

Alerta de seguridad informática	8FFR20-00287-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Marzo de 2020
Última revisión	26 de Marzo 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 afecta 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 detectado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de **Banco BCI**, 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

bci-seguridad[.]cl

IP

162[.]241[.]61[.]53

## DOMINIOS DONDE SE ALOJA URL

Domain bci-seguridad.cl 			
bci-seguridad / cl /  Subdomains			
record type	TTL	value	
A	14400	<a href="https://www.whois.com/whois/162.241.61.53">162.241.61.53</a>	
NS	86400	<a href="https://www.whois.com/whois/nspro12.hostgator.cl">nspro12.hostgator.cl</a>	 Zones on DNS server <a href="https://www.whois.com/whois/162.241.61.51">162.241.61.51</a>
NS	86400	<a href="https://www.whois.com/whois/nspro13.hostgator.cl">nspro13.hostgator.cl</a>	 Zones on DNS server <a href="https://www.whois.com/whois/162.241.61.52">162.241.61.52</a>
MX	14400	0 mail.bci-seguridad.cl	
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all	
SOA	86400	Mname	nspro12.hostgator.cl
		Rname	root.sh-pro12.hostgator.cl
		Serial number	2020032604
		Refresh	86400
		Retry	7200
		Expire	3600000
		Minimum TTL	86400

## CERTIFICADOS

### ✓ Certificate Name matches bci-seguridad.cl



Subject bci-seguridad.cl

Valid from 26/Mar/2020 to 26/Mar/2021

Issuer Sectigo RSA Domain Validation Secure Server CA



Subject Sectigo RSA Domain Validation Secure Server CA


Valid from 02/Nov/2018 to 31/Dec/2030

Issuer USERTrust RSA Certification Authority

### ✓ TLS Certificate

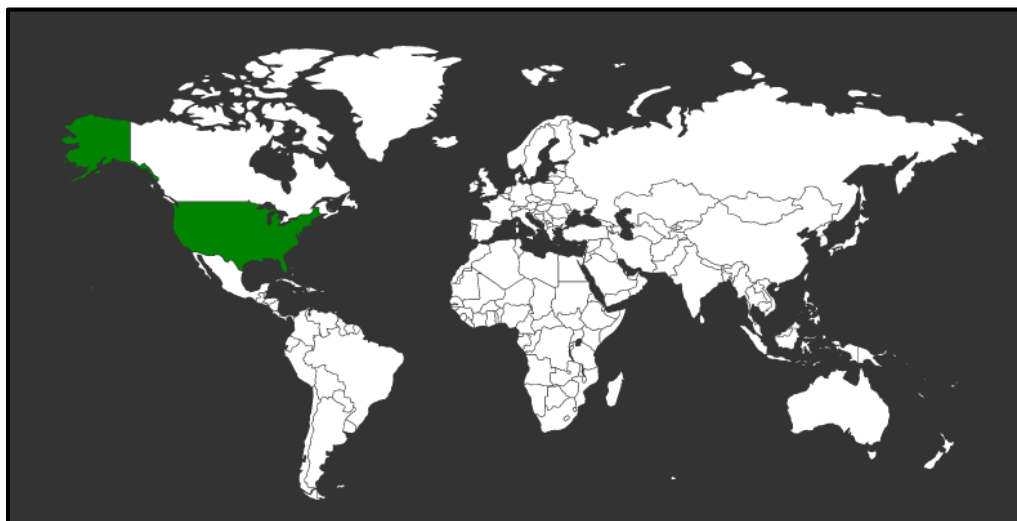
```
Common Name = bci-seguridad.cl
Subject Alternative Names = bci-seguridad.cl, www.bci-seguridad.cl
Issuer = Sectigo RSA Domain Validation Secure Server CA
Serial Number = F75D4ABEFAD210C2180867F75D767465
SHA1 Thumbprint = 89DE9DB3A7F4B2F919705435BAFE545BBDE70BC9
Key Length = 2048
Signature algorithm = SHA256-RSA
Secure Renegotiation:
```

## IP DE ORIGEN DONDE SE ALOJA SITIO

<b>Domain <u>bci-seguridad.cl</u> is located on IP address &lt;&lt; 162.241.61.53 &gt;&gt;</b>	
<b>Block start</b>	162.240.0.0
<b>End of block</b>	162.241.255.255
<b>Block size</b>	131072  Domains in block
<b>Block name</b>	UNIFIEDLAYER-NETWORK-16
<b>AS number</b>	46606
<b>Parent block</b>	162.0.0.0 - 162.255.255.255
<b>Organization</b>	UnifiedLayer

