Ecopetrol denuncia ciberataque: hackean información de 15 empresas del grupo y extorsión

17 de julio de 2026

Un actor externo logró acceder a sistemas de almacenamiento en la nube y descargar información asociada a cerca de 3.300 cuentas de usuario. La compañía activó protocolos de emergencia, presentó denuncia penal y advirtió sobre posibles riesgos reputacionales.

Ecopetrol confirmó este viernes que fue víctima de un grave incidente de ciberseguridad que comprometió información de varias empresas del grupo empresarial. Según informó la compañía, un actor externo no identificado logró ingresar de manera irregular a entornos de almacenamiento en la nube y descargar datos corporativos, tras lo cual lanzó amenazas de extorsión para evitar la divulgación pública de la información obtenida.

La petrolera colombiana aseguró que el ataque incluyó un **intento de secuestro de información mediante la modalidad conocida como *ransomware*, aunque este fue neutralizado** gracias a los sistemas de protección implementados por la organización.

¿Qué pasó?

De acuerdo con el comunicado oficial divulgado por Ecopetrol, los equipos de seguridad detectaron un acceso no autorizado a recursos digitales pertenecientes al grupo empresarial.

La compañía explicó que **«un actor externo aún no identificado»** logró ingresar a plataformas de almacenamiento en la nube utilizadas por aproximadamente **15 empresas del Grupo Ecopetrol**, generando la descarga irregular de información relacionada con cerca de **3.300 cuentas de usuario**.

En el documento, la petrolera señala que **«el acceso no autorizado afectó entornos de almacenamiento de archivos en la nube de aproximadamente 15 compañías del GE, lo que resultó en la descarga no autorizada de datos asociados con aproximadamente 3.300 cuentas de usuario»**.

CASO NIÑAS TALIO – ENTREVISTA ZULMA GUZMÁN

QUÉ NOTICIA BUSCAS?

BUSCAR ...

ULTIMAS NOTICIAS

Ecopetrol denuncia ciberataque: hackean información de 15 empresas del grupo y extorsión

Momentos de terror en Bogotá: hombre tomó como rehén a una mujer con un cuchillo en plena vía

Así avanza la conformación del gabinete presidencial de Abelardo de la Espriella: estos son los ministros ya designados y los cargos que siguen vacantes

Paola Holguín asumirá el Ministerio de Cultura en el gobierno de Abelardo de la Espriella

Bogotá vivirá un histórico 20 de Julio: el desfile militar llega por primera vez a Ciudad Bolívar y habrá cambios masivos en TransMilenio

Alerta por la calidad del aire para la final del Mundial 2026 entre Argentina y España

a ciertos recursos digitales de su propiedad, por parte de un actor externo aún no identificado, así como un intento de ejecución de Ransomware (secuestro de información) que fue bloqueado oportunamente por los controles de ciberseguridad implementados al interior del Grupo Empresarial (GE). El acceso no autorizado afectó entornos de almacenamiento de archivos en la nube de aproximadamente 15 compañías del GE lo que resultó en la descarga no autorizada de datos asociados con aproximadamente 3.300 cuentas de usuario. El actor externo comunicó exigencias de extorsión, amenazando con divulgar públicamente la información extraída ilegalmente.

Ante el desarrollo de este incidente Ecopetrol S.A. inició una investigación y activó los protocolos de atención y respuesta a incidentes, además del despliegue de las siguientes actividades, con el propósito de evitar que la información, objeto de extracción ilegal, sea divulgada públicamente por el actor externo, se materialicen afectaciones reputacionales, actuaciones de entidades de supervisión y/o potenciales costos financieros asociados con la investigación, la remediación y el cumplimiento normativo:

a. Revocación inmediata de accesos no autorizados a los activos digitales comprometidos.
b. Bloqueo de mecanismos asociados a descargas masivas de información.
c. Identificación, análisis y contención de las tácticas, técnicas y procedimientos (TTPs) utilizados por el actor malicioso.
d. Formulación de denuncia penal ante la Fiscalía General de la Nación y despliegue de actividades de cooperación con entidades nacionales especializadas.
e. Identificación de infraestructuras externas utilizadas para el almacenamiento o descarga de información con el fin de gestionar acciones de restricción o bloqueo.
f. Activación de mecanismos de acompañamiento con aseguradoras y áreas especializadas de mercado de capitales para la adecuada gestión del evento.
g. Valoración detallada de la información descargada y determinación de su criticidad.
h. Monitoreo intensificado de la infraestructura tecnológica bajo esquemas de alertamiento crítico y validación continua de controles preventivos y detectivos.

A la fecha, Ecopetrol S.A. no ha identificado ninguna interrupción material de sus operaciones críticas, capacidad de producción o servicios esenciales, ningún impacto financiero directo que le impida seguir desarrollando su objeto social o la divulgación efectiva de la información objeto de acceso ilegal. Sin embargo, continúa evaluando la posible exposición de información corporativa que podría incluir datos confidenciales, de carácter reservado, de propiedad exclusiva o datos personales, pues no es posible asegurar que este incidente no vaya a tener algún tipo de efecto adverso material sobre el negocio, la reputación, los resultados operacionales o la situación financiera de la Compañía.

