

Alerta de seguridad cibernética	8FFR20-00437-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Mayo de 2020
Última revisión	30 de Mayo 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 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 portale 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 compromiso

URL

bancestado-actualizaciondeinformacion[.].ml

IP

178[.]159[.]36[.]211


## Dominios donde se aloja url

Domain bancestado-actualizaciondeinformacion.ml																	
bancestado-actualizaciondeinformacion / ml / Subdomains																	
record type	TTL	value															
A	300	<a href="#">178.159.36.211</a>															
NS	300	<a href="#">ns02.freenom.com</a>	<a href="#">Zones on DNS server</a> 52.19.156.76														
NS	300	<a href="#">ns04.freenom.com</a>	<a href="#">Zones on DNS server</a> 104.155.29.241														
NS	300	<a href="#">ns03.freenom.com</a>	<a href="#">Zones on DNS server</a> 104.155.27.112														
NS	300	<a href="#">ns01.freenom.com</a>	<a href="#">Zones on DNS server</a> 54.171.131.39														
SOA	300	<table border="1"> <tr> <td>Mname</td> <td>ns01.freenom.com</td> </tr> <tr> <td>Rname</td> <td>soa.freenom.com</td> </tr> <tr> <td>Serial number</td> <td>1590709182</td> </tr> <tr> <td>Refresh</td> <td>10800</td> </tr> <tr> <td>Retry</td> <td>3600</td> </tr> <tr> <td>Expire</td> <td>604800</td> </tr> <tr> <td>Minimum TTL</td> <td>3600</td> </tr> </table>		Mname	ns01.freenom.com	Rname	soa.freenom.com	Serial number	1590709182	Refresh	10800	Retry	3600	Expire	604800	Minimum TTL	3600
Mname	ns01.freenom.com																
Rname	soa.freenom.com																
Serial number	1590709182																
Refresh	10800																
Retry	3600																
Expire	604800																
Minimum TTL	3600																

## Certificados


<b>Subject DN</b>	CN=www.bancestado-actualizaciondeinformacion.ml
<b>Issuer DN</b>	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
<b>Serial</b>	Decimal: 271248125665247465589733784120879271444159 Hex: 0x31d2068c1fca359f7c4a6cfcb380e64febf
<b>Validity</b>	2020-05-28 23:52:07 to 2020-08-26 23:52:07 (90 days, 0:00:00)
<b>Names</b>	<a href="#">bancestado-actualizaciondeinformacion.ml</a> <a href="#">www.bancestado-actualizaciondeinformacion.ml</a>

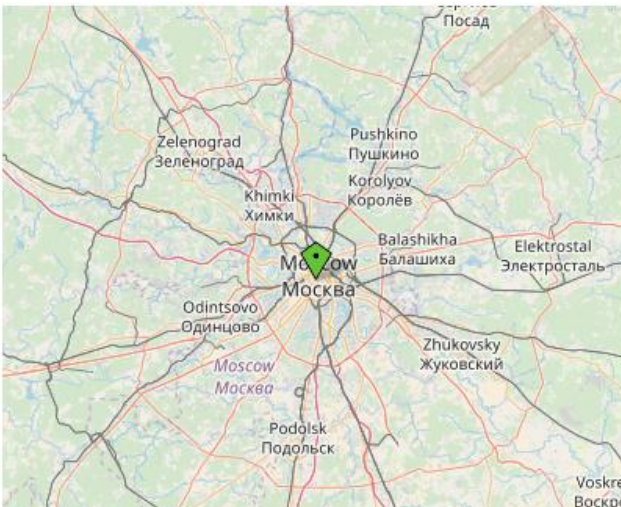
## Ip de origen donde se aloja sitio

<b>Domain <u>bancestado-actualizaciondeinformacion.ml</u> is located on IP address &lt;&lt; 178.159.36.211 &gt;&gt;</b>	
<b>Block start</b>	178.159.36.0
<b>End of block</b>	178.159.36.255
<b>Block size</b>	256  Domains in block
<b>Block name</b>	PrivateInternetHosting
<b>AS number</b>	<u>35196</u>
<b>Parent block</b>	<u>178.0.0.0 - 178.255.255.255</u>
<b>Organization</b>	ORG-PIHL2-RIPE

