Alerta de seguridad informática	8FFR20-00269-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Marzo de 2020
Última revisión	18 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 IoC 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 IoC 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

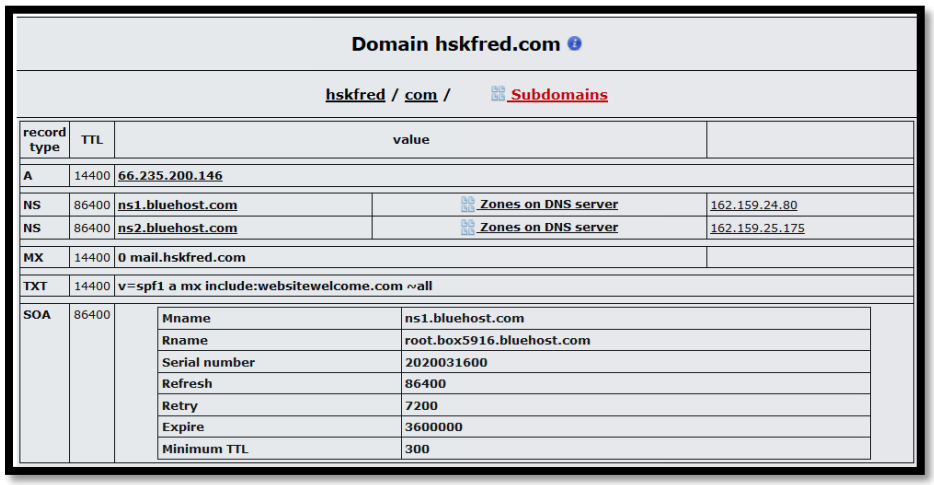
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de cuatro portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial del **Banco Estado**, el que podría servir para robar credenciales de usuarios de esa entidad.

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

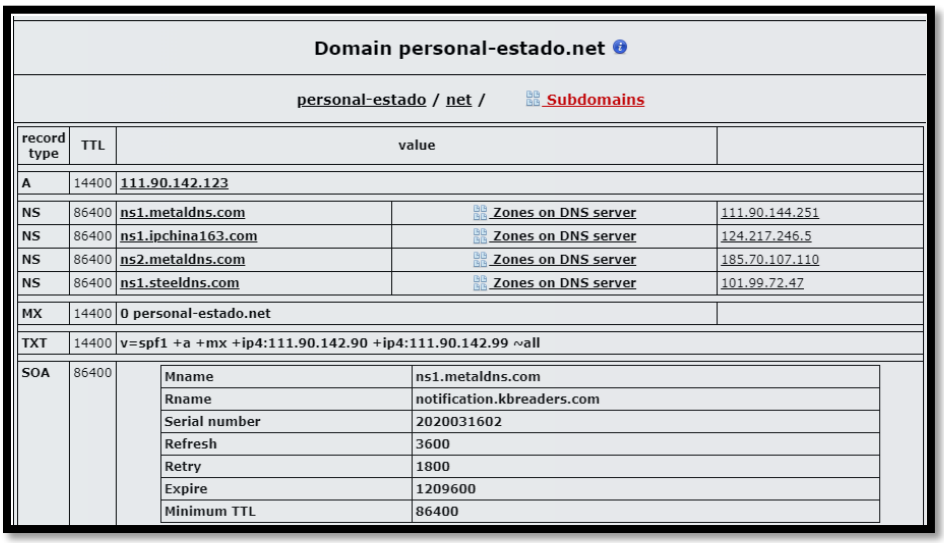
bencoestadooenlinea[.]hskfred[.]com
personal-estado[.]net
estadonuevocl[.]com
www[.]estadonuevocl[.]com
www[.]estadonuevocl[.]com/site/control[.]php



