Alerta de seguridad informática	8FFR20-00181-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Enero de 2020
Última revisión	14 de Enero 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 12 portales fraudulentos asociados a tres IP's que suplantan el sitio web oficial de **Banco Scotiabank**, los que podrían 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

URL Sitio Clonado:

scotia[.]cl[.]acceso-cl[.]com
scotia[.]cl[.]acceso-cl[.]com/Personas/
scotia[.]cl[.]acceso-cl[.]com/login/personas/
scotia[.]cl[.]acceso-cl[.]com/portalempresas/
www1[.]online-scotia[.]cl[.]acc-chile[.]info
www1[.]online-scotia[.]cl[.]acc-chile[.]info/Personas/
www1[.]online-scotia[.]cl[.]acc-chile[.]info/login/personas/
www1[.]online-scotia[.]cl[.]acc-chile[.]info/portalempresas/
online-scotia[.]cl[.]cv-chile[.]info
online-scotia[.]cl[.]cv-chile[.]info/Personas/
online-scotia[.]cl[.]cv-chile[.]info/login/personas/
online-scotia[.]cl[.]cv-chile[.]info/portalempresas/

Domain scotia.cl.acceso-cl.com

scotia / cl / acceso-cl / com / Subdomains

record type	TTL	value	
A	7207	142.93.226.63	

Domain acceso-cl.com

acceso-cl / com / Subdomains

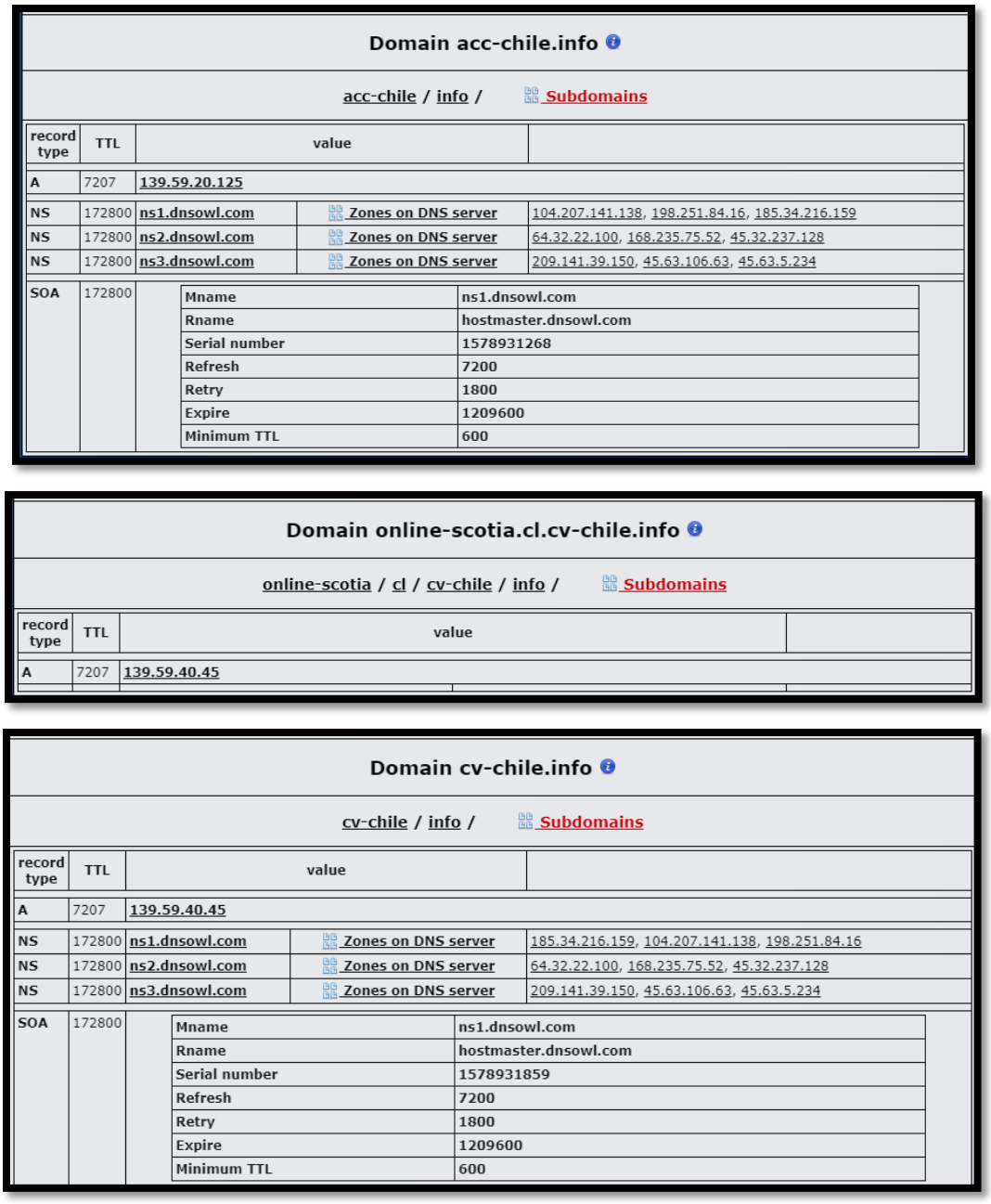
record type	TTL	value		
A	7207	142.93.226.63		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 185.34.216.159, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	45.32.237.128, 64.32.22.100, 168.235.75.52
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.5.234, 45.63.106.63

SOA	172800		
		Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1578921664
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Domain www1.online-scotia.cl.acc-chile.info

www1 / online-scotia / cl / acc-chile / info / Subdomains

record type	TTL	value	
A	7207	139.59.20.125	



Domain acc-chile.info

acc-chile / info / Subdomains

record type	TTL	value		
A	7207	139.59.20.125		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 198.251.84.16, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 168.235.75.52, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.106.63, 45.63.5.234
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1578931268	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

Domain online-scotia.cl.cv-chile.info

online-scotia / cl / cv-chile / info / Subdomains

record type	TTL	value
A	7207	139.59.40.45

Domain cv-chile.info

cv-chile / info / Subdomains

record type	TTL	value		
A	7207	139.59.40.45		
NS	172800	ns1.dnsowl.com	Zones on DNS server	185.34.216.159, 104.207.141.138, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	64.32.22.100, 168.235.75.52, 45.32.237.128
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.106.63, 45.63.5.234
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1578931859	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	

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

Certificados

Subject DN	CN=scotia.cl.acceso-cl.com
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	313635442077128469023797951100616075928389
Validity	2020-01-13 11:56:25 **to** 2020-04-12 11:56:25 (90 days, 0:00:00)
Names	scotia.cl.acceso-cl.com

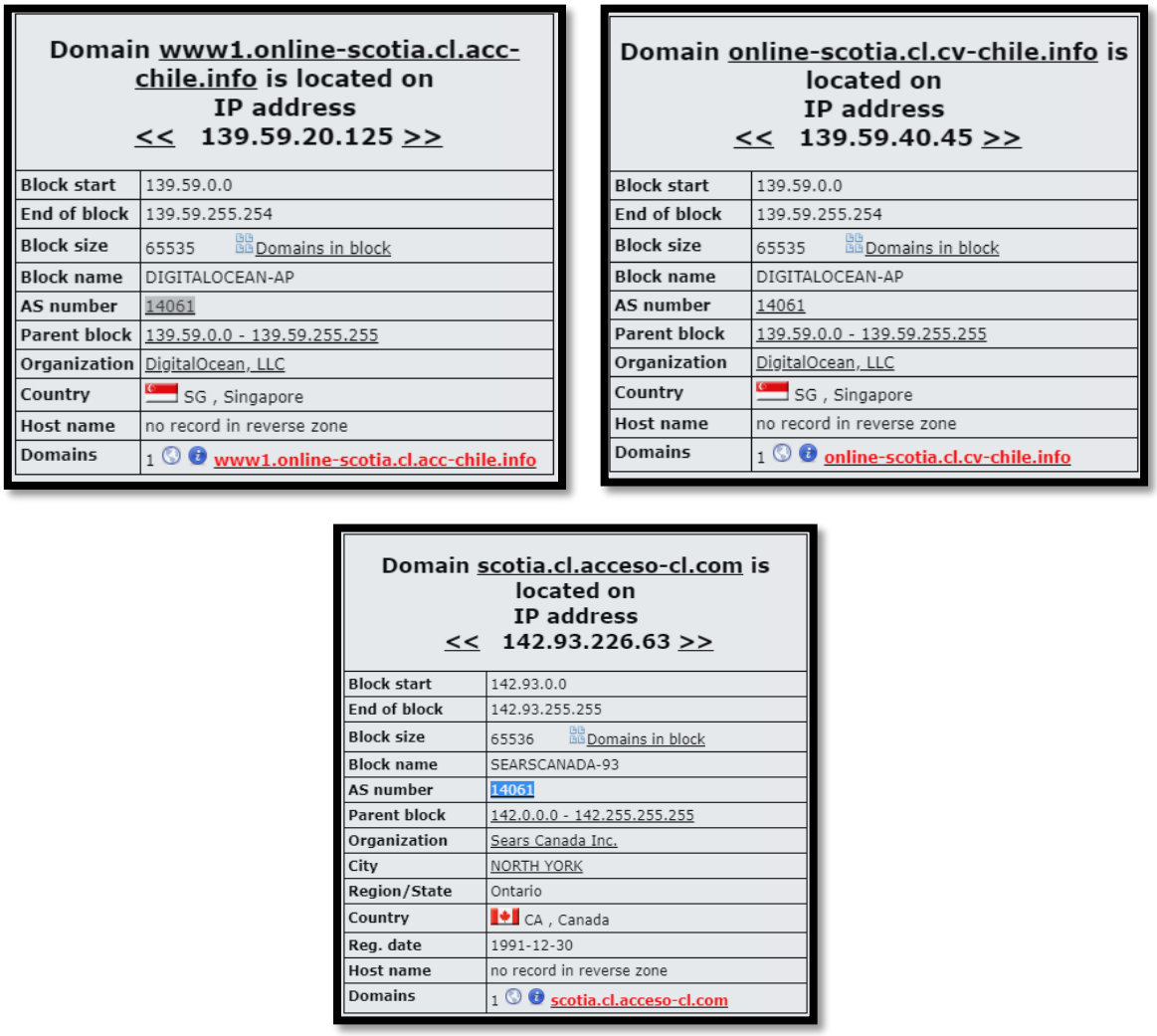
Subject DN	CN=www1.online-scotia.cl.acc-chile.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	311505113823684388055948999520276008976087
Validity	2020-01-07 04:16:38 **to** 2020-04-06 04:16:38 (90 days, 0:00:00)
Names	www1.online-scotia.cl.acc-chile.info

Subject DN	CN=online-scotia.cl.cv-chile.info
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	342392009929563578390733750190897621138980
Validity	2020-01-07 05:10:06 **to** 2020-04-06 05:10:06 (90 days, 0:00:00)
Names	online-scotia.cl.cv-chile.info

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Scotiabank.

IP

142.93.226.63
139.59.20.125
139.59.40.45



Domain www1.online-scotia.cl.acc-chile.info is located on IP address << 139.59.20.125 >>

Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC
Country	SG , Singapore
Host name	no record in reverse zone
Domains	1 www1.online-scotia.cl.acc-chile.info

Domain online-scotia.cl.cv-chile.info is located on IP address << 139.59.40.45 >>

Block start	139.59.0.0
End of block	139.59.255.254
Block size	65535 Domains in block
Block name	DIGITALOCEAN-AP
AS number	14061
Parent block	139.59.0.0 - 139.59.255.255
Organization	DigitalOcean, LLC
Country	SG , Singapore
Host name	no record in reverse zone
Domains	1 online-scotia.cl.cv-chile.info