Ecopetrol S.A. continuará monitoreando la evolución de esta situación y, en caso de identificarse hechos o información material que deba ser divulgada al mercado, informará oportunamente de conformidad con la normativa aplicable.

Amenazas y exigencias de extorsión

Uno de los aspectos que más preocupa a la compañía es que, una vez obtenida la información, el responsable del ataque inició contactos para exigir compensaciones económicas a cambio de no divulgar los datos extraídos.

Según detalló Ecopetrol, **«el actor externo comunicó exigencias de extorsión, amenazando con divulgar públicamente la información extraída ilegalmente»**.

La empresa no reveló el monto de las exigencias ni especificó el tipo exacto de información comprometida, pero advirtió que continúa evaluando el alcance real de la filtración.

Las medidas adoptadas por Ecopetrol

Tras detectar el incidente, la petrolera activó sus protocolos de respuesta y puso en marcha un amplio plan de contención para evitar nuevas filtraciones y reducir los riesgos asociados al ataque.

Entre las principales acciones adoptadas se encuentran:

- Revocación inmediata de accesos no autorizados a los activos digitales comprometidos.
- Bloqueo de mecanismos asociados a descargas masivas de información.
- Investigación forense para identificar las tácticas y procedimientos utilizados por los atacantes.
- Monitoreo intensivo de la infraestructura tecnológica.
- Denuncia penal ante la Fiscalía General de la Nación.
- Cooperación con entidades especializadas en ciberseguridad.
- Identificación y bloqueo de infraestructuras externas utilizadas para almacenar la información sustraída.
- Activación de mecanismos de respaldo con aseguradoras y expertos del mercado de capitales.

La empresa informó que estas medidas buscan evitar que la información obtenida ilegalmente sea divulgada y minimizar posibles consecuencias reputacionales y financieras.

No hay afectaciones operativas, pero continúan las investigaciones

Pese a la gravedad del incidente, Ecopetrol aseguró que hasta ahora no se han detectado impactos sobre sus operaciones estratégicas.

En el comunicado, la compañía afirmó que **«a la fecha, Ecopetrol S.A. no ha identificado ninguna interrupción material de sus operaciones críticas, capacidad de producción o servicios esenciales»**.

Asimismo, señaló que tampoco se ha identificado una afectación financiera inmediata ni evidencia de que la información haya sido publicada.

Sin embargo, la empresa reconoció que la investigación sigue en marcha y que todavía se analiza la naturaleza de los datos comprometidos.

Información sensible podría estar involucrada

Uno de los elementos que permanece bajo evaluación es el contenido exacto de los archivos descargados por los atacantes.

Ecopetrol indicó que la información comprometida podría incluir datos corporativos de carácter reservado, documentos confidenciales, información personal e incluso contenido considerado propiedad exclusiva de la organización.

Por ello, la petrolera advirtió que no puede descartar completamente consecuencias futuras derivadas del incidente.

«No es posible asegurar que este incidente no vaya a tener algún tipo de efecto adverso material sobre el negocio, la reputación, los resultados operacionales o la situación financiera de la compañía», señaló la empresa en su reporte.

Fiscalía investiga el caso

La compañía confirmó que ya instauró una denuncia penal ante la Fiscalía General de la Nación, entidad que será la encargada de avanzar en la identificación de los responsables del ataque.

Paralelamente, expertos en seguridad informática realizan labores de análisis forense para determinar la forma en que se produjo la intrusión y establecer si la filtración tiene relación con estructuras criminales especializadas en ciberextorsión.

Una de las mayores alertas de ciberseguridad en la historia reciente de Ecopetrol

El incidente se convierte en uno de los eventos de ciberseguridad más relevantes reportados por la compañía en los últimos años debido al volumen de información comprometida, la cantidad de empresas afectadas y la posterior extorsión denunciada por la organización.

Aunque la petrolera mantiene un parte de tranquilidad sobre la continuidad de sus operaciones, el caso vuelve a poner sobre la mesa los riesgos crecientes que enfrentan las grandes compañías frente a ataques informáticos cada vez más sofisticados.

Mientras avanzan las investigaciones, Ecopetrol aseguró que continuará monitoreando la situación y se comprometió a informar oportunamente cualquier hecho relevante que pueda impactar a inversionistas, accionistas, clientes o al mercado.

CIBERATAQUE | DATOS FILTRADOS | ECOPETROL | EXTORSIÓN | FISCALÍA | GRUPO ECOPETROL | HACKEO ECOPETROL | RANSOMWARE | ROBO DE INFORMACIÓN | SEGURIDAD INFORMÁTICA

ARTÍCULOS RELACIONADOS

A la cárcel seis extranjeros que harían parte de 'Los de la Cañada'

A 36 años de cárcel fue condenado alias «Jei» extranjero señalado de abusar de estudiante en la localidad de Kennedy