28-05-2020 | Año 1 | N°47

Boletín de Seguridad Cibernética

Semana del 21 al 27 de mayo 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

División de Redes y Seguridad Informática.

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Resumen de la semana en cifras

Parches

13

para vulnerabilidades

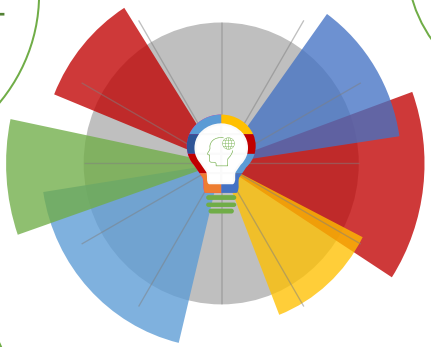
Las mitigaciones son útiles para productos de DNS, SQLite, Wire Shark, Apache, Fortinet, OpenSSH y OpenConnect

Se advirtieron

15

sitios fraudulentos

Asociadas a 9 IP maliciosas



Phishing

5

Campañas

Entre ellos se cuentan phishing bancarios, de servicios de pago y correos corporativos

IPs

134

bloqueadas

Listado de IPs que trataron de realizar escaneos de puertos, DDoS o infectar códigos maliciosos, entre otros.

*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl

Contenido

Sitios fraudulentos

Imagen del sitio

CSIRT advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00426-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Mayo de 2020
Última revisión	21 de Mayo de 2020
Indicadores de compromiso	
URL	
bancochile-cl-portal[.]spectr-store[.]com[.]ua	
IP	
31[.]131[.]19[.]186	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00426-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00426-01.pdf	

Imagen del sitio

CSIRT advierte de un sitio de entrega de bonos fraudulento	
Alerta de seguridad cibernética	8FFR20-00427-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Mayo de 2020
Última revisión	22 de Mayo de 2020
Indicadores de compromiso	
URL	
bonosdechile[.]cl	
IP	
138[.]186[.]9[.]45	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00427-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00427-01.pdf	

Imagen del sitio

CSIRT advierte de un portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00428-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Mayo de 2020
Última revisión	23 de Mayo de 2020
Indicadores de compromiso	
URL	
bancapersonas[.]bancoestado[.]cl[.]arzala[.]com/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
199[.]168[.]189[.]50	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00428-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00428-01.pdf	

Imagen del sitio

CSIRT advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00429-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Mayo de 2020
Última revisión	24 de Mayo de 2020
Indicadores de compromiso	
URL	
https[://]jp-ffm[.]de/_personas/www[.]santander[.]cl/pagina/mobil/movil[.]Bancoenlinea	
IP	
173[.]212[.]192[.]146	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00429-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00429-01.pdf	

Imagen del sitio

CSIRT informa de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00430-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Mayo de 2020
Última revisión	26 de Mayo de 2020
Indicadores de compromiso	
URL	
acceso[.]bacochile[.]com/portal-aoN3ZqWRnpJqq5Nnq6kA0B	
IP	
161[.]35[.]15[.]121	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00430-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00430-01.pdf	

Imagen del sitio

CSIRT advierte de un portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00431-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Mayo de 2020
Última revisión	26 de Mayo de 2020
Indicadores de compromiso	
URL	
acceso[.]bacoestado[.]win	
IP	
95[.]179[.]254[.]172	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00431-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00431-01.pdf	

Imagen del sitio

CSIRT advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00432-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Mayo de 2020
Última revisión	27 de Mayo de 2020
Indicadores de compromiso	
URL	
bancostado[.]me	
IP	
45[.]56[.]114[.]12	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00432-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00432-01.pdf	

Phishing

Imagen del sitio

CSIRT advierte phishing por servicio de streaming suspendido	
Alerta de seguridad cibernética	8FPH20-00227-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Mayo de 2020
Última revisión	21 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://netflix-activa[.]com	
IP	
hxxps://netflix-activaciones[.]com/cl/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00227-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00227-01.pdf	

