

Alerta de seguridad informática	8FFR-00064-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Septiembre de 2019
Última revisión	17 de Septiembre de 2019

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones propias 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 fraude 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 fraude, 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 la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de **Banco Estado**, el que podría servir para robar credenciales de usuarios de esa entidad..

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

## Indicadores de Compromisos

### URL's

http[://]www[.]anexpromet[.]com[.]ba/cp/comun2008/

Al ingresar a las URL, esta se redirigen a la siguiente url:

https[://]terrium[.]cl/css/date/imagenes/comun2008/banca-en-linea-personas[.]html

https[://]fuyueiieiiisiasd[.]000webhostapp[.]com/comun2008/index[.]html.html

### IP's

195[.]222[.]33[.]178

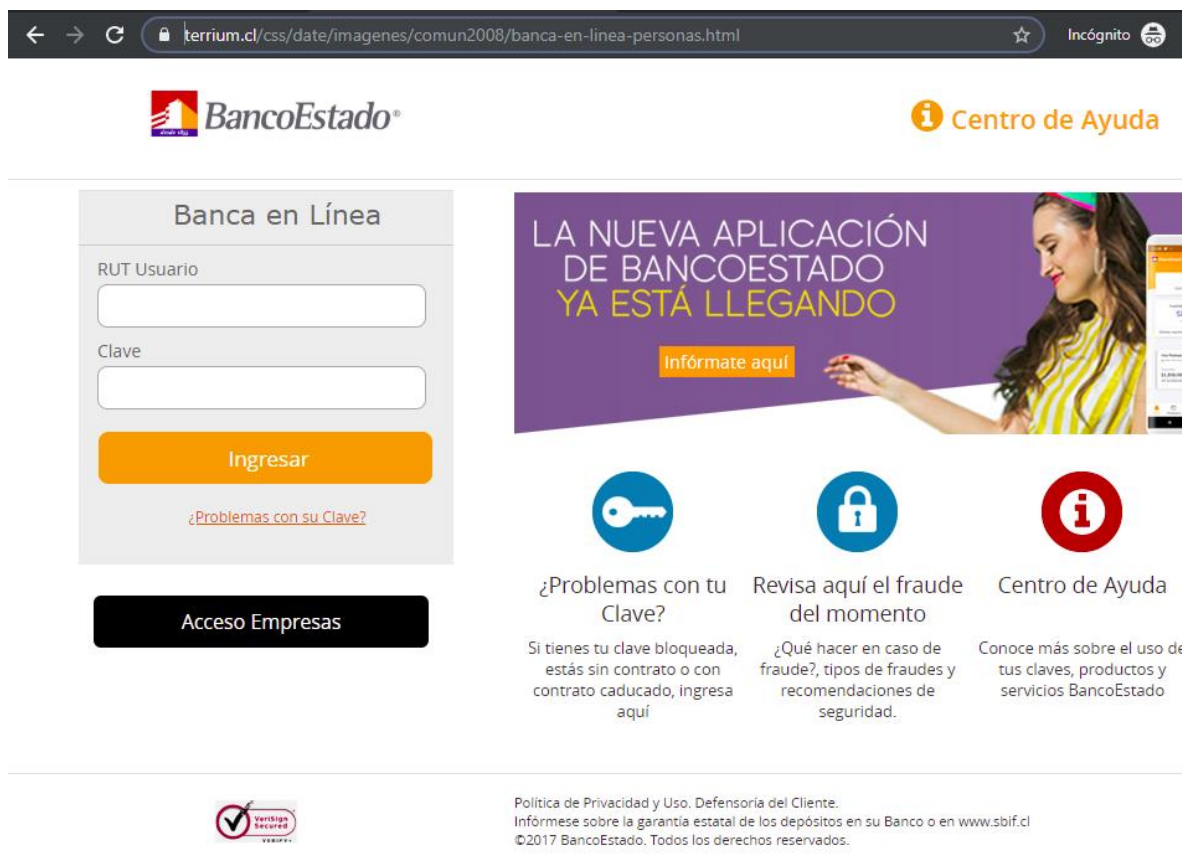
145[.]14[.]144[.]140

### Localización

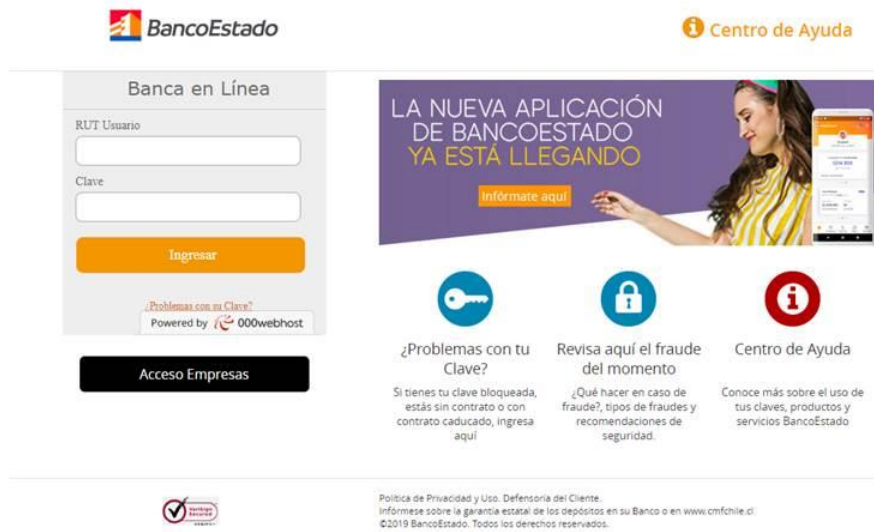
Sarajevo, Federacija, Bosnia and Herzegovina

Charlotte, North Carolina, Estados Unidos

## Ejemplo de Imagen del sitio



The screenshot shows a web browser window with the URL `terrium.cl/css/date/imagenes/comun2008/banca-en-linea-personas.html`. The page features the BancoEstado logo and a 'Centro de Ayuda' link. On the left, there is a login form titled 'Banca en Línea' with fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below the form is a button for 'Acceso Empresas'. On the right, a purple banner promotes a new app: 'LA NUEVA APLICACIÓN DE BANCOESTADO YA ESTÁ LLEGANDO' with a '¡Infórmate aquí!' button. Below the banner are three icons: a key for '¿Problemas con tu Clave?', a padlock for 'Revisa aquí el fraude del momento', and an information icon for 'Centro de Ayuda'. Each icon has a corresponding text block explaining the service. At the bottom, there is a 'Verifica Seguro' logo and a footer with privacy policy information: 'Política de Privacidad y Uso. Defensoría del Cliente. Infórmese sobre la garantía estatal de los depósitos en su Banco o en [www.sbif.cl](http://www.sbif.cl) ©2017 BancoEstado. Todos los derechos reservados.'



The screenshot shows the BancoEstado website interface. At the top left is the BancoEstado logo. To the right is a 'Centro de Ayuda' (Help Center) link. The main content area is divided into two sections. On the left is the 'Banca en Línea' (Online Banking) login form, which includes fields for 'RUT Usuario' and 'Clave' (password), an 'Ingresar' (Login) button, and a link for 'Problemas con tu Clave?'