Alerta de seguridad informática	8FFR20-00250-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Marzo de 2020
Última revisión	10 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

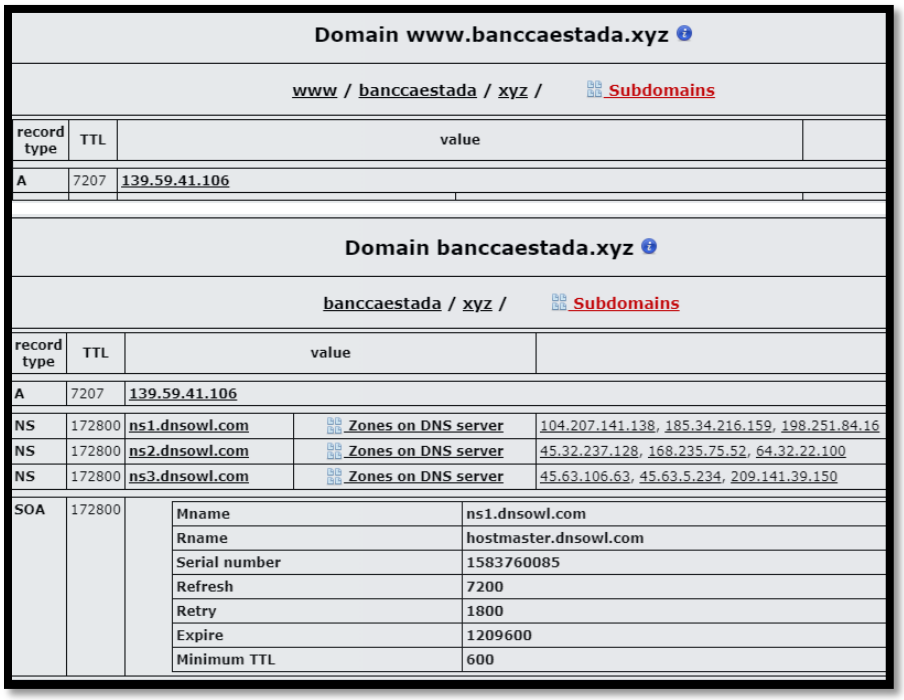
El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de dos portales fraudulentos asociados a dos IPs que suplantan el sitio web oficial del Banco Estado, el que podría servir para robar credenciales de usuarios de esa entidad.

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

www[.]banccaestada[.]xyz
www[.]banccaestada[.]xyz/imagenes/comun2008/banca-en-linea-personas[.]php?html
empresasbancestado[.]ddns[.]net
empresabancestado[.]ddns[.]net



Domain www.banccaestada.xyz

www / banccaestada / xyz / Subdomains

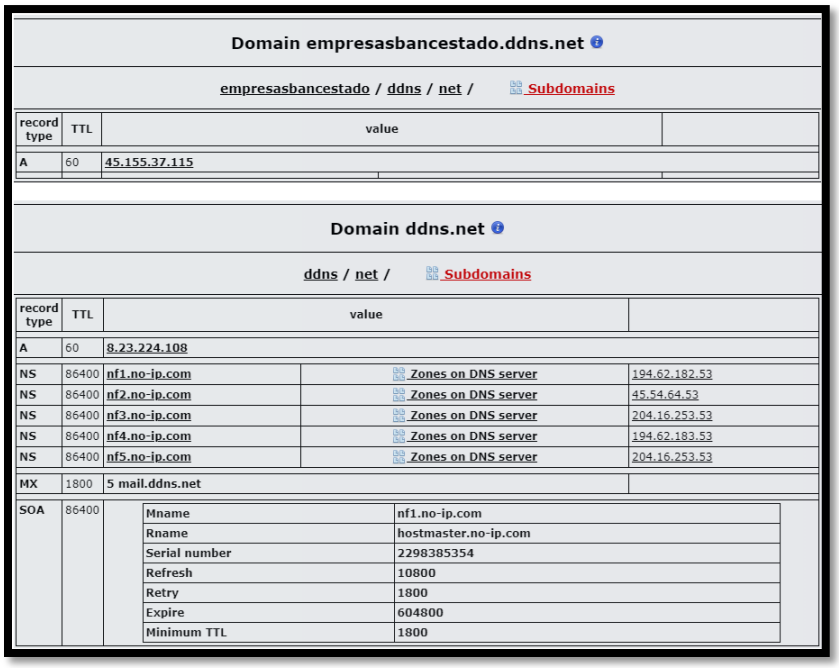
record type	TTL	value
A	7207	139.59.41.106