Domain hskfred.com

hskfred / com / Subdomains

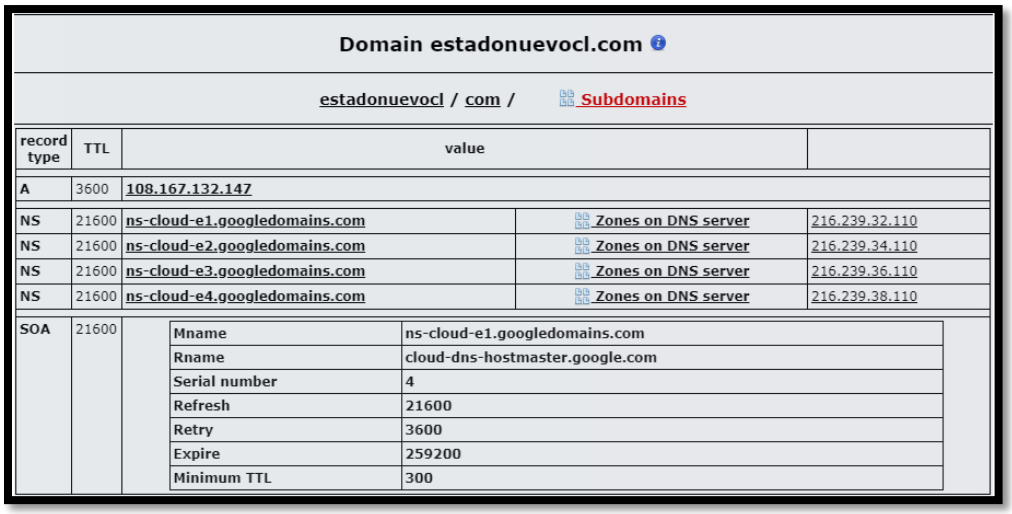
record type	TTL	value		
A	14400	66.235.200.146		
NS	86400	ns1.bluehost.com	Zones on DNS server	162.159.24.80
NS	86400	ns2.bluehost.com	Zones on DNS server	162.159.25.175
MX	14400	0 mail.hskfred.com		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname	ns1.bluehost.com	
		Rname	root.box5916.bluehost.com	
		Serial number	2020031600	
		Refresh	86400	
		Retry	7200	
		Expire	3600000	
		Minimum TTL	300	



Domain personal-estado.net

personal-estado / net / Subdomains

record type	TTL	value		
A	14400	111.90.142.123		
NS	86400	ns1.metaldns.com	Zones on DNS server	111.90.144.251
NS	86400	ns1.ipchina163.com	Zones on DNS server	124.217.246.5
NS	86400	ns2.metaldns.com	Zones on DNS server	185.70.107.110
NS	86400	ns1.steeldns.com	Zones on DNS server	101.99.72.47
MX	14400	0 personal-estado.net		
TXT	14400	v=spf1 +a +mx +ip4:111.90.142.90 +ip4:111.90.142.99 ~all		
SOA	86400	Mname	ns1.metaldns.com	
		Rname	notification.kbreaders.com	
		Serial number	2020031602	
		Refresh	3600	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	86400	