. Below the login form is an 'Acceso Empresas' (Business Access) button. On the right is a promotional banner for the new mobile application, 'LA NUEVA APLICACIÓN DE BANCOESTADO YA ESTÁ LLEGANDO', with an 'informate aquí' (learn more here) button. Below the banner are three circular icons with corresponding text: a key icon for '¿Problemas con tu Clave?', a padlock icon for 'Revisa aquí el fraude del momento', and an information icon for 'Centro de Ayuda'. Each icon has a short paragraph of text below it. At the bottom of the page, there is a small logo on the left and a 'Política de Privacidad y Uso. Defensoría del Cliente.' link on the right, along with a copyright notice for 2019 BancoEstado.

## Whois

```
soc@kali:~$ whois -h whois.nic.cl terrium.cl
%%
%% This is the NIC Chile Whois server (whois.nic.cl).
%%
%% Rights restricted by copyright.
%% See https://www.nic.cl/normativa/politica-publicacion-de-datos-cl.pdf
%%

Domain name: terrium.cl
Registrant name: COMERCIAL EPULLEN LIMITADA
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 2010-03-02 15:02:43 CLST
Expiration date: 2023-04-01 12:02:04 CLST
Name server: ns1.terrium.cl (108.179.227.230)
Name server: ns2.terrium.cl (108.179.227.229)
```

```
Domain Name: 000WEBHOSTTAPP.COM
Registry Domain ID: 2101612842_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-05-05T02:21:54Z
Creation Date: 2017-03-01T22:31:53Z
Registrar Registration Expiration Date: 2020-03-01T22:31:53Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Domain Admin
Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
Registrant Street: 10 Corporate Drive
Registrant City: Burlington
Registrant State/Province: MA
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.8022274003
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact@privacyprotect.org
Registry Admin ID: Not Available From Registry
Admin Name: Domain Admin
Admin Organization: Privacy Protect, LLC (PrivacyProtect.org)
Admin Street: 10 Corporate Drive
Admin City: Burlington
Admin State/Province: MA
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.8022274003
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: contact@privacyprotect.org
Registry Tech ID: Not Available From Registry
Tech Name: Domain Admin
Tech Organization: Privacy Protect, LLC (PrivacyProtect.org)
Tech Street: 10 Corporate Drive
Tech City: Burlington
Tech State/Province: MA
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.8022274003
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: contact@privacyprotect.org
Name Server: ns1.mytrafficmanagement.com
Name Server: ns2.mytrafficmanagement.com
DNSSEC: Unsigned
```

## Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido, hacia la URL maliciosa
- 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