Domain banccaestada.xyz

banccaestada / xyz / Subdomains

record type	TTL	value		
A	7207	139.59.41.106		
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, 168.235.75.52, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 45.63.5.234, 209.141.39.150

SOA	172800	Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1583760085
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600



Domain empresasbancestado.ddns.net

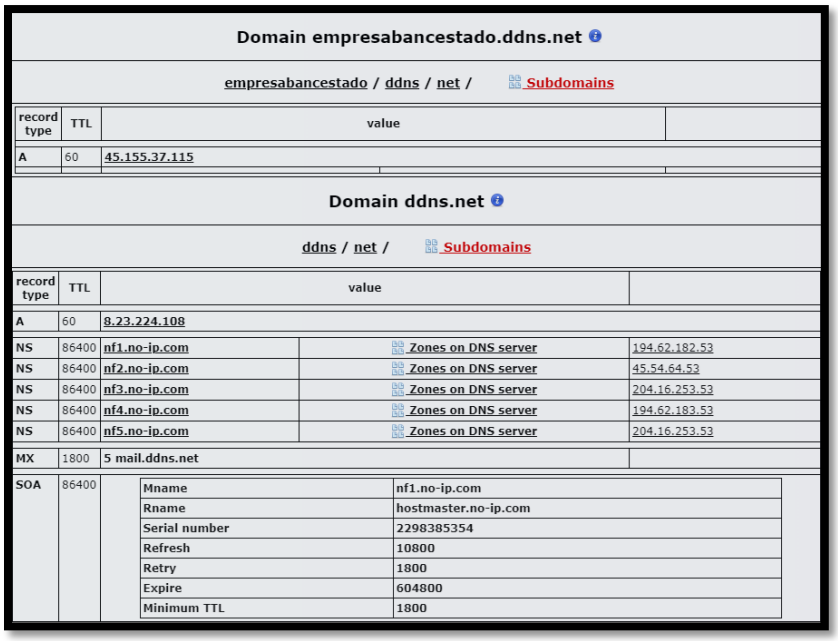
empresasbancestado / ddns / net / Subdomains

record type	TTL	value
A	60	45.155.37.115

Domain ddns.net

ddns / net / Subdomains

record type	TTL	value		
A	60	8.23.224.108		
NS	86400	nf1.no-ip.com	Zones on DNS server	194.62.182.53
NS	86400	nf2.no-ip.com	Zones on DNS server	45.54.64.53
NS	86400	nf3.no-ip.com	Zones on DNS server	204.16.253.53
NS	86400	nf4.no-ip.com	Zones on DNS server	194.62.183.53
NS	86400	nf5.no-ip.com	Zones on DNS server	204.16.253.53
MX	1800	5 mail.ddns.net		
SOA	86400	Mname: nf1.no-ip.com Rname: hostmaster.no-ip.com Serial number: 2298385354 Refresh: 10800 Retry: 1800 Expire: 604800 Minimum TTL: 1800		



Domain empresabancestado.ddns.net

empresabancestado / ddns / net / Subdomains

record type	TTL	value
A	60	45.155.37.115

Domain ddns.net

ddns / net / Subdomains

record type	TTL	value		
A	60	8.23.224.108		
NS	86400	nf1.no-ip.com	Zones on DNS server	194.62.182.53
NS	86400	nf2.no-ip.com	Zones on DNS server	45.54.64.53
NS	86400	nf3.no-ip.com	Zones on DNS server	204.16.253.53
NS	86400	nf4.no-ip.com	Zones on DNS server	194.62.183.53
NS	86400	nf5.no-ip.com	Zones on DNS server	204.16.253.53
MX	1800	5 mail.ddns.net		
SOA	86400	Mname: nf1.no-ip.com Rname: hostmaster.no-ip.com Serial number: 2298385354 Refresh: 10800 Retry: 1800 Expire: 604800 Minimum TTL: 1800		

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

Certificados

Subject DN	CN=www.banccaestada.xyz
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	341645734206421737229892648407570050896380
Validity	2020-03-09 05:46:22 **to** 2020-06-07 05:46:22 (90 days, 0:00:00)
Names	www.banccaestada.xyz

Subject DN	CN=empresasbancestado.ddns.net
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	310636134723878032976002859039434266284651
Validity	2020-03-09 14:01:49 **to** 2020-06-07 14:01:49 (90 days, 0:00:00)
Names	empresasbancestado.ddns.net

Subject DN	CN=empresabancestado.ddns.net
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	303211733132586234637097424924591177830608
Validity	2020-03-09 18:07:50 **to** 2020-06-07 18:07:50 (90 days, 0:00:00)
Names	empresabancestado.ddns.net