Domain estadonuevocl.com

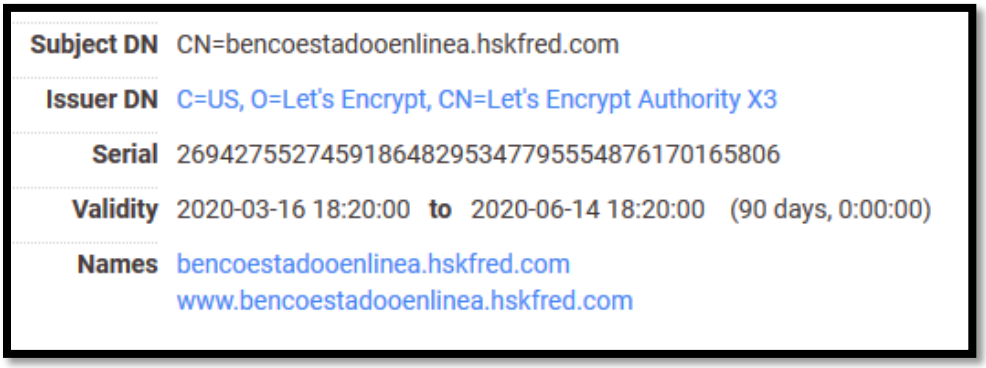
estadonuevocl / com / Subdomains

record type	TTL	value		
A	3600	108.167.132.147		
NS	21600	ns-cloud-e1.googledomains.com	Zones on DNS server	216.239.32.110
NS	21600	ns-cloud-e2.googledomains.com	Zones on DNS server	216.239.34.110
NS	21600	ns-cloud-e3.googledomains.com	Zones on DNS server	216.239.36.110
NS	21600	ns-cloud-e4.googledomains.com	Zones on DNS server	216.239.38.110
SOA	21600			

Mname	ns-cloud-e1.googledomains.com
Rname	cloud-dns-hostmaster.google.com
Serial number	4
Refresh	21600
Retry	3600
Expire	259200
Minimum TTL	300

Ilustración 1 Dominio donde se Aloja Url del Banco Estado Falso y DNS que utiliza

Certificados



Subject DN CN=bencoestadooenlinea.hskfred.com

Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Serial 269427552745918648295347795554876170165806

Validity 2020-03-16 18:20:00 **to** 2020-06-14 18:20:00 (90 days, 0:00:00)

Names bencoestadooenlinea.hskfred.com
www.bencoestadooenlinea.hskfred.com

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2587708053	2020-03-16	2020-03-16	2020-06-14	autodiscover.personal-estado.net cpanel.personal-estado.net cpcalendars.personal-estado.net cpcontacts.personal-estado.net mail.personal-estado.net personal-estado.net webdisk.personal-estado.net webmail.personal-estado.net www.personal-estado.net	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

