# *Nota Técnica de PwC*

**El día 27 de agosto de 2018, la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN) envió la circular SIB-DSB-14539, sobre la "Protección integral de los clientes, usuarios y usuarias del sistema bancario nacional que realizan operaciones mediante la banca a distancia o banca por Internet fuera de la República Bolivariana de Venezuela".**

Al respecto, la SUDEBAN instruye a las instituciones bancarias, entre otras cosas, a efectuar bloqueos preventivos sobre los accesos para realizar transferencias en línea a las personas que no hayan notificado a la institución bancaria sobre los viajes que tengan previsto a realizar al exterior del país. Dichos bloqueos deberán ser realizados a las personas que se autentiquen en el sistema de banca por Internet desde una dirección IP (Internet Protocol) fuera del país.

Es importante señalar que las direcciones IP son números de identificación que utilizan los dispositivos conectados a Internet para establecer comunicación con la red de redes. Dichas direcciones son administradas a nivel internacional por la Autoridad de asignación de números de Internet (IANA, por sus siglas en inglés), quien asigna bloques de direcciones a las entidades regionales, quienes a su vez los asignan a los países y proveedores locales.

Es por esta razón que técnicamente resulta muy fácil determinar a qué país pertenece una dirección IP en particular, aunque no en todos los casos el uso de una dirección IP sea evidencia inequívoca que la persona se encuentre allí.


En la actualidad, el uso de tecnologías como las Redes Privadas Virtuales (VPN, por sus siglas en inglés), servidores proxy y túneles de comunicación son utilizados con mucha frecuencia tanto por organizaciones y particulares dada las ventajas, tanto operativas como de seguridad, que brinda el poder consolidar la gestión del uso de Internet. Así entonces como algunas empresas con sedes en diferentes ciudades o países consolidan el tráfico de datos hacia Internet en un solo lugar, con el fin de poder implementar soluciones integrales de protección a sus usuarios.

En este sentido, la implementación de los controles descritos en la referida circular puede generar una afectación directa sobre personas y organizaciones que, estando en Venezuela, vean restringido el acceso a los sistemas bancarios debido a la detección incorrecta de su localidad.

Por otra parte, es posible que las personas al verse en la necesidad de movilizar sus instrumentos financieros y no querer informar a las instituciones financieras su actual ubicación, recurran a tecnologías similares a las descritas, para establecer canales de comunicación con Venezuela, con el fin de poder realizar sus operaciones como si se encontraran dentro del país, y eventualmente se ofrecerán este tipo de servicios. Un servidor proxy o VPN mal configurado, o configurado intencionalmente como herramienta de ataque, podría ser utilizado para interceptar los datos de identificación de los usuarios o capturar información financiera de aquellas personas que lo utilicen. Este tipo de ataques, no requiere de capacidades técnicas sofisticadas y tiene un mercado potencialmente importante.

Grandes empresas como Google ya habían utilizado controles de geolocalización basado en direccionamiento IP para restringir o permitir el acceso a servicios destinados a regiones particulares en el mundo, y se vieron en la necesidad de replantear sus controles al percatarse que eventualmente los usuarios presentaban problemas operativos y en la práctica no se lograba el objetivo.

En conclusión, el uso de la geolocalización a través del uso de direcciones IP para controlar el acceso a la banca por Internet trae consigo los siguientes inconvenientes:

- La ubicación geográfica obtenida a partir de una dirección IP no es garantía de que la persona se encuentre en ese país o región.
- Las personas o empresas que utilicen tecnologías como VPN o Proxies para utilizar puntos de salida a Internet fuera de Venezuela serían afectadas
- Una persona con ciertos conocimientos técnicos es capaz de saltarse estos controles mediante el uso de herramientas de dominio público. En este sentido el crimen organizado ha demostrado en el pasado ser técnicamente competente e innovador en el uso de técnica para la evasión de controles como éste, por lo que su eficacia sería muy limitada
- Existe la posibilidad de que proliferen aplicaciones maliciosas que prometan servir de herramienta a las personas que se encuentren fuera del país, pero cuyo objetivo real sea obtener de manera fraudulenta la información personal y financiera de los usuarios

**Contáctenos**

**Roberto Sánchez V.**
roberto.sanchez@ve.pwc.com
@robersv
**Edwin Orrico**
edwin.orrico@ve.pwc.com
@3dorr