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

IP

139[.]59[.]41[.]106
45[.]155[.]37[.]115

Domain www.banccaestada.xyz is located on IP address << 139.59.41.106 >>

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

Domain empresasbancestado.ddns.net is located on IP address << 45.155.37.115 >>

Block start	45.155.36.0
End of block	45.155.39.255
Block size	1024 Domains in block
Block name	US-SHOCK11-20190917
AS number	395092
Parent block	45.128.0.0 - 45.159.255.255
Organization	ORG-SHL36-RIPE

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

Localización
Bengaluru, Karnataka, India
Maidenhead, England, United Kingdom

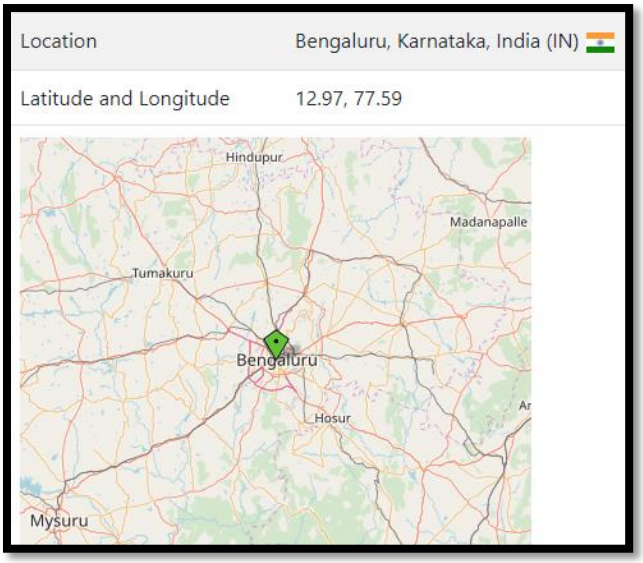
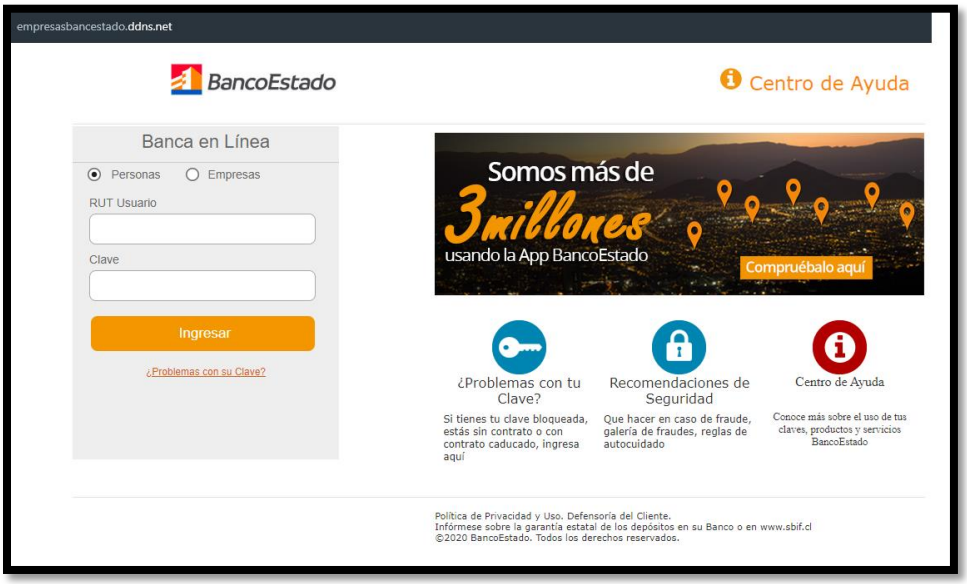
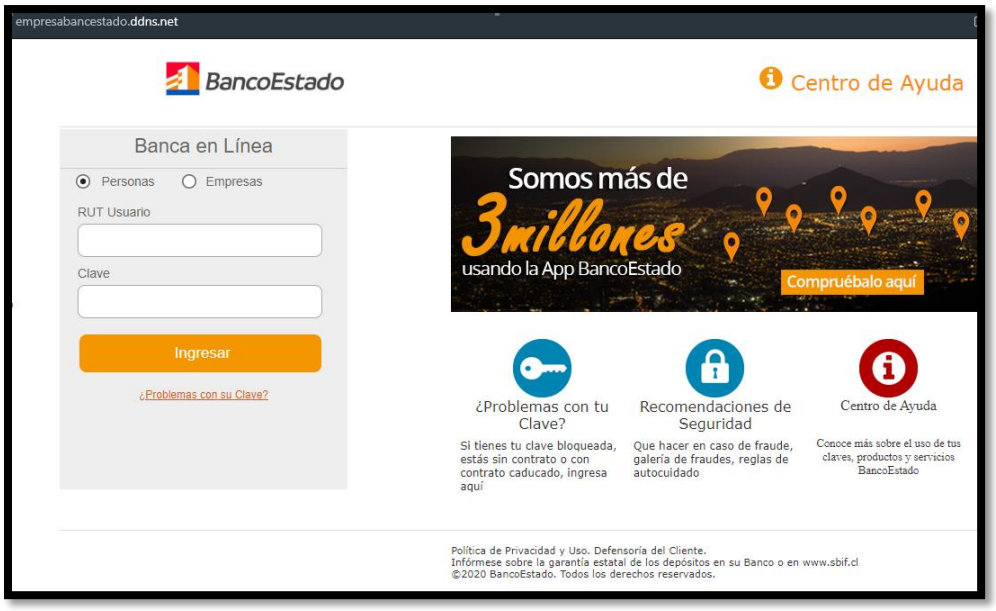