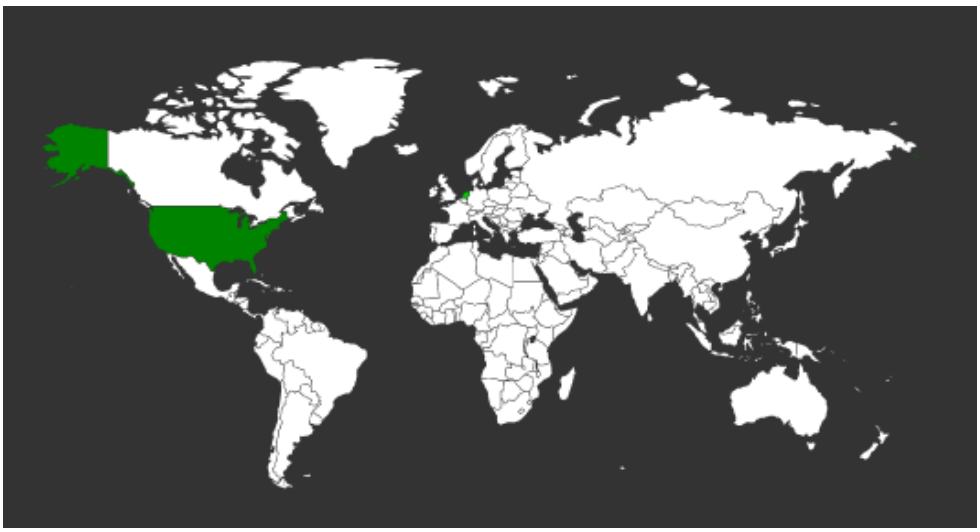
Domain scotia.cl.acceso-cl.com is located on IP address << 142.93.226.63 >>

Block start	142.93.0.0
End of block	142.93.255.255
Block size	65536 Domains in block
Block name	SEARSCANADA-93
AS number	14061
Parent block	142.0.0.0 - 142.255.255.255
Organization	Sears Canada Inc.
City	NORTH YORK
Region/State	Ontario
Country	CA , Canada
Reg. date	1991-12-30
Host name	no record in reverse zone
Domains	1 scotia.cl.acceso-cl.com

