# Alerta de Seguridad Informática (8FPH-00041-001)

## Nivel de Riesgo: Alto

## Tipo: Phishing

Fecha de lanzamiento original: 05 de Julio de 2019 | Última revisión 05 de Julio de 2019

### Notificación

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

### Resumen

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Estado. El correo trata de persuadir a los clientes del Banco indicándoles que por motivos de seguridad han bloqueado la clave de acceso a la banca en línea y ofrece la posibilidad de verificar su cuenta ingresando al link indicado en el correo. Al seleccionar el enlace redirigen a la víctima a un sitio semejante al de Banco Estado, tratando de convencer a las personas para que ingresen sus credenciales de acceso y así obtener sus datos.

> “Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño”

**Observación**

Solicitamos tener en consideración las señales de compromiso en su conjunto

**Indicadores de compromisos**

**Url's:**

- http[:]//jeevansamruddhi[.]org/wp-includes/Activacion[.]php
- http[:]//implemenit[.]com/wp-includes/Activacion[.]php
- http://tonk.blisto.com/include/Activacion[.]php
- http://projectbox.com/tos/Activacion[.]php
- http[:]//www.bricktechindia[.]in/fonts/www.bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

**Smtp Host**

110-170-232-163.static.asianet.co[.]th [110.170.232.163]

list.silmedia[.]es [212.48.78.100]

server.bizimagewebdesign.co[.]uk [109.228.50.94]

host63-92-88-80.serverdedicati.aruba[.]it [80.88.92.63]

dns2.podernet.com[.]mx [200.36.1.250]

**Sender**

www-data@hosting2.bsru.ac[.]th
fincaelsitiodeja@vl21793.dns-privadas[.]es
pgi@pgi-insurance.co[.]uk
apache@enterprise1.connectisweb[.]net
webmaster@podernet.com[.]mx

**From (Asunto falsificado para engañar a las personas):**

BancoEstado noreply@bancoestado.cl

**Subject:**

Fw:Su Cuenta esta Bloqueada.
Fw:Cuenta Bloqueada.

## Imagen Phishing correo

BancoEstado <noreply@bancoestado.cl>

Fw:Su Cuenta esta Bloqueada.


**Cuenta Bloqueada**

**Estimado(a):**

**Banco de Estado,**le comunica que se realizo un mantenimiento en nuestro Servicio(Caja Vecina,ServiEstado).Encontramos error en su cuenta.

Su cuenta no se encuentra registrada correctamente,nos vemos en la obligacion de **Bloquearla Temproralmente.**

Puede Restablecer su cuenta haciendo click en el enlace, con esta accion su cuenta quedara restaurada de forma permanente. solo podra hacerlo por medio de este e-mail.

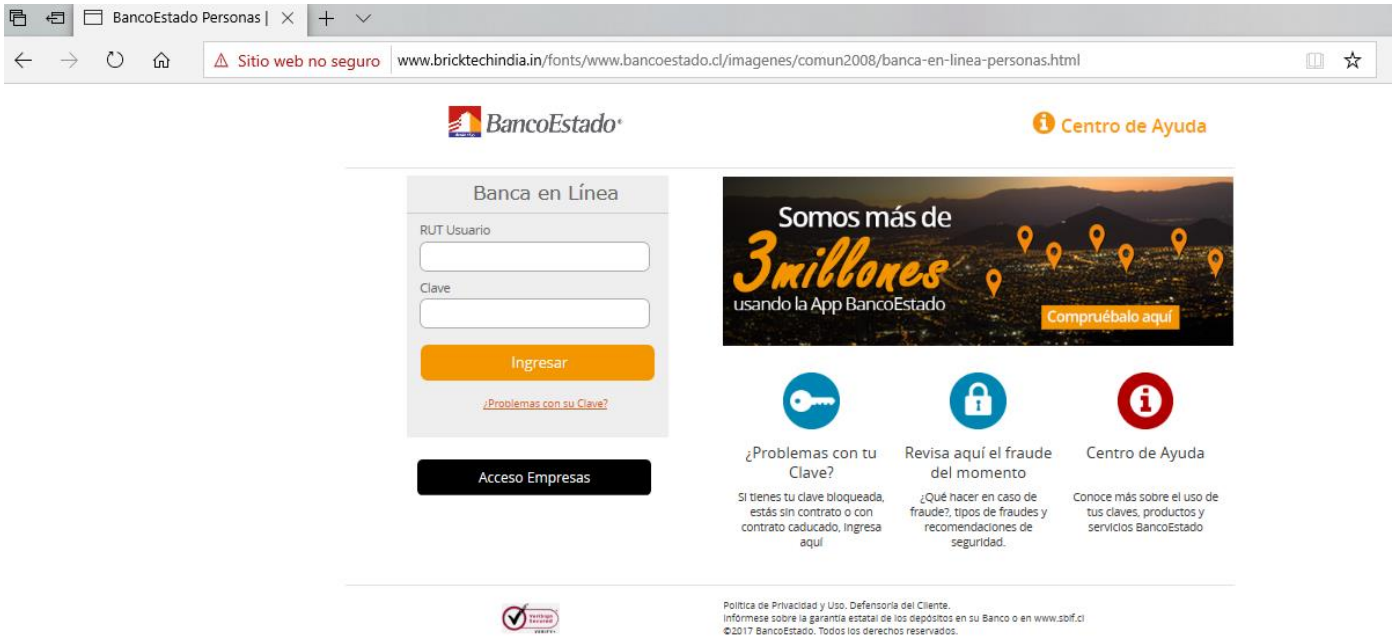
https://www.bancoestado.cl/Seguridad/Activacion_Cuenta


Te invitamos a revisar las distintas opciones de **Ahorro e Inversiï¿½n** que tenemos para ti, desde tu **Banca en Lï¿½nea.**

www.bancoestado.cl

600 400 7000 • bancoestado.cl

## Imagen Sitio Phishing



## Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas
- Visualizar los sitios web que se ingresen que sean los oficiales

## Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob