04-06-2020 | Año 1 | N°48

Boletín de Seguridad Cibernética

Semana del 28 de mayo al 03 de junio 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

*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 tres sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00433-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Mayo de 2020
Última revisión	29 de Mayo de 2020
Indicadores de compromiso	
URL	
bancoestado-portal-cl[.]cf	
bancoestado-cl-datos-actualizados[.]tk	
bancoestado-cl-datos-actualizados[.]ml	
IP	
178[.]159[.]36[.]211	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00433-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00433-01.pdf	

Imagen del sitio

CSIRT advierte de dos portales bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00434-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Mayo de 2020
Última revisión	29 de Mayo de 2020
Indicadores de compromiso	
URL	
https[://]bankestado[.]net	
bancoestado-validacion-person-cl[.]ml	
IP	
8[.]208[.]91[.]252	
178[.]159[.]36[.]211	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00434-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00434-01.pdf	

Imagen del sitio

CSIRT advierte de tres sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00435-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Mayo de 2020
Última revisión	30 de Mayo de 2020
Indicadores de compromiso	
URL	
www[.]bancoestado-cl[.]loughgallpresbyterian[.]co[.]uk/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
acceso[.]bacoestado[.]com	
bancoestado-validacion-personas-cl[.]ga	
IP	
185[.]199[.]220[.]102	
64[.]225[.]126[.]81	
178[.]159[.]36[.]211	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00435-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00435-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00436-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Mayo de 2020
Última revisión	30 de Mayo de 2020
Indicadores de compromiso	
URL	
chouhanprinter[.]com/Personas/www[.]itau[.]cl/	
IP	
111[.]118[.]215[.]77	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00436-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00436-01.pdf	

Imagen del sitio

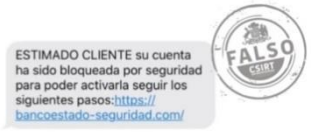
CSIRT informa de un portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00437-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Mayo de 2020
Última revisión	30 de Mayo de 2020
Indicadores de compromiso	
URL	
bancestado-actualizaciondeinformacion[.]ml	
IP	
178[.]159[.]36[.]211	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00437-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00437-01.pdf	

Imagen del sitio

CSIRT informa de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00438-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Junio de 2020
Última revisión	01 de Junio de 2020
Indicadores de compromiso	
URL	
https[://]www[.]bancapersonas-bancoestado[.]euromob[.]cl	
IP	
186[.]64[.]117[.]55	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00438-01/	
https://www.csirt.gob.cl/media/2020/06/8FFR20-00438-01.pdf	

Phishing

Imagen del mensaje



CSIRT informa sobre Smishing bancario por bloqueo de cuenta	
Alerta de seguridad cibernética	8FPH20-00232-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Mayo de 2020
Última revisión	28 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://bancoestado-seguridad[.]com/personas/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00232-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00232-01.pdf	

Imagen del mensaje

CSIRT advierte phishing en falsa transferencia de beneficios estatales	
Alerta de seguridad cibernética	8FPH20-00233-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Mayo de 2020
Última revisión	28 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxp://bigforum[.]in/js/enviar.php?l=589944743	
hxxps://chouhanprinter[.]com/Pension/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[45.236.129.232]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00233-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00233-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing de correo corporativo	
Alerta de seguridad cibernética	8FPH20-00234-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Mayo de 2020
Última revisión	28 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://accoutadmindoutloo.wixsite[.]com/outlook	
IP	
[62.153.78.18]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00234-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00234-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por entrega de beneficio estatal	
Alerta de seguridad cibernética	8FPH20-00235-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Mayo de 2020
Última revisión	29 de Mayo de 2020
Indicadores de compromiso	
URL	
https[:]//bit[.]ly/3gBfrLq?l=www[.]bancoestado[.]cl	
http://www[.]bancoestado-cl[.]loughgallpresbyterian[.]co[.]uk/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
[82.165.40.146]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00235-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00235-01.pdf	