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

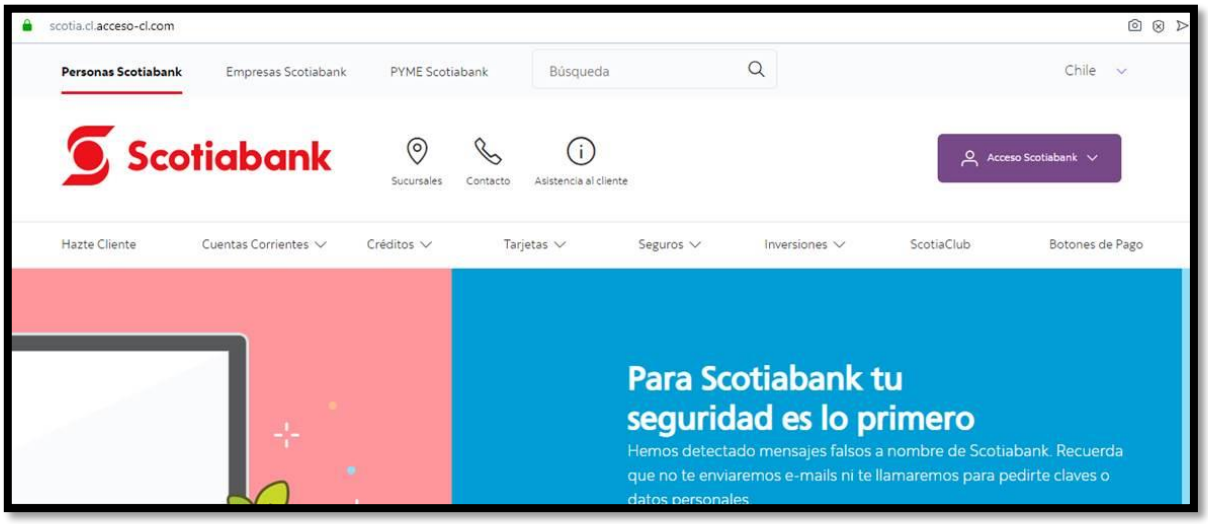
Localización

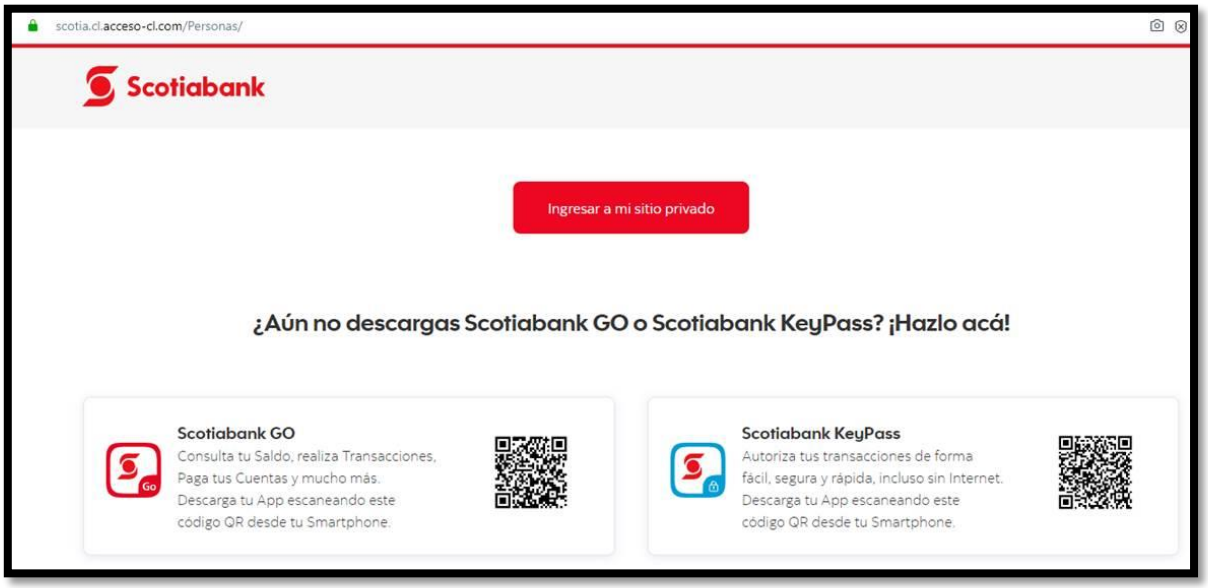
Amsterdam, Noord-Holland, Holanda

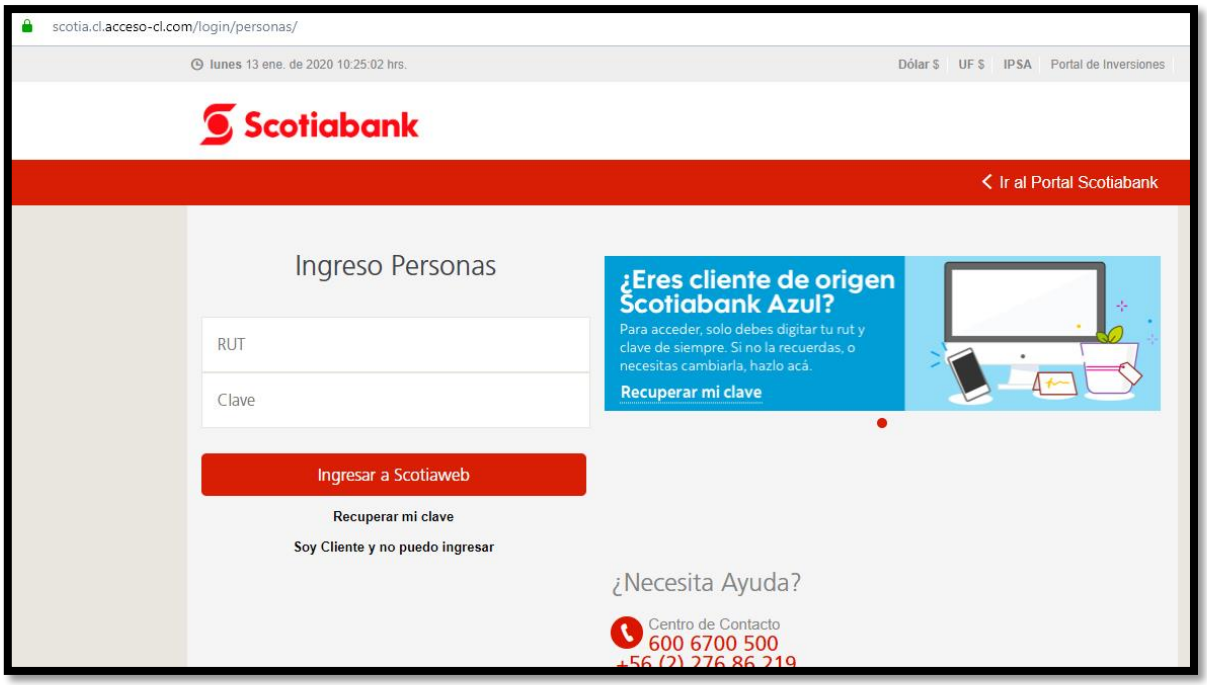


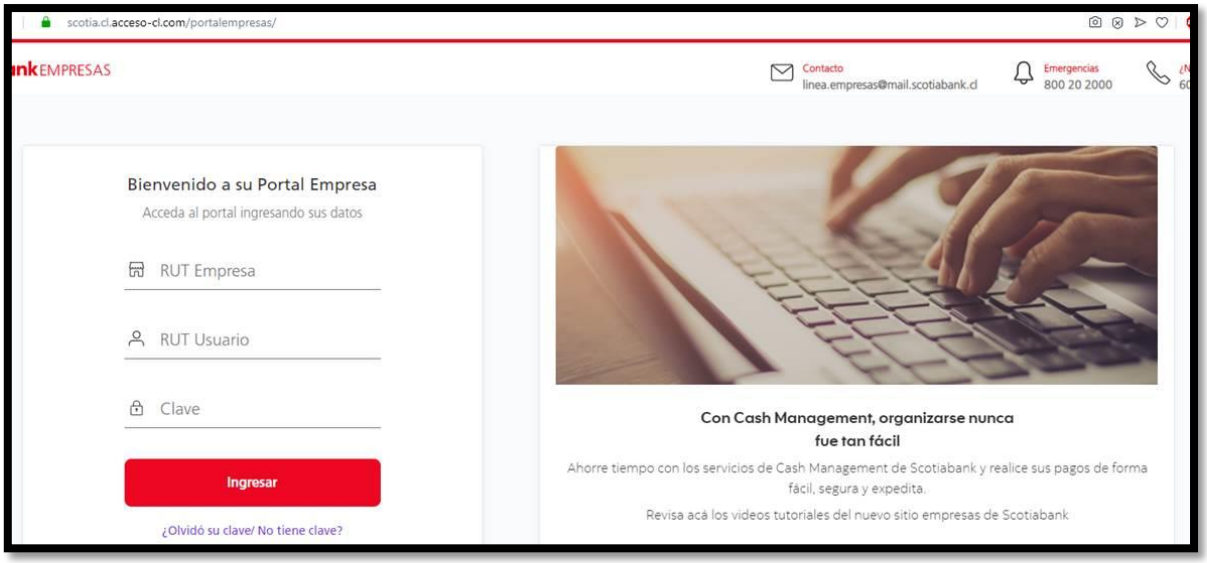
Bangalore, Karnataka, India

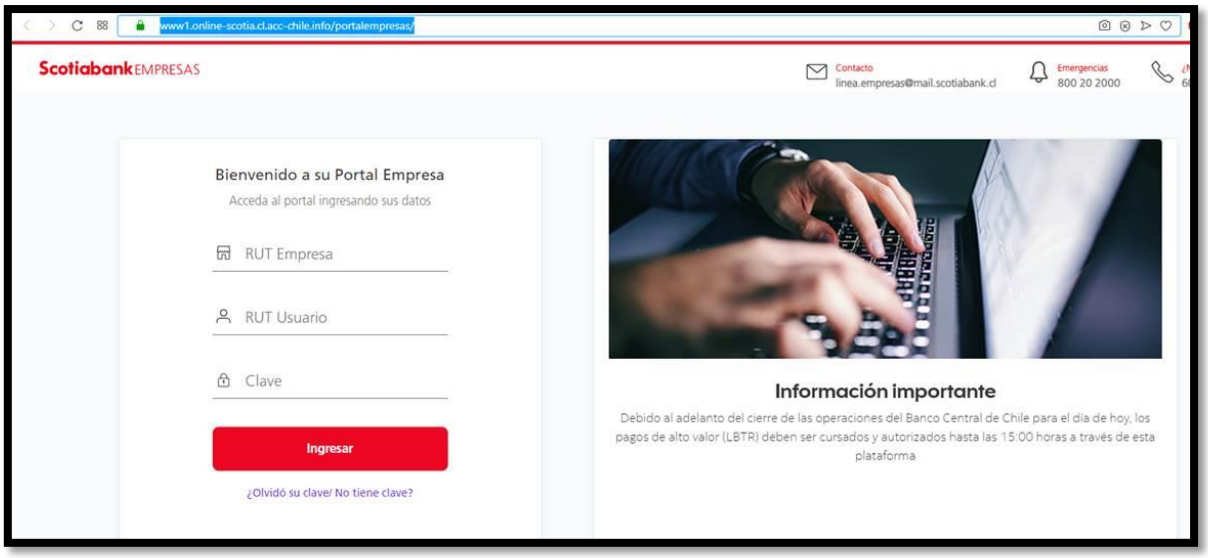
Imagen del sitio

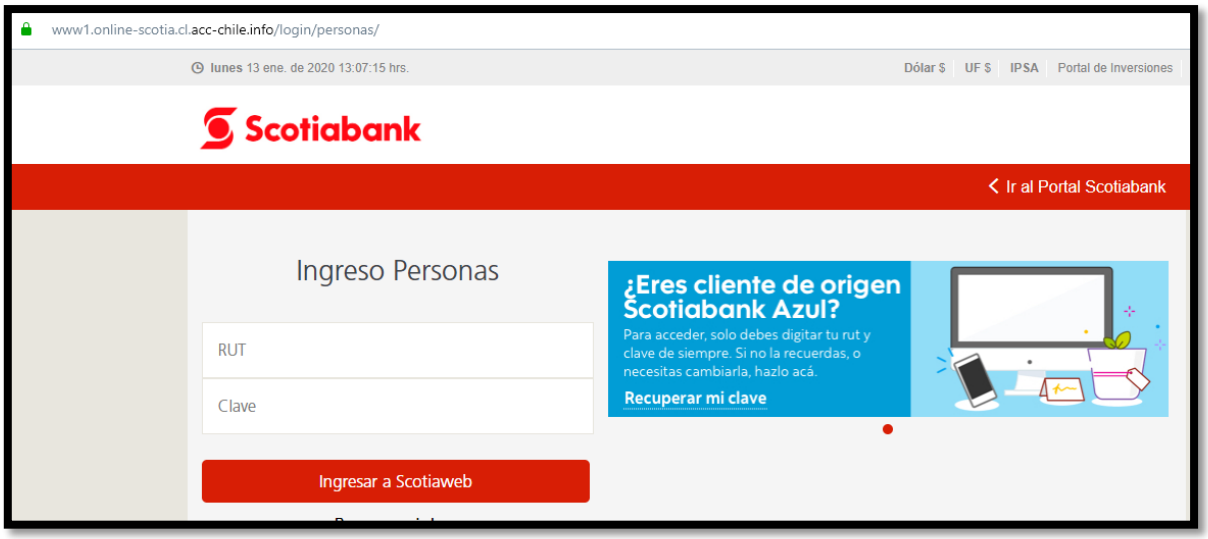


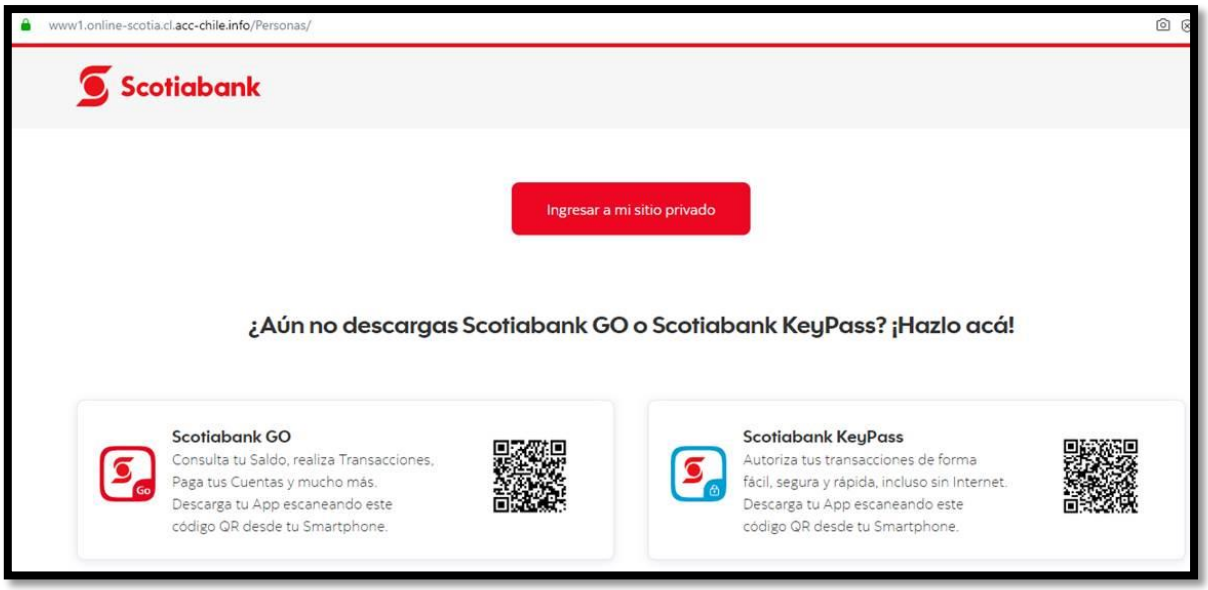


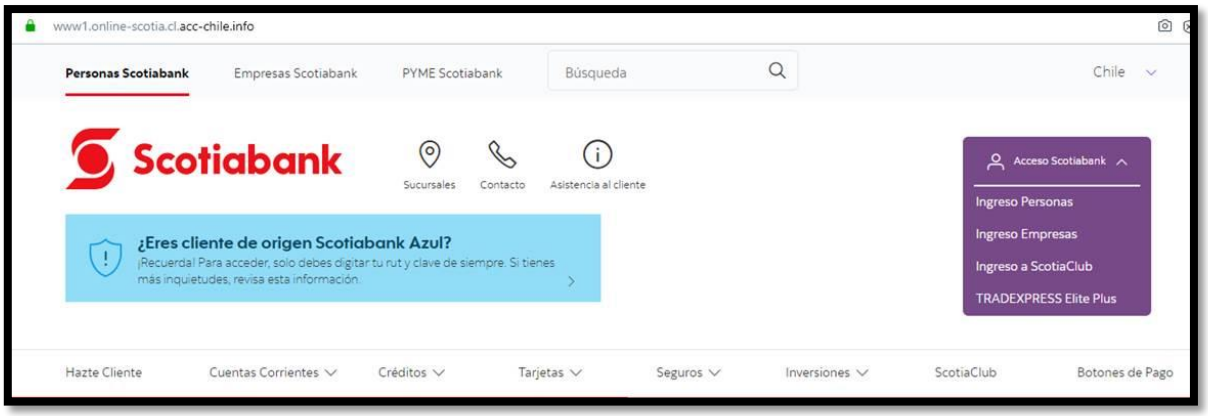

scotia.cl.acceso-cl.com/login/personas/
