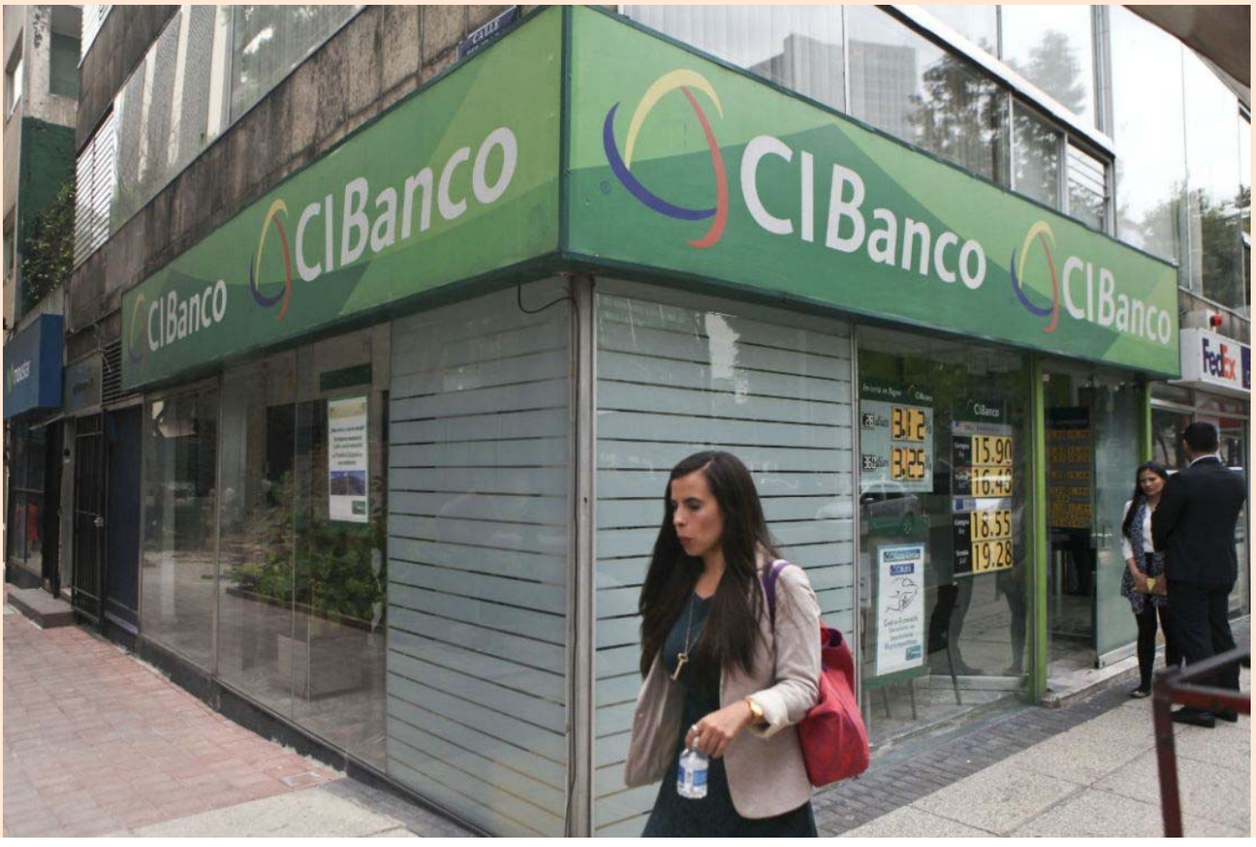
EL ECONOMISTA 30 ANIVERSARIO

CI Banco reactiva ciertos servicios tras intento de ciberataque

CI Banco informó este jueves que, tras haber restringido sus operaciones bancarias por un virus detectado en sus equipos en días pasados, ha reactivado ya ciertos canales.

Edgar Juárez14 de febrero de 2019, 16:52



CI Banco informó este jueves que, tras haber restringido sus operaciones bancarias por un virus detectado en sus equipos en días pasados, ha reactivado ya ciertos canales.

En sus redes sociales detalló a sus clientes que su Servicio de Pagos Electrónicos Interbancarios (SPEI), así como su banca electrónica y sus cajeros automáticos, se encuentran ya activos desde la mañana del jueves.

Asimismo, refirió que su personal seguía trabajando para restablecer, lo antes posible, el resto de sus servicios bancarios.

De igual forma, el llamado banco verde informó que su call center puso a su disposición los números temporales 5140 69 00, extensiones 4907 y 4904, ello para robo, extravío, tarjeta de débito, cheques, chequeras, y tarjetas; mientras que para temas relacionados con Finanmadrid, el número 5140 69 00, extensión 4903.

La noche del martes, CI Banco informó que procedió a restringir sus operaciones bancarias como protocolo de seguridad para proteger su sistema informático de un virus.

En ese momento, precisó que dicha acción no afectó el patrimonio ni información de sus clientes, ni del propio banco, tal y como lo informó a las autoridades financieras.

La Comisión Nacional Bancaria y de Valores (**CNBV**) confirmó por su parte la noche de ese mismo martes en su sitio de Internet, que "una institución financiera", detectó un virus informático del tipo Ransomware que actuó sobre equipos basados en plataforma Windows, pero subrayó que el incidente fue contenido de forma oportuna y efectiva por la institución, y que sólo algunos equipos de cómputo personal se vieron afectados.

"De acuerdo con la información que la institución proporcionó a las autoridades, no estuvieron en riesgo sus recursos ni la información ni recursos de sus clientes. El Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información (GRI), activo oportunamente los protocolos correspondientes", refirió la dependencia.