Imagen del mensaje

CSIRT advierte phishing bancario por abono de beneficio	
Alerta de seguridad cibernética	8FPH20-00236-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Junio de 2020
Última revisión	03 de Junio de 2020
Indicadores de compromiso	
URL	
hxxp://bigforum[.]in/js/enviar.php?l=589944743	
http://bizitsystem[.]com/_Pensiones/www.bancoestado.cl	
IP	
[45.236.131.160]	
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	

Malware

CSIRT advierte malware por facturación electrónica	
Alerta de seguridad cibernética	2CMV20-00066-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Mayo de 2020
Última revisión	28 de Mayo de 2020
Indicadores de compromiso	
URL	
hxxps://dispaross.nserviciosprontos.com[.]br/mkt	
hxxp://www.richmondtech.co[.]uk/lib/jquery/bixix/?counter	
hxxp://40.83.77[.]255/clucs/UMN8CR12804801[.]pen	
IP	
[52.138.98.85]	
[52.147.1.153]	
[13.67.68.75]	
[52.147.29.233]	
[51.144.118.115]	
[52.147.5.183]	
[52.236.176.139]	
[52.179.101.150]	
[104.215.150.53]	
[40.86.98.155]	
[104.215.46.64]	
[104.215.10.50]	
[52.141.36.232]	
Otros IOCs del informe:	
13 sender; 8 Hash	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00066-01/	
https://www.csirt.gob.cl/media/2020/05/2CMV20-00066-01.pdf	

CSIRT advierte malware por facturación electrónica	
Alerta de seguridad cibernética	2CMV20-00067-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Junio de 2020
Última revisión	03 de Junio de 2020
Indicadores de compromiso	
URL	
hxxps://www.hosaa[.]com/main/wp-content/themes/twentyeleven/languages/00100299019301/0901902A009192390B009901C9901/index1.php,	
hxxps://www3.ufrb.edu[.]br/lehrb/wp-content/themes/twentyeleven/colors/002145987879845456/indexx2.php	
hxxp://191.232.53.216/007/0099012A00109293190B001092301H0901238JA12[.]sadia	
5 tipos de hash	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00067-01/	
https://www.csirt.gob.cl/media/2020/06/2CMV20-00067-01.pdf	

Vulnerabilidades

CSIRT comparte actualizaciones liberados por Mozilla	
Alerta de seguridad cibernética	9VSA20-00229-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Junio de 2020
Última revisión	01 de Junio de 2020
CVE	
CVE-2020-12404	
Fabricante	
Mozilla	
Producto afectado	
Todas las versiones de Mozilla Firefox para el sistema operativo iOS.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00229-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00229-01.pdf	

CSIRT comparte actualizaciones liberadas por VMWare	
Alerta de seguridad cibernética	9VSA20-00230-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Junio de 2020
Última revisión	02 de Junio de 2020
CVE	
CVE-2020-3956 - CVE-2020-3957 CVE-2020-3958 - CVE-2020-3959	
Fabricante	
VMWare	
Producto afectado	
Fusion versión 11.x para OS X. VMRC versión 11.x y anteriores para OS X en Mac. Horizon Client versión 5.x y anteriores para OS X en Mac.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00230-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00230-01.pdf	

CSIRT comparte actualizaciones liberadas por Apple para sus productos	
Alerta de seguridad cibernética	9VSA20-00231-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de Junio de 2020
Última revisión	02 de Junio de 2020
CVE	
CVE-2020-3956	
Fabricante	
Apple	
Producto afectado	
Apple Watch Series 1 y posteriores Apple TV 4K y Apple TV HD macOS High Sierra 10.13.16 macOS Catalina 10.15.5 iPhone 6s y posteriores iPad Air 2 y posteriores iPad Mini 4 y posteriores iPod Touch 7th generation	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00231-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00231-01.pdf	

CSIRT comparte actualizaciones