lunes 13 ene. de 2020 10:25:02 hrs.
Dólar $ UF $ IPSA Portal de Inversiones
Scotiabank
Ir al Portal Scotiabank
Ingreso Personas
RUT
Clave
Ingresar a Scotiaweb
Recuperar mi clave
Soy Cliente y no puedo ingresar
¿Eres cliente de origen Scotiabank Azul?
Para acceder, solo debes digitar tu rut y clave de siempre. Si no la recuerdas, o necesitas cambiarla, hazlo acá.
Recuperar mi clave
¿Necesita Ayuda?
Centro de Contacto
600 6700 500
+56 (2) 276 86 219

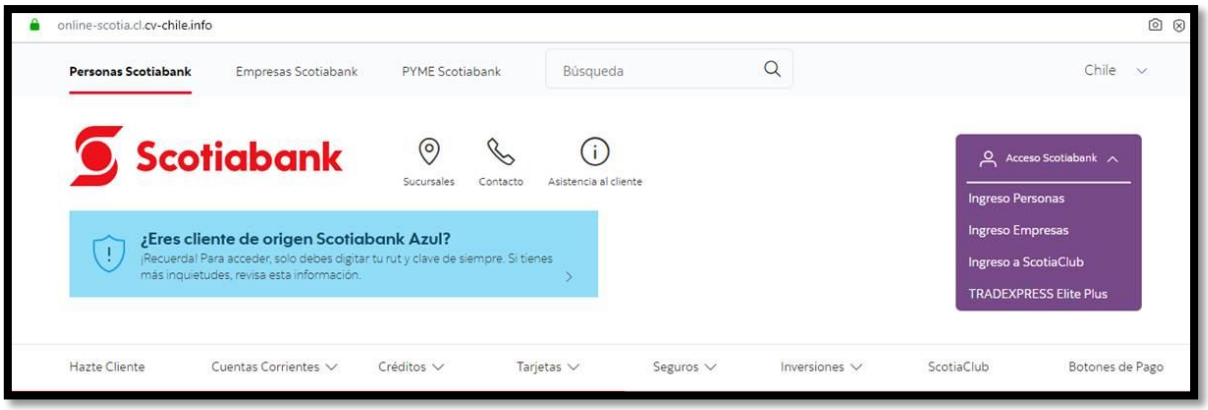

scotia.cl.acceso-cl.com/portalempresas/
nk EMPRESAS
Contacto
linea.empresas@mail.scotiabank.cl
Emergencias
800 20 2000
Bienvenido a su Portal Empresa
Acceda al portal ingresando sus datos
RUT Empresa
RUT Usuario
Clave
Ingresar
¿Olvidó su clave/ No tiene clave?
Con Cash Management, organizarse nunca fue tan fácil
Ahorre tiempo con los servicios de Cash Management de Scotiabank y realice sus pagos de forma fácil, segura y expedita.
Revisa acá los videos tutoriales del nuevo sitio empresas de Scotiabank

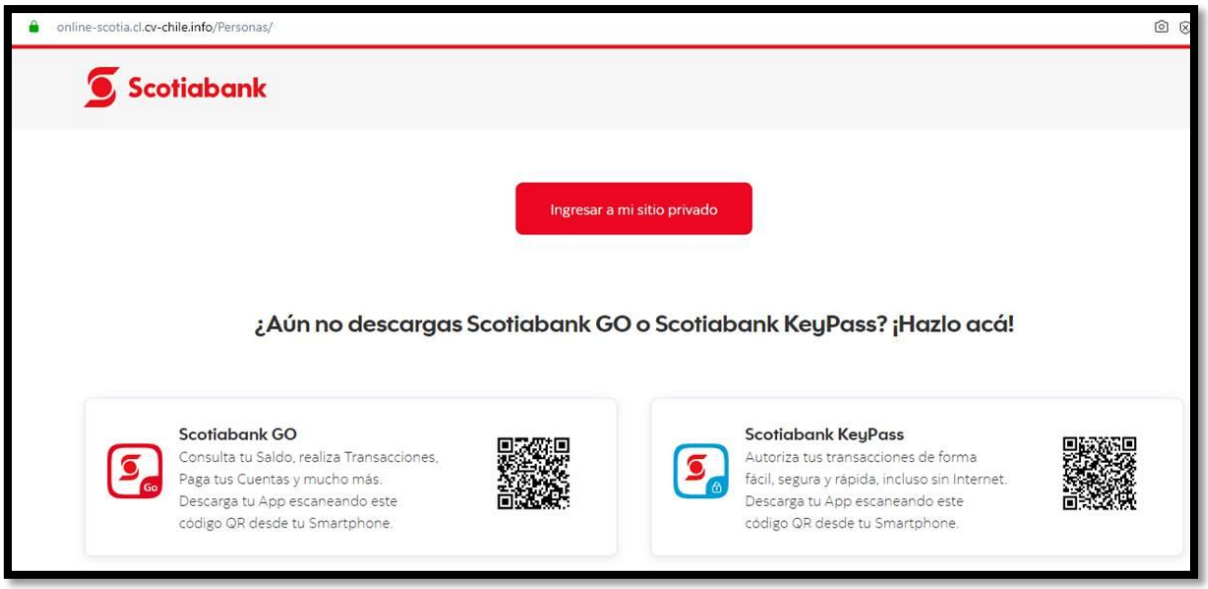

www1.online-scotia.cl.acc-chile.info/portalempresas/
ScotiabankEMPRESAS
Contacto
linea.empresas@mail.scotiabank.cl
Emergencias
800 20 2000
Bienvenido a su Portal Empresa
Acceda al portal ingresando sus datos
RUT Empresa
RUT Usuario
Clave
Ingresar
¿Olvidó su clave/ No tiene clave?
Información importante
Debido al adelanto del cierre de las operaciones del Banco Central de Chile para el día de hoy, los pagos de alto valor (LBTR) deben ser cursados y autorizados hasta las 15:00 horas a través de esta plataforma

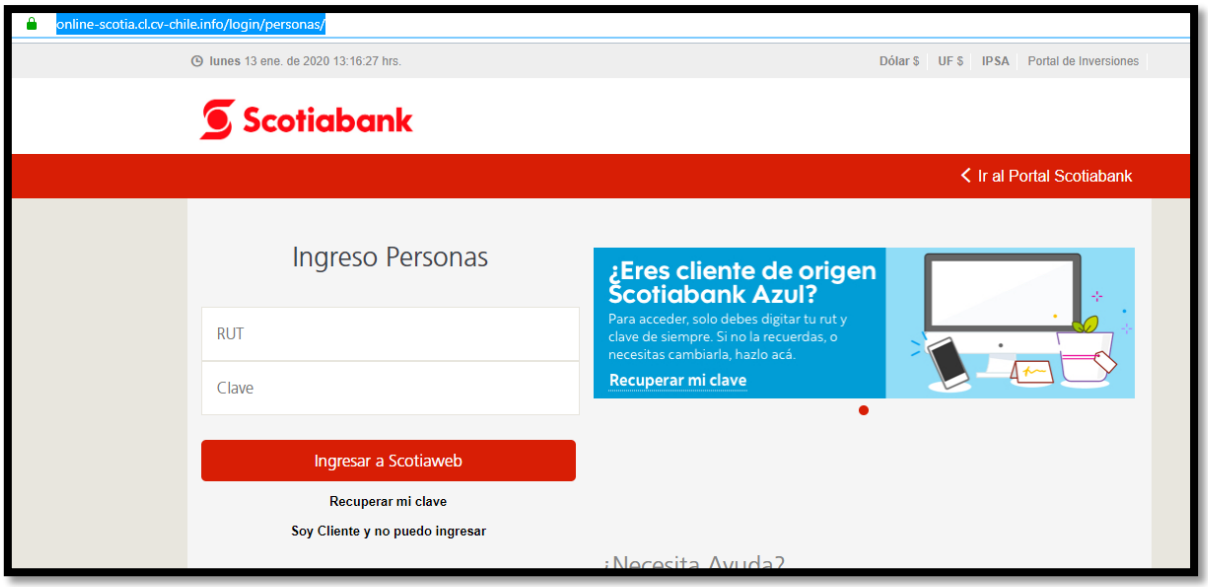

www1.online-scotia.cl.acc-chile.info/login/personas/
lunes 13 ene. de 2020 13:07:15 hrs.
Dólar $
UF $
IPSA
Portal de Inversiones
Scotiabank
Ir al Portal Scotiabank
Ingreso Personas
RUT
Clave
Ingresar a Scotiaweb
¿Eres cliente de origen Scotiabank Azul?
Para acceder, solo debes digitar tu rut y clave de siempre. Si no la recuerdas, o necesitas cambiarla, hazlo acá.
Recuperar mi clave

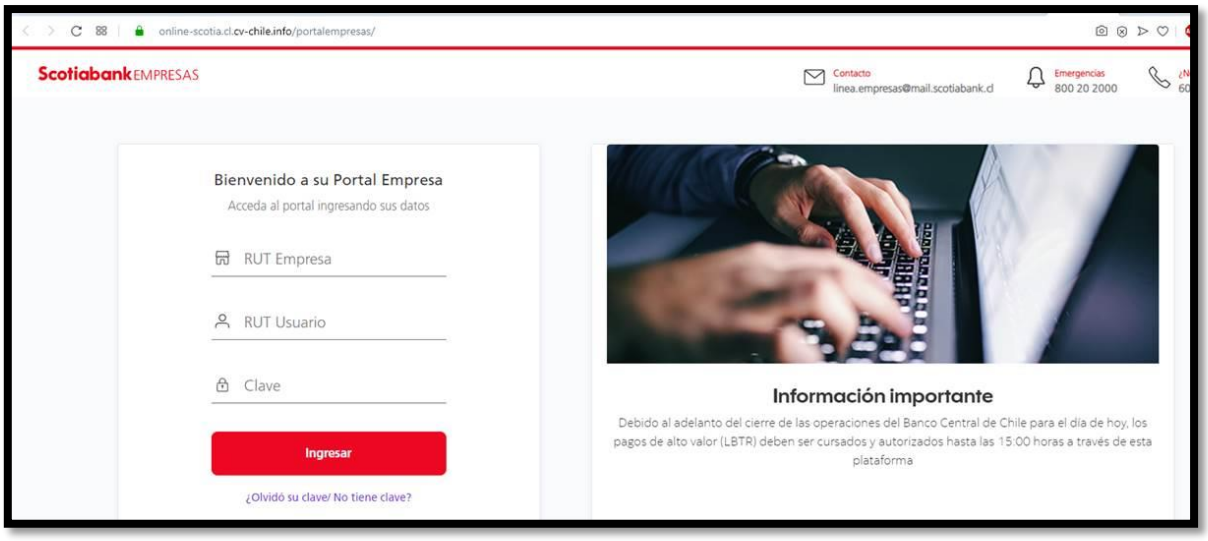

www1.online-scotia.cl.acc-chile.info/Personas/
Scotiabank
Ingresar a mi sitio privado
¿Aún no descargas Scotiabank GO o Scotiabank KeyPass? ¡Hazlo acá!
Scotiabank GO
Consulta tu Saldo, realiza Transacciones, Paga tus Cuentas y mucho más. Descarga tu App escaneando este código QR desde tu Smartphone.
Scotiabank KeyPass
Autoriza tus transacciones de forma fácil, segura y rápida, incluso sin Internet. Descarga tu App escaneando este código QR desde tu Smartphone.


www1.online-scotia.cl.acc-chile.info
Personas Scotiabank
Empresas Scotiabank
PYME Scotiabank
Búsqueda
Chile
Scotiabank
Sucursales
Contacto
Asistencia al cliente
Acceso Scotiabank
Ingreso Personas
Ingreso Empresas
Ingreso a ScotiaClub
TRADEXPRESS Elite Plus
¿Eres cliente de origen Scotiabank Azul?
¡Recuerda! Para acceder, solo debes digitar tu rut y clave de siempre. Si tienes más inquietudes, revisa esta información.
Hazte Cliente
Cuentas Corrientes
Créditos
Tarjetas
Seguros
Inversiones
ScotiaClub
Botones de Pago


online-scotia.cl.cv-chile.info
Personas Scotiabank
Empresas Scotiabank
PYME Scotiabank
Búsqueda
Chile
Scotiabank
Sucursales
Contacto
Asistencia al cliente
Acceso Scotiabank
Ingreso Personas
Ingreso Empresas
Ingreso a ScotiaClub
TRADEXPRESS Elite Plus
¿Eres cliente de origen Scotiabank Azul?
¡Recuerda! Para acceder, solo debes digitar tu rut y clave de siempre. Si tienes más inquietudes, revisa esta información.
Hazte Cliente
Cuentas Corrientes
Créditos
Tarjetas
Seguros
Inversiones
ScotiaClub
Botones de Pago


online-scotia.cl.cv-chile.info/Personas/
Scotiabank
Ingresar a mi sitio privado
¿Aún no descargas Scotiabank GO o Scotiabank KeyPass? ¡Hazlo acá!
Scotiabank GO
Consulta tu Saldo, realiza Transacciones, Paga tus Cuentas y mucho más. Descarga tu App escaneando este código QR desde tu Smartphone.
Scotiabank KeyPass
Autoriza tus transacciones de forma fácil, segura y rápida, incluso sin Internet. Descarga tu App escaneando este código QR desde tu Smartphone.


online-scotia.cl.cv-chile.info/login/personas/
lunes 13 ene. de 2020 13:16:27 hrs.
Dólar $
UF $
IPSA
Portal de Inversiones
Scotiabank
Ir al Portal Scotiabank
Ingreso Personas
RUT
Clave
Ingresar a Scotiaweb
Recuperar mi clave
Soy Cliente y no puedo ingresar
¿Eres cliente de origen Scotiabank Azul?
Para acceder, solo debes digitar tu rut y clave de siempre. Si no la recuerdas, o necesitas cambiarla, hazlo acá.
Recuperar mi clave
¿Necesita Ayuda?


online-scotia.cl.cv-chile.info/portalempresas/
ScotiabankEMPRESAS
Contacto
linea.empresas@mail.scotiabank.cl
Emergencias
800 20 2000
Bienvenido a su Portal Empresa
Acceda al portal ingresando sus datos
RUT Empresa
RUT Usuario
Clave
Ingresar
¿Olvidó su clave/ No tiene clave?
Información importante
Debido al adelanto del cierre de las operaciones del Banco Central de Chile para el día de hoy, los pagos de alto valor (LBTR) deben ser cursados y autorizados hasta las 15:00 horas a través de esta plataforma

Whois

```
Domain Name: acceso-cl.com
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-01-13T07:00:00Z
Creation Date: 2020-01-13T07:00:00Z
Registrar Registration Expiration Date: 2021-01-13T07:00:00Z
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-88de636fa79dadee5ee0861bc50e69f3@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-88de636fa79dadee5ee0861bc50e69f3@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-88de636fa79dadee5ee0861bc50e69f3@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: 2020-01-13T07:00:00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

```
Domain Name: acc-chile.info
Registry Domain ID: D503300001182776359-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-01-07T07:00:00Z
Creation Date: 2020-01-06T07:00:00Z
Registrar Registration Expiration Date: 2021-01-06T07:00:00Z
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-64892b412b6f5473843bdf7100078159@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-64892b412b6f5473843bdf7100078159@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-64892b412b6f5473843bdf7100078159@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: 2020-01-13T07:00:00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE AND TERMS OF USE: You are not authorized to access or query our WHOIS
```

```
Domain Name: cv-chile.info
Registry Domain ID: D503300001182777139-LRMS
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-01-07T07:00:00Z
Creation Date: 2020-01-06T07:00:00Z
Registrar Registration Expiration Date: 2021-01-06T07:00:00Z
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-d742bde2a6e5fe29f021dce29adbf740@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-d742bde2a6e5fe29f021dce29adbf740@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-d742bde2a6e5fe29f021dce29adbf740@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: 2020-01-13T07:00:00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

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.