Imagen del sitio




empresabancestado.ddns.net
BancoEstado
Centro de Ayuda
Banca en Línea
Personas
Empresas
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Somos más de
3millones
usando la App BancoEstado
Compruébalo aquí
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Recomendaciones de Seguridad
Que hacer en caso de fraude, galería de fraudes, reglas de autocuidado
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.sbif.cl
©2020 BancoEstado. Todos los derechos reservados.

Whois

```
Domain Name: banccaestada.xyz
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-09T07:00:00Z
Creation Date: 2020-03-08T07:00:00Z
Registrar Registration Expiration Date: 2021-03-08T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: ok https://www.icann.org/epp#ok
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-52af39996f7aa0cce65ab621d88154d7@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-52af39996f7aa0cce65ab621d88154d7@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-52af39996f7aa0cce65ab621d88154d7@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: ddns.net
Registry Domain ID: 73816572_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2020-02-07T16:50:29Z
Creation Date: 2001-06-28T16:04:59Z
Registrar Registration Expiration Date: 2022-06-28T16:04:59Z
Registrar: TLDS LLC. d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Dan Durrer
Registrant Organization: No-IP.com
Registrant Street: 425 Maestro  Dr. Second Floor
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89511
Registrant Country: US
Registrant Phone: +1.7758531883
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: domains@no-ip.com
Registry Admin ID:
Admin Name: Dan Durrer
Admin Organization: No-IP.com
Admin Street: 425 Maestro  Dr. Second Floor
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89511
Admin Country: US
Admin Phone: +1.7758531883
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: domains@no-ip.com
Registry Tech ID:
Tech Name: Dan Durrer
Tech Organization: No-IP.com
Tech Street: 425 Maestro  Dr. Second Floor
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89511
Tech Country: US
Tech Phone: +1.7758531883
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: domains@no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf1.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf3.no-ip.com
DNSSEC: Unsigned
```

```
Domain Name: ddns.net
Registry Domain ID: 73816572_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2020-02-07T16:50:29Z
Creation Date: 2001-06-28T16:04:59Z
Registrar Registration Expiration Date: 2022-06-28T16:04:59Z
Registrar: TLDS LLC. d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Dan Durrer
Registrant Organization: No-IP.com
Registrant Street: 425 Maestro  Dr. Second Floor
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89511
Registrant Country: US
Registrant Phone: +1.7758531883
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: domains@no-ip.com
Registry Admin ID:
Admin Name: Dan Durrer
Admin Organization: No-IP.com
Admin Street: 425 Maestro  Dr. Second Floor
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89511
Admin Country: US
Admin Phone: +1.7758531883
Admin Phone Ext.:
Admin Fax:
Admin Fax Ext.:
Admin Email: domains@no-ip.com
Registry Tech ID:
Tech Name: Dan Durrer
Tech Organization: No-IP.com
Tech Street: 425 Maestro  Dr. Second Floor
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89511
Tech Country: US
Tech Phone: +1.7758531883
Tech Phone Ext.:
Tech Fax:
Tech Fax Ext.:
Tech Email: domains@no-ip.com
Name Server: nf2.no-ip.com
Name Server: nf1.no-ip.com
Name Server: nf4.no-ip.com
Name Server: nf3.no-ip.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8773812449
```

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: 2020.03.10 12:24:12 -03'00'