

Alerta de seguridad informática	8FPH20-00103-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Enero de 2020
Última revisión	31 de Enero de 2020

## 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 afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC 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 loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

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.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Estado.

El mensaje informa a la víctima sobre la suspensión de la cuenta producto de un registro incorrecto de la cuenta. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que es necesario que ingrese para reactivar la cuenta o de lo contrario se procederá al bloqueo de los servicios por internet. Al seleccionar el vínculo la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales.

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

## Indicadores de compromisos

### Url's

[http://naveg0\[.\]site/Activacion/cuenta-izfc/](http://naveg0[.]site/Activacion/cuenta-izfc/)

[http://redvipervdc\[.\]com/cream/imagenes/comun2008/banca-en-linea-personas\[.\]html](http://redvipervdc[.]com/cream/imagenes/comun2008/banca-en-linea-personas[.]html)

### Sender

apache@despacho[.]io

### Smtip Host

[45.7.231.174]

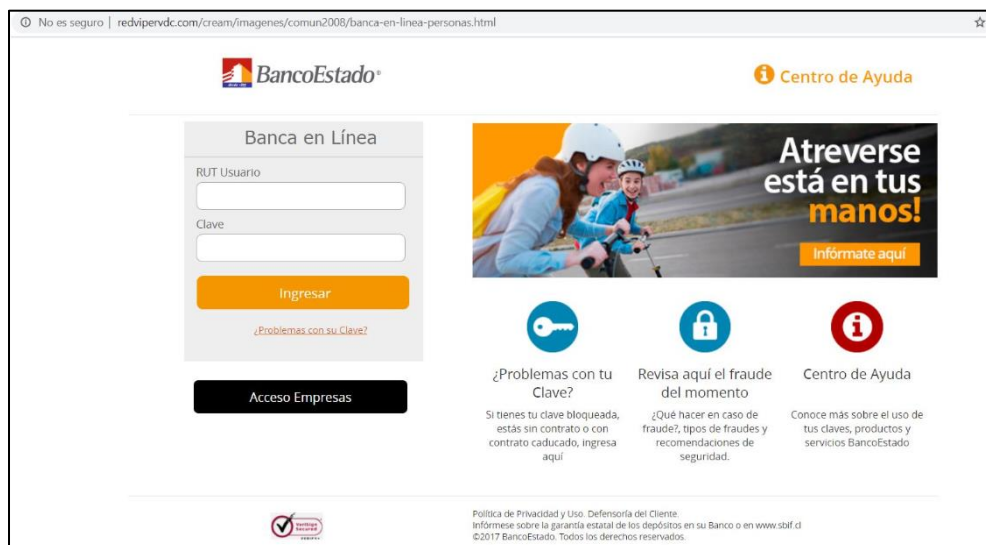
### Subject

Fw: Cuenta Deshabilitada

## Imagen del correo



## Imagen Sitio Web



## Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y 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