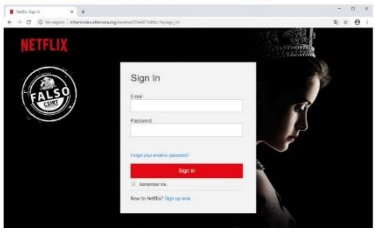
Imagen del sitio

CSIRT advierte de Smishing bancario sobre bono covid-19	
Alerta de seguridad cibernética	8FPH20-00228-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Mayo de 2020
Última revisión	23 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://bit[.]ly/2ZohSLn?l=www.santander.cl,	
hxxps://www.zouavespontificaux[.]be/activacion/cuenta-feza/	
hxxps://jp-ffm[.]de/_personas/www.santander.cl/pagina/Bancoenlinea	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00228-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00228-01.pdf	

CSIRT advierte de phishing sobre supuesta ayuda del gobierno	
Alerta de seguridad cibernética	8FPH20-00229-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Mayo de 2020
Última revisión	24 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://www.tarjetas-solicitud[.]xyz/?APLICAR	
hxxps://www.ayudas[.]club/?APLICAR	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00229-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00229-01.pdf	

CSIRT advierte phishing por retención de correos	
Alerta de seguridad cibernética	8FPH20-00230-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Mayo de 2020
Última revisión	25 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://kwiksurveys[.]com/s/QKTYAyRJ#/0	
IP	
[212.5.159.59]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/8fph20-00230-01/	
https://csirt.gob.cl/media/2020/05/8FPH20-00230-01.pdf	

Imagen del sitio



CSIRT advierte de phishing de servicio de streaming	
Alerta de seguridad cibernética	8FPH20-00231-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Mayo de 2020
Última revisión	25 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxp://ottienivideo.altervista[.]org/newbie/f20e4973d8bc1fe/sign_in/	
IP	
[50.116.86.60]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/8fph20-00231-01/	
https://csirt.gob.cl/media/2020/05/8FPH20-00231-01.pdf	

Vulnerabilidades

CSIRT comparte información sobre vulnerabilidad en protocolo DNS	
Alerta de seguridad cibernética	9VSA20-00221-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Mayo de 2020
Última revisión	21 de Mayo de 2020
CVE	
CVE-2020-8616, CVE-2020-12662, CVE-2020-10995,CVE-2020-12667	
Producto afectado	
Protocolo DNS	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00221-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00221-01.pdf	

CSIRT comparte actualizaciones liberadas por Apache para Apache Tomcat	
Alerta de seguridad cibernética	9VSA20-00222-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Mayo de 2020
Última revisión	24 de Mayo de 2020
CVE	
CVE-2020-9484	
Fabricante	
Apache	
Producto afectado	
Apache Tomcat desde la versión 10.0.0-M1 hasta la 10.0.0-M4. Apache Tomcat desde la versión 9.0.0.M1 hasta la 9.0.34. Apache Tomcat desde la versión 8.5.0 hasta la 8.5.54. Apache Tomcat desde la versión 7.0.0 hasta la 7.0.103.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00222-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00222-01.pdf	

CSIRT comparte actualizaciones de WireShark	
Alerta de seguridad cibernética	9VSA20-00223-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Mayo de 2020
Última revisión	24 de Mayo de 2020
CVE	
CVE-2020-13164	
Fabricante	
WireShark	
Producto afectado	
Wireshark desde la versión 3.2.0 hasta la 3.2.3, desde la 3.0.0 hasta la 3.0.10 y desde la 2.6.0 hasta la 2.6.16.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00223-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00223-01.pdf	

CSIRT comparte actualizaciones liberadas por OpenConnect	
Alerta de seguridad cibernética	9VSA20-00224-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Mayo de 2020
Última revisión	26 de Mayo de 2020
CVE	
CVE-2020-12823	
Fabricante	
OpenConnect	
Producto afectado	
OpenConnect VPN desde la versión 3.99 hasta la 8.09.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00224-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00224-01.pdf	

CSIRT comparte actualizaciones de jQuery	
Alerta de seguridad cibernética	9VSA20-00225-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Mayo de 2020
Última revisión	26 de Mayo de 2020
CVE	
CVE-2020-7656	
Fabricante	
jQuery	
Producto afectado	
jQuery desde la versión 1.0 hasta la 1.8.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00225-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00225-01.pdf	

