

Alerta de seguridad informática	8FFR-00074-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2019
Última revisión	30 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[[:]//]bncoestado[.]xyz/imagenes/comun2009/en-linea-personas[.]php

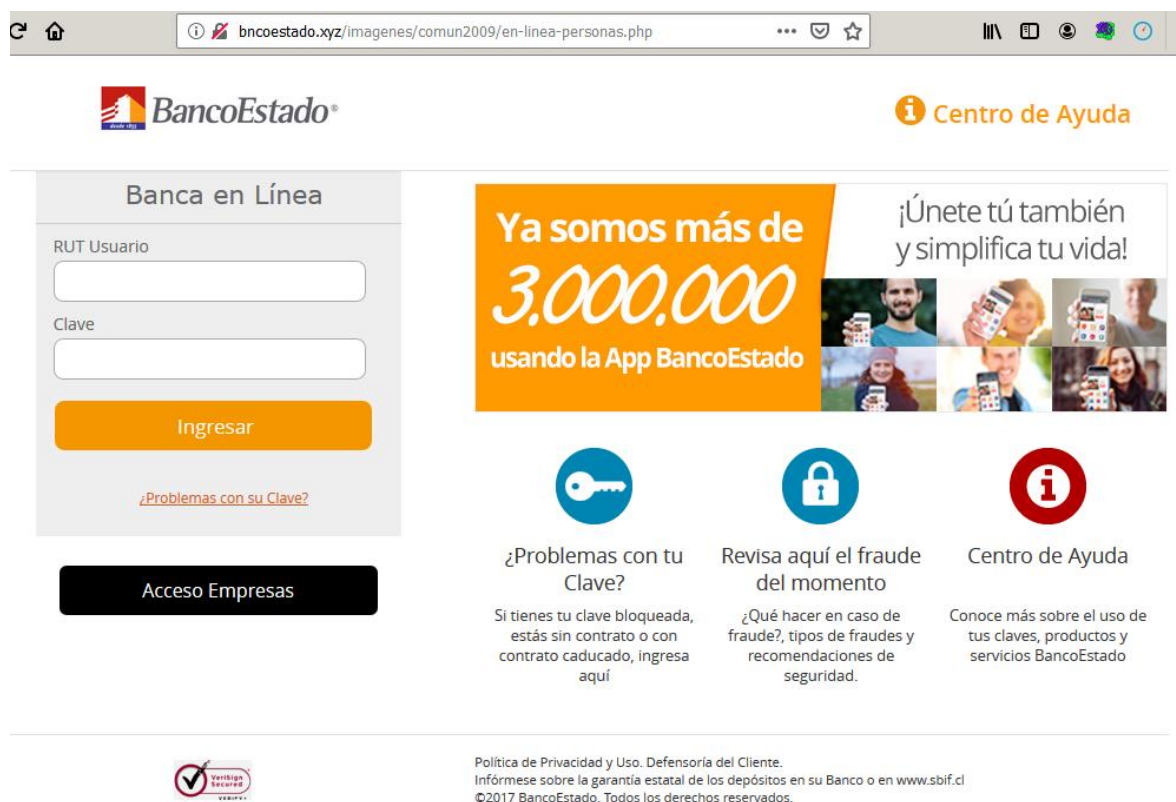
### IP's

167[.]71[.]224[.]121

### Localización

York City, New York, Estados Unidos

### Imagen del sitio



The screenshot shows the BancoEstado website. At the top left is the BancoEstado logo. To the right is a 'Centro de Ayuda' link. The main content area is divided into two sections. On the left is the 'Banca en Línea' login form, which includes fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below the login form is a black button for 'Acceso Empresas'. On the right is a promotional banner for the mobile app. The banner features the text 'Ya somos más de 3.000.000 usando la App BancoEstado' and '¡Únete tú también y simplifica tu vida!'. Below the banner are three circular icons: a key, a padlock, and an information icon. Each icon has a corresponding text block: '¿Problemas con tu Clave?' (with a subtext about blocked keys), 'Revisa aquí el fraude del momento' (with a subtext about fraud types), and 'Centro de Ayuda' (with a subtext about app usage). At the bottom of the page, there is a 'Verifica Seguridad' logo and a footer containing the 'Política de Privacidad y Uso' link, a contact number, and copyright information for BancoEstado.

## Whois

```
Domain Name: bncoestado.xyz
Registry Domain ID: D131540766-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-09-28T07:00:00Z
Creation Date: 2019-09-27T07:00:00Z
Registrar Registration Expiration Date: 2020-09-27T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-50813ff3dc3d269b8f79f7a4b4f6fc42@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-50813ff3dc3d269b8f79f7a4b4f6fc42@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-50813ff3dc3d269b8f79f7a4b4f6fc42@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-09-30T07:00:00Z <<<
```

## 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