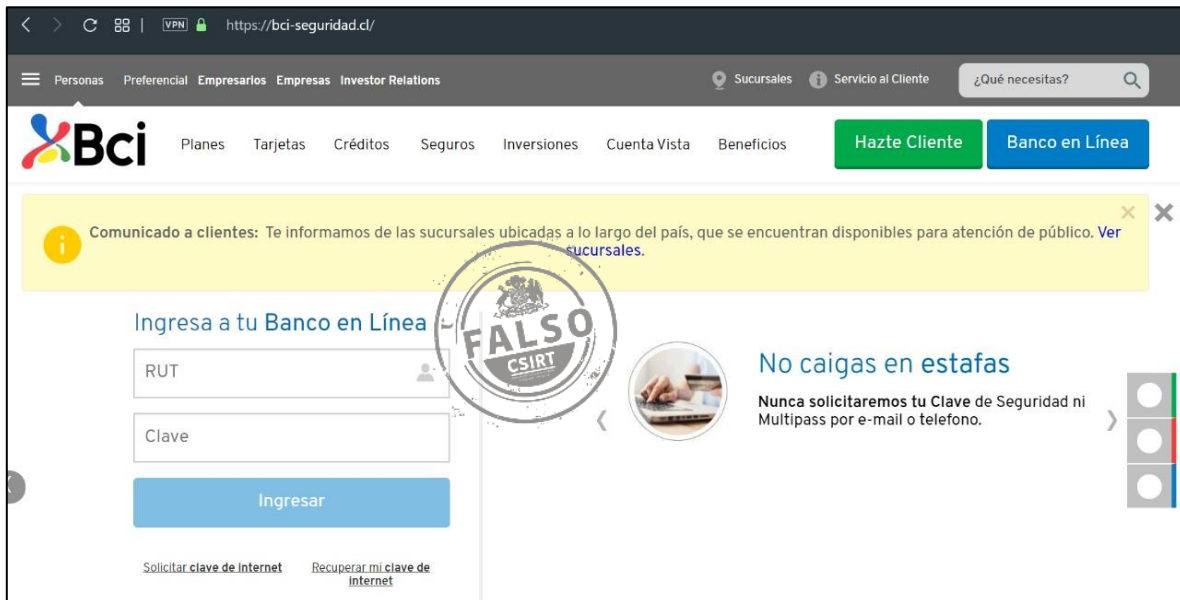
## LOCALIZACIÓN

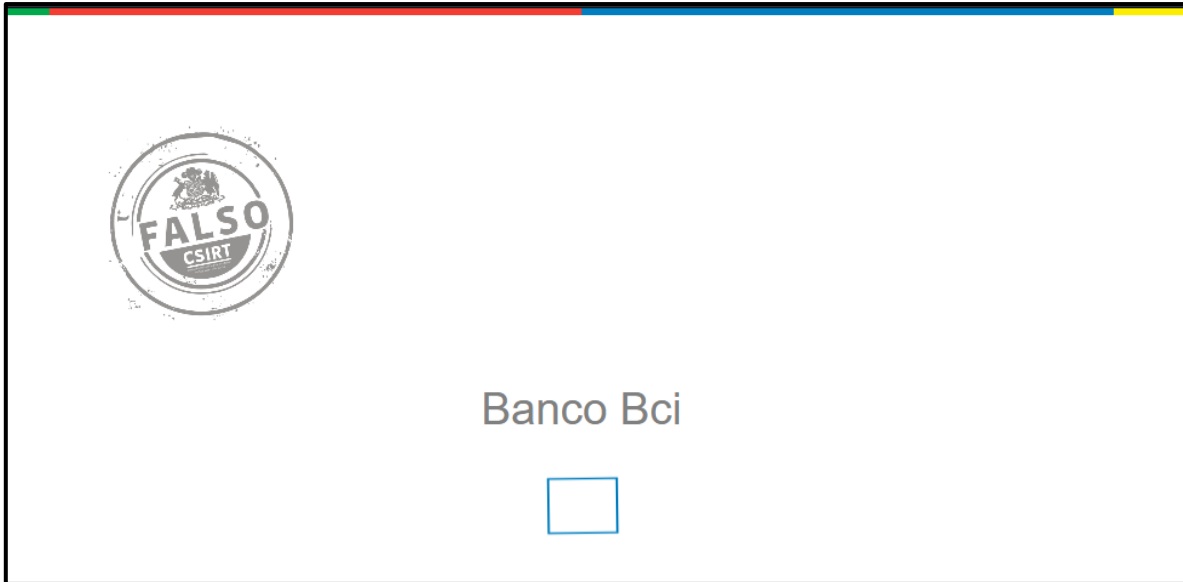
Provo, Utah, USA





## IMAGEN DEL SITIO





**Multipass - Bcypass**

RUT  
96.███-5

Fecha:  
Jueves, 26 de Marzo de 2020,  
16:22

**ERROR** Por favor espere que su Multipass renueve la clave del visor para poder ingresar, de este modo evitara problemas por uso de clave Multipass repetida.

Clave Multipass:

Ingrese el **numero de 6 digitos** que aparece en el **visor de su Bci Multipass**.

Esta clave le entrega una doble seguridad.  
La Clave Multipass es una segunda clave de seguridad que le permite realizar: Transferencias de Fondos hasta por \$5.000.000 diarios, Pago de Cuentas, Recarga de Celular, Recarga Tarjeta Bip! y adquirir Tarjeta Virtual.

Si tiene dudas o comentarios, desde Chile llame al **600 824 2424**, desde el Extranjero llame al **562 692 8000**

## WHOIS

```
Domain name: bci-seguridad.cl  
Registrant name: manuel oses  
Registrant organisation: N/A  
Registrar name: PDR Ltd. d/b/a PublicDomainRegistry.com  
Registrar URL: https://www.publicdomainregistry.com  
Creation date: 2020-03-26 12:09:40 CLST  
Expiration date: 2021-03-26 12:09:40 CLST  
Name server: nspro12.hostgator.cl  
Name server: nspro13.hostgator.cl
```

## 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.