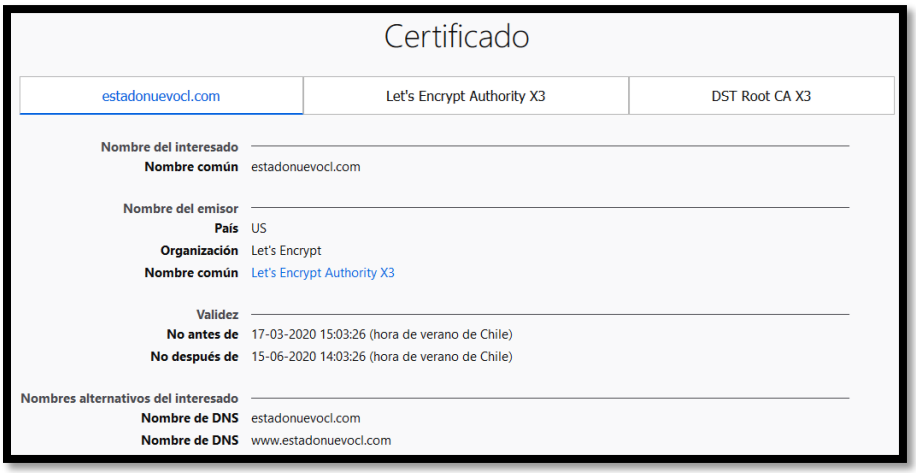


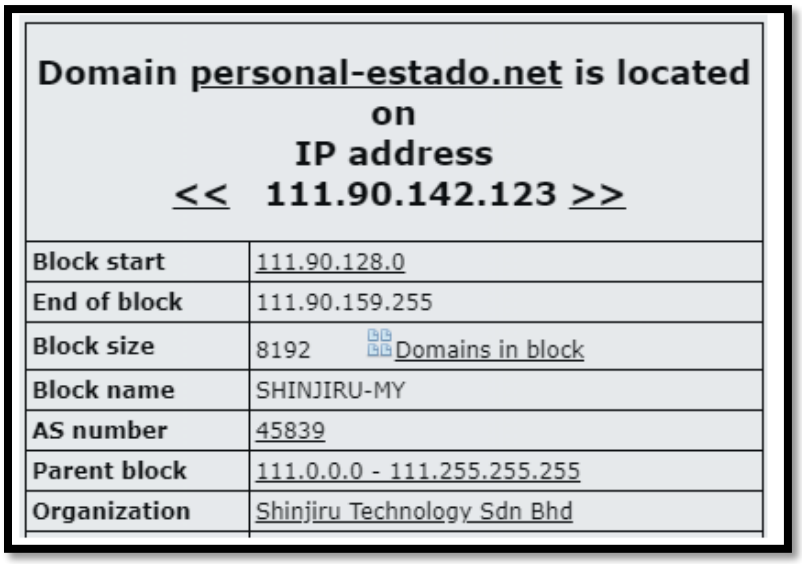
Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Estado

IP

162[.]241[.]30[.]51
111[.]90[.]142[.]123
108[.]167[.]132[.]147

Domain bencoestadooenlinea.hskfred.com is located on IP address << 162.241.30.51 >>

Block start	162.240.0.0
End of block	162.241.255.255
Block size	131072 Domains in block
Block name	UNIFIEDLAYER-NETWORK-16
AS number	46606
Parent block	162.0.0.0 - 162.255.255.255
Organization	UnifiedLayer



Domain personal-estado.net is located on IP address << 111.90.142.123 >>

Block start	111.90.128.0
End of block	111.90.159.255
Block size	8192 Domains in block
Block name	SHINJIRU-MY
AS number	45839
Parent block	111.0.0.0 - 111.255.255.255
Organization	Shinjiru Technology Sdn Bhd

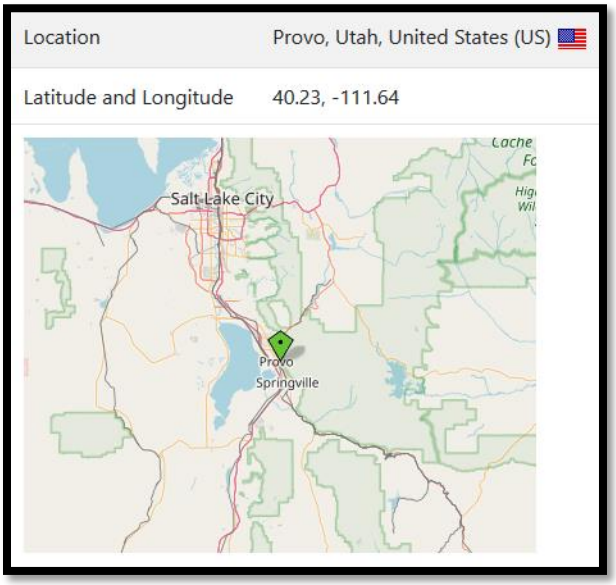
Domain www.estadonuevocl.com is located on IP address << 108.167.132.147 >>

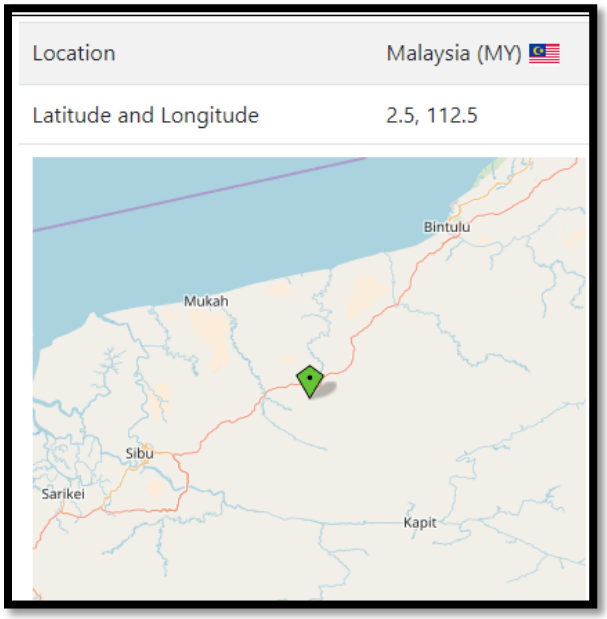
Block start	108.167.128.0
End of block	108.167.191.255
Block size	16384 Domains in block
Block name	HGBLOCK-4
AS number	46606
Parent block	108.0.0.0 - 108.255.255.255
Organization	WEBSITEWELCOME.COM

Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado

Localización

Provo, Utah, Estados Unidos
Malaysia
Houston, Texas, Estados Unidos





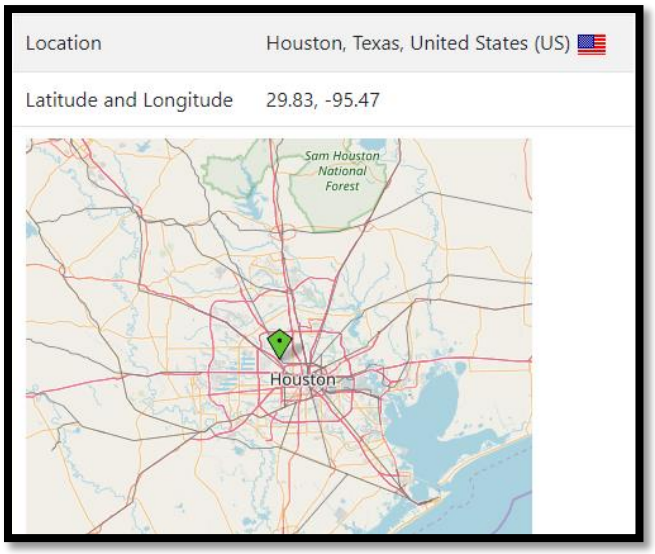
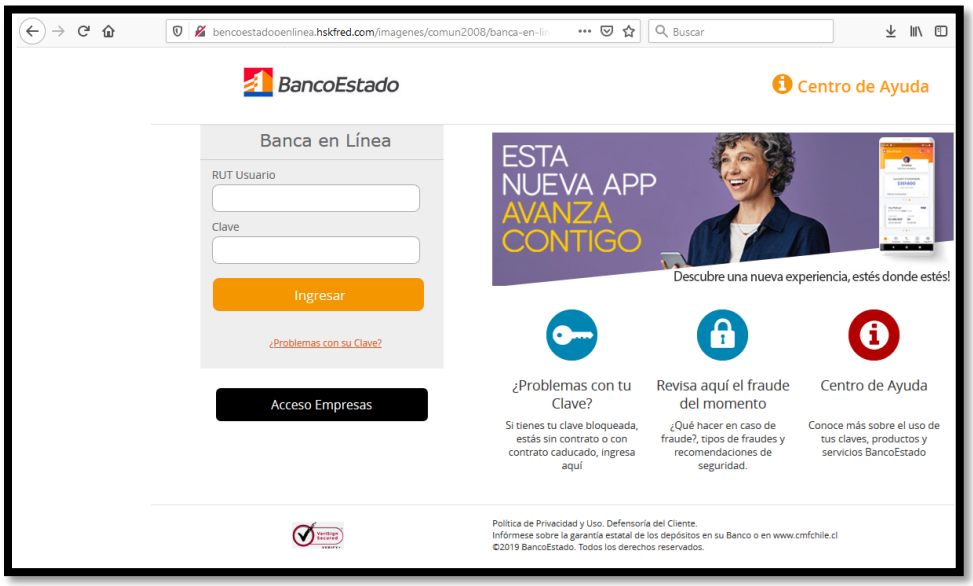
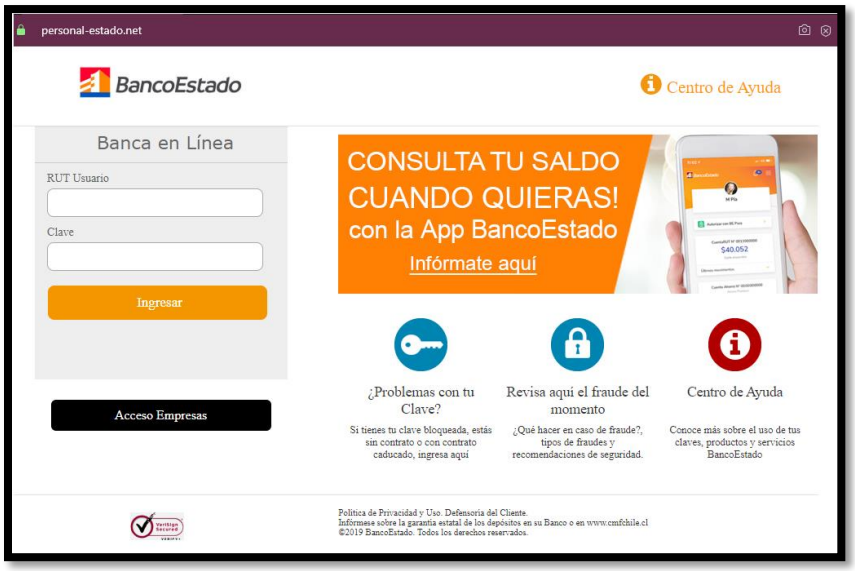
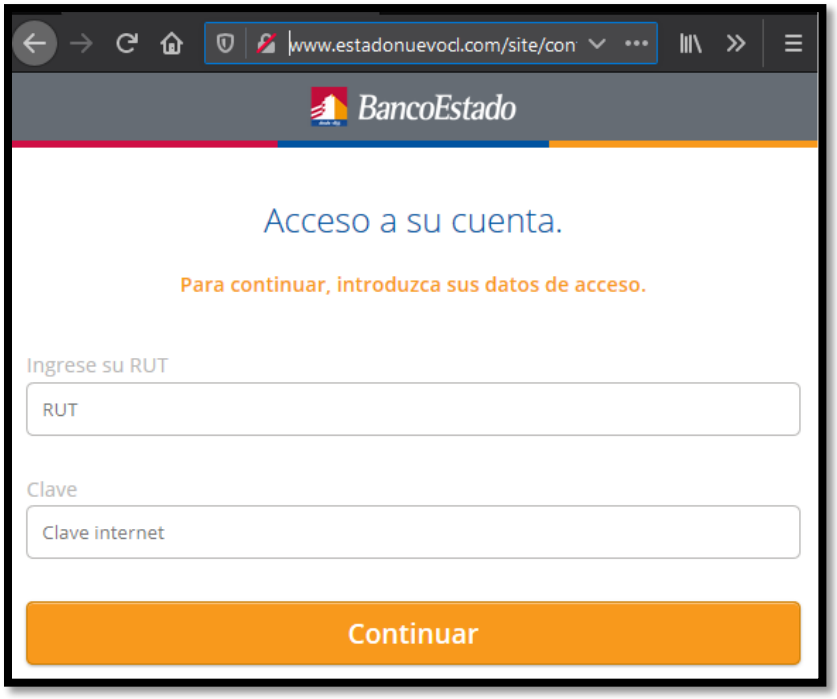


Imagen del sitio




personal-estado.net
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
Acceso Empresas
CONSULTA TU SALDO
CUANDO QUIERAS!
con la App BancoEstado
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
©2019 BancoEstado. Todos los derechos reservados.


