

## Ciberataque en Costa Rica

**Por: ELIANA QUIROZ. 12/06/2022**

Costa Rica está bajo ataque cibernético desde el 17 de abril de este año. El ciberataque ha afectado a varios sistemas del Ministerio de Hacienda, del Ministerio de Trabajo, del Instituto Meteorológico y la Caja Costarricense de Seguro Social, entre otros 30 sistemas informáticos de organismos públicos.

El grupo ruso Conti se ha atribuido los ataques y ha pedido inicialmente \$us 10 millones de recompensa para devolver el acceso a la información robada de los sistemas, y ante la negativa del Gobierno de pagar, ha procedido a publicar algo de esa información y ha incrementado a 20 millones la recompensa como forma de presión, y finalmente ha decidido dirigir sus ataques también a empresas privadas.

Estas acciones han causado la interrupción de varios servicios críticos y a que el 8 de mayo el presidente Rodrigo Chaves declare estado de emergencia. Se ha interrumpido el cobro de impuestos, así como el pago de salarios de empleados del sector público, se ha reducido dramáticamente el flujo de importaciones y exportaciones, y la atención de los servicios de salud se ha ralentizado.

En abril, además del ataque a Costa Rica, Conti ha atacado a organismos públicos de Perú y parece ser que otro grupo, LockBit, ha atacado también a organizaciones en Argentina, Chile, México y Brasil.

Si bien los ataques cibernéticos suceden constantemente en el mundo —no hay día que no se registren varios incidentes—, la importancia del actual ciberataque en Costa Rica es su gran magnitud y que está afectando servicios públicos críticos. Expertos han explicado que las posibles razones para elegir a Costa Rica es que tiene un nivel importante de digitalización, pero débiles sistemas de ciberseguridad.

Esta debilidad de ciberseguridad especialmente en sistemas informáticos de gobierno es una característica común a los países latinoamericanos, esa es probablemente la explicación para la expansión de esos ataques a otros países de la región. Por lo que sabemos, en Bolivia no hemos experimentado ciberataques del grupo Conti o de otros similares en las últimas semanas, pero si sucediera es muy probable que estemos igual o menos preparados para resistir que el Gobierno

costarricense.

Este es un resultado de la acelerada digitalización que está experimentando el mundo como resultado de la pandemia. Los Estados tienen que incrementar sus niveles de seguridad. En Bolivia, esta gestión no es transparente, por lo que ignoramos nuestra verdadera situación. En todo caso, necesitamos revisar las políticas de ciberseguridad más allá de hacer test de vulnerabilidades y reportes de ataques, que es con lo que contamos según los reportes del Centro de Gestión de Incidentes Informáticos (CGII).

*Eliana Quiroz es ciberactivista y burócrata.*

[LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ](#)

Fotografía: La razón

**Fecha de creación**

2022/06/12