CSIRT comparte actualizaciones de SQLite	
Alerta de seguridad cibernética	9VSA20-00226-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Mayo de 2020
Última revisión	26 de Mayo de 2020
CVE	
CVE-2020-13434, CVE-2020-13435	
Fabricante	
SQLite	
Producto afectado	
Afecta a todas las versiones de SQLite desde que la función “printf()” fue introducida en la versión 3.8.2 (03-02-2014).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00226-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00226-01.pdf	

CSIRT comparte actualizaciones de Fortinet	
Alerta de seguridad cibernética	9VSA20-00227-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Mayo de 2020
Última revisión	27 de Mayo de 2020
CVE	
CVE-2020-9291, CWE-79	
Fabricante	
Fortinet	
Producto afectado	
FortiClient para Windows versión 6.2.1 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00227-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00227-01.pdf	

CSIRT comparte actualizaciones de OpenSSH	
Alerta de seguridad cibernética	9VSA20-00228-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de Mayo de 2020
Última revisión	20 de Mayo de 2020
CVE	
CWE-399	
Fabricante	
OpenSSH	
Producto afectado	
OpenSSH desde la versión 5.0p1 hasta la 8.2p1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00228-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00228-01.pdf	

Indicadores de Compromisos

Se comparte a continuación el listado de IPs que fueron detectadas durante la pasada semana por el Equipo del CSIRT intentando ejecutar escaneaos puertos, ataques de denegación de servicios o tratando de infectar con códigos maliciosos, entre otros ataques, para el conocimiento de la comunidad:

IoC	Motivo	IoC	Motivo
103.99.2.170	Port Scan	159.65.247.164	Port Scan
103.145.12.131	Port Scan	96.44.162.82	Port Scan
139.59.98.34	Port Scan	37.49.226.165	Port Scan
194.180.224.123	Port Scan	91.241.19.135	Port Scan
103.145.12.122	Port Scan	163.172.52.221	Port Scan
142.93.14.109	Port Scan	123.51.152.52	Port Scan
192.241.233.163	Port Scan	79.137.121.166	Port Scan
51.83.52.66	Port Scan	51.159.0.77	Port Scan
103.133.105.31	Port Scan	103.99.2.7	Port Scan
156.231.45.78	Port Scan	185.232.65.105	Port Scan
208.91.109.50	Port Scan	139.180.217.95	Port Scan
185.209.0.26	Port Scan	95.179.187.83	Port Scan
209.141.43.150	Port Scan	78.130.254.164	Port Scan
185.66.189.13	Port Scan	51.159.31.42	Port Scan
198.98.52.15	Port Scan	51.159.57.58	Port Scan
199.195.252.242	Port Scan	162.219.179.228	Port Scan
198.98.49.192	Port Scan	107.180.238.174	Port Scan
185.234.219.12	Port Scan	201.155.204.151	Malware
162.243.136.201	Port Scan	45.148.121.3	Port Scan
192.236.176.143	Port Scan	162.243.136.200	Port Scan
185.144.80.58	Port Scan	45.143.220.94	Port Scan
156.96.156.69	Port Scan	193.226.185.66	Port Scan
162.243.136.121	Port Scan	37.49.226.253	Port Scan
45.143.220.149	Port Scan	45.33.57.147	Port Scan
103.145.12.122	Port Scan	144.91.127.206	Port Scan
190.111.255.219	Malware	162.243.136.246	Port Scan
51.83.216.215	Port Scan	195.154.94.244	Port Scan
103.141.136.150	Port Scan	103.145.12.134	Port Scan
51.83.216.214	Port Scan	66.219.18.145	Port Scan
51.83.216.213	Port Scan	104.236.80.32	Port Scan