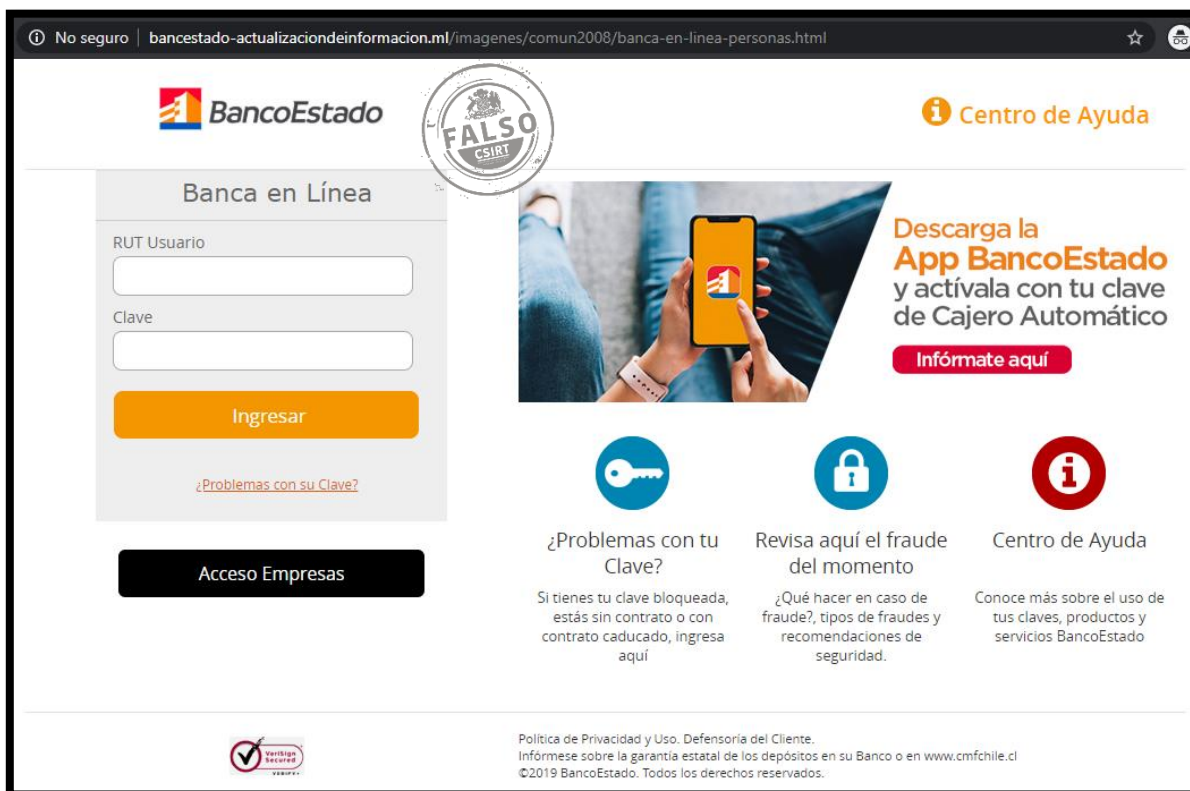
## Localización

Moscú, Federación Rusa

<b>Location</b>	Russia (RU) 
<b>Latitude and Longitude</b>	55.74, 37.61



## Imagen del sitio



🔒 No seguro | [bancestado-actualizaciondeinformacion.ml/imagenes/comun2008/banca-en-linea-personas.html](https://bancestado-actualizaciondeinformacion.ml/imagenes/comun2008/banca-en-linea-personas.html) ☆

**BancoEstado** **FALSO CSIRT** **Centro de Ayuda**

### Banca en Línea

RUT Usuario

Clave


**Ingresar**

[¿Problemas con su Clave?](#)

**Acceso Empresas**

**Descarga la App BancoEstado y actívala con tu clave de Cajero Automático**  
**Infórmate aquí**

- ¿Problemas con tu Clave?**  
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
- Revisa aquí el fraude del momento**  
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
- Centro de Ayuda**  
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado

 Política de Privacidad y Uso. Defensoría del Cliente.  
Infórmese sobre la garantía estatal de los depósitos en su Banco o en [www.cmfchile.cl](http://www.cmfchile.cl)  
©2019 BancoEstado. Todos los derechos reservados.

## Whois

```
Domain name:
BANCESTADO-ACTUALIZACIONDEINFORMACION.ML

Organisation:
Mali Dili B.V.
Point ML administrator
P.O. Box 11774
1001 GT Amsterdam
Netherlands
Phone: +31 20 5315725
Fax: +31 20 5315721
E-mail: abuse: abuse@freenom.com, copyright infringement: copyright@freenom.com

Domain Nameservers:
NS01.FREENOM.COM
NS02.FREENOM.COM
NS03.FREENOM.COM
NS04.FREENOM.COM

Your selected domain name is a Free Domain. That means that,
according to the terms and conditions of Free Domain domain names
the registrant is Mali Dili B.V.

Due to restrictions in Point ML 's Privacy Statement personal information
about the user of the domain name cannot be released.

ABUSE OF A DOMAIN NAME
If you want to report abuse of this domain name, please send a
detailed email with your complaint to abuse@freenom.com.
In most cases Point ML responds to abuse complaints within one business day.

COPYRIGHT INFRINGEMENT
If you want to report a case of copyright infringement, please send
an email to copyright@freenom.com, and include the full name and address of
your organization. Within 5 business days copyright infringement notices
will be investigated.

Record maintained by: Point ML Domain Registry
```

## 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.