www.estadonuevocl.com/site/con
BancoEstado
Acceso a su cuenta.
Para continuar, introduzca sus datos de acceso.
Ingrese su RUT
RUT
Clave
Clave internet
Continuar

Whois

```
Domain Name: HSKFRED.COM
Registry Domain ID: 2497405887_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.bluehost.com
Registrar URL: http://www.bluehost.com/
Updated Date: 2020-02-26T21:23:52Z
Creation Date: 2020-02-26T21:23:52Z
Registrar Registration Expiration Date: 2021-02-26T21:23:52Z
Registrar: FastDomain Inc.
Registrar IANA ID: 1154
Registrar Abuse Contact Email: support@bluehost.com
Registrar Abuse Contact Phone: +1.8017659400
Reseller: BlueHost.Com
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProh
ibited
Registry Registrant ID:
Registrant Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Registrant Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Registrant Street: 10 CORPORATE DR, STE 300
Registrant City: BURLINGTON
Registrant State/Province: MASSACHUSETTS
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.8017659400
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: WHOIS@BLUEHOST.COM
Registry Admin ID:
Admin Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Admin Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Admin Street: 10 CORPORATE DR, STE 300
Admin City: BURLINGTON
Admin State/Province: MASSACHUSETTS
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.8017659400
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: WHOIS@BLUEHOST.COM
Registry Tech ID:
Tech Name: DOMAIN PRIVACY SERVICE FBO REGISTRANT
Tech Organization: THE ENDURANCE INTERNATIONAL GROUP, INC.
Tech Street: 10 CORPORATE DR, STE 300
Tech City: BURLINGTON
Tech State/Province: MASSACHUSETTS
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.8017659400
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: WHOIS@BLUEHOST.COM
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
```

```
Domain Name: PERSONAL-ESTADO.NET
Registry Domain ID: 2504189337_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.ilovewww.com
Registrar URL: http://www.ilovewww.com
Updated Date: 2020-03-16T21:31:59Z
Creation Date: 2020-03-16T21:31:58Z
Registrar Registration Expiration Date: 2021-03-16T21:31:58Z
Registrar: Shinjiru MSC Sdn Bhd
Registrar IANA ID: 1741
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.metaldns.com
Name Server: ns2.metaldns.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@ilovewww.com
Registrar Abuse Contact Phone: +603 2031 8850
```

```
Domain Name: estadonuevocl.com
Registry Domain ID: 2504524441_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2020-03-17T18:56:09Z
Creation Date: 2020-03-17T18:56:03Z
Registrar Registration Expiration Date: 2021-03-17T18:56:07Z
Registrar: Google LLC
Registrar IANA ID: 895
Registrar Abuse Contact Email: registrar-abuse@google.com
Registrar Abuse Contact Phone: +1.8772376466
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 1246699362
Registrant Organization: Contact Privacy Inc. Customer 1246699362
Registrant Street: 96 Mowat Ave
Registrant City: Toronto
Registrant State/Province: ON
Registrant Postal Code: M4K 3K1
Registrant Country: CA
Registrant Phone: +1.4165385487
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: ue4shzdem208@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1246699362
Admin Organization: Contact Privacy Inc. Customer 1246699362
Admin Street: 96 Mowat Ave
Admin City: Toronto
Admin State/Province: ON
Admin Postal Code: M4K 3K1
Admin Country: CA
Admin Phone: +1.4165385487
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: ue4shzdem208@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1246699362
Tech Organization: Contact Privacy Inc. Customer 1246699362
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
Tech Postal Code: M4K 3K1
Tech Country: CA
Tech Phone: +1.4165385487
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: ue4shzdem208@contactprivacy.email
Name Server: ns-cloud-e1.googledomains.com
Name Server: ns-cloud-e2.googledomains.com
Name Server: ns-cloud-e3.googledomains.com
Name Server: ns-cloud-e4.googledomains.com
DNSSEC: signedDelegation
```

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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.18 00:28:02 -03'00'