185.176.27.210	Port Scan	37.49.226.40	Port Scan
23.94.93.106	Malware	185.200.118.48	Port Scan
45.143.220.122	Port Scan	212.59.0.2	Malware
194.180.224.60	Port Scan	164.52.24.169	Port Scan
199.19.226.221	Port Scan	167.172.36.176	Hacking
205.185.121.153	Port Scan	70.35.207.197	Hacking
142.44.136.2	DDoS	20.37.111.213	Hacking
192.241.199.63	Port Scan	128.199.46.178	Hacking
45.55.38.214	Port Scan	72.167.20.142	Hacking
162.243.136.166	Port Scan	176.53.21.30	Hacking
162.243.136.108	Port Scan	94.130.209.126	Hacking
181.214.243.10	Port Scan	89.248.160.152	Hacking
51.159.71.63	Port Scan	195.54.160.130	Hacking
51.159.57.29	Port Scan	131.72.236.173	Hacking
209.159.151.27	Port Scan	209.90.225.226	Hacking
128.14.181.122	Port Scan	180.244.233.163	Hacking
209.141.53.207	Port Scan	51.222.30.247	Hacking
5.181.156.109	Port Scan	5.101.0.209	Hacking
156.96.155.231	Port Scan	148.251.33.195	Malware
205.171.2.64	Port Scan	37.228.117.90	Malware
67.115.118.5	Port Scan	5.9.128.163	Malware
37.49.226.11	Port Scan	50.116.86.205	Malware
162.243.136.52	Port Scan	51.255.165.160	Malware
194.61.24.37	Port Scan	165.227.192.27	Port Scan
185.216.140.101	Port Scan	89.248.168.196	Port Scan
163.172.58.63	Port Scan	162.243.136.70	Port Scan
82.223.253.144	Port Scan	45.148.10.72	Port Scan
171.67.71.243	Port Scan	45.143.220.6	Port Scan
185.110.95.5	Port Scan	5.182.211.241	Port Scan
176.57.138.50	Port Scan	103.145.12.26	Port Scan
37.49.226.56	Port Scan	199.201.110.206	Port Scan
51.79.146.179	Port Scan	167.172.105.219	Port Scan
45.14.224.136	Port Scan	119.159.150.176	Malware
45.143.223.207	Port Scan	198.12.97.84	Port Scan
162.243.136.238	Port Scan	103.31.232.93	Malware
103.145.12.123	Port Scan	185.53.88.205	Port Scan
104.248.63.105	Port Scan	5.182.210.96	Port Scan

Recomendaciones y Buenas Prácticas

Recomendaciones generales de seguridad

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Investigación

Malware Belonard. El caso de Counter Strike 1.6.

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la quinta edición de su publicación sobre amenazas cibernéticas el que analiza el Malware Belonard, que afectó hace unos meses atrás al juego Counter Strike 1.6. Este artículo que fue elaborado por Gabriela Sepúlveda Bravo, analista de nivel 2 de CSIRT.

El malware infectó a miles de usuarios del popular juego Counter Strike 1.6 (C.S.1.6) aprovechando una vulnerabilidad RCE (Remote Code Execution) en el lado del cliente para crear servidores proxy con malware que ofrecían ventajas de latencia comparativamente mejores frente a otros proxys legítimos. Belonard llegó a crear una extensa botnet que estuvo activa por varios meses.

Este artículo tiene como objetivo analizar la estructura y el impacto de Belonard, para que sea tomado en consideración y sirva de advertencia frente a potenciales ataques que imiten su método en el futuro.

Ver en: https://www.csirt.gob.cl/reportes/an2-2020-05/

Actualidad

Tener acceso a Internet hoy es un gran beneficio. Nos permite mantenernos comunicados y continuar trabajando y estudiando. Pero los riesgos y amenazas de su uso son diversos y las consecuencias de una navegación insegura podrían afectar tus dispositivos, el control de tu información e incluso generar pérdidas económicas. Para navegar con seguridad, te invitamos a seguir algunos ciberconsejos.

Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos públicos del Estado, al informar problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución del mismo.

- Pier Rivera
  Linkedin:
  https://www.linkedin.com/in/pier-angeli-rivera-contreras-08071946/
- Patricio Campos. Linkedin:
  https://www.linkedin.com/in/pcamposo/
- Matia Cornejo
  Linkedin:
  https://www.linkedin.com/in/matia-cornejo/
- Rodrigo Benavides
  Linkedin:
  https://www.linkedin.com/in/rbenavides/
- Benjamin Vega
  Twitter: @benjavega123
- Miguel Ángel
  Linkedin:
  https://www.linkedin.com/in/miguel-angel-mz/

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.05.29 17:19:31 -04'00'