pueden negociar con este tipo de organizaciones por las restricciones legales y los protocolos de cumplimiento. En otros casos documentados a nivel internacional, **las exigencias económicas por ataques de ransomware han oscilado entre 250.000 dólares y hasta 10 millones de dólares**”, concluyó.

Escuche la entrevista completa a continuación:



Escuchar Caracol Radio EN VIVO:



La IA que hace dinero: ¿por qué está causando tanto ruido en la web?

Una aplicación que utiliza IA para ganar dinero ha sido lanzada al ...

Hivora



Una aplicación que utiliza inteligencia artificial para ganar dinero ha sido lanzada al...

La IA que hace dinero: ¿por qué está causando tanto ruido en la web?

Altrix



CFD: La IA que hace dinero: ¿por qué está causando tanto ruido en la web?

¿Por qué todos están hablando de los CFD con IA que generan ingresos?

Lenrbey



Una inversión en CFD con IA podría proporcionarle un ingreso adicional.

¡Deja que la tecnología de IA cambie tu vida financiera! Comienza ahora ...

Eraeyt



Expresidente Uribe aseguró tener información de reunión entre el Pacto Histórico con...

El expresidente Uribe hizo esa afirmación en medio de las reuniones...

Caracol Radio



Futuros de oro vs CFDs: Lo que los traders deben saber

Aprende cómo el trading de CFDs te permite especular sobre los precios ...

IC

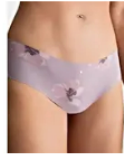
Más información



Colombianos: conoce cómo funciona una plataforma con Grupo Argos empezando desde...

Descubre Grupo Argos desde \$205 [Únete]

Gemrgo



Panty cachetero microfibra invisible estampado - S

Panty tipo cachetero invisible. De tiro medio, elaborado en tejido ...

Punto Blanco C.O

¡lo quiero!



Curso gratuito para aprender a invertir en los mercados financieros

iFOREX

Empieza ahora



Tu próxima fuente de ingresos podría estar en Avianca CFD

Empieza a ganar un segundo sueldo con Avianca CFD [Regístrate]

segundo ingreso

Solicita ahora



“Es algo grave”: experto en geopolítica sobre abandono de cúpula militar en discurso de...

Luis Alberto Villamarín Pulido señaló que la relación entre las cúpulas y el...

Caracol Radio



Cajicá: Consulta el valor de cualquier casa al instante por dirección

WonderMapped

Más información



Audio del general Ospina.



Cuchillos japoneses:



Gobiernos De la Esperiella y

excomandante del Ejército, confirmaría montaje contra el...

En la conversación, Ospina también reconoce que había personas con ...

Caracol Radio



Cada mañana merece un gran café

Con De'Longhi, el aroma, el sabor y la crema perfecta se convierten en part...

USA Electrodomésticos

liquidación 50% off ya disponible en Cajicá

Hojas forjadas a mano en acero carbono a precio de fábrica

mejorentrega



¿Rostro caído? Olvida el colágeno. Haz esto por la noche (muy fácil)

Míralo antes de que lo borren, está dando que hablar

Piel Renovada

Petro se vuelven a reunir para hablar de la posesión del 7 d...

Aunque no se reanudará el empalme, ambos gobiernos sí se reúnen para ...

Caracol Radio



Combina comodidad y estilo con estos tenis para mujer

Paga al recibirlos en casa ¡El envío es gratis!

Tenis Skechers

Compra ahora



Capturaron a alias 'Melissa Fierro', una temida sicaria de 18 años en Girardot

La mujer tenía orden judicial por homicidio en grado de tentativa y ...

Caracol Radio



Los aires acondicionados sin unidad exterior son tendencia en 2026 (ver precios)

PocketNotebooked

Más información



"Hay más de 4.000 pruebas": Federico Gutiérrez rechaza freno a investigación contra...

El mandatario distrital confirmó la apelación del caso y advirtió presunt...

Caracol Radio

Enlaces Promovidos por Taboola

Artículo anterior



Policía que participó en las interceptaciones a Marellys Meza será testigo de la Fiscalía

Juan Esteban Quintero
29/07/2026

Artículo siguiente



Altos mandos sabían que asesinábamos a inocentes: exmilitar por falsos positivos en la Costa Caribe

Cristina Navarro 28/07/2026

© CARACOL S.A. Todos los derechos reservados.

CARACOL S.A. realiza una reserva expresa de las reproducciones y usos de las obras y otras prestaciones accesibles desde este sitio web a medios de lectura mecánica u otros medios que resulten adecuados.

Contacto | Contacto Ventas | Newsletter | Pago electrónico clientes | Alta de Clientes | Registro de proveedores | Aviso legal | Política de Protección de Datos | Política de cookies | Configuración de cookies | Transparencia | Código Ético



Bogotá

La Luciérnaga Gabriel Delascasas



Directo



Directo



Noticias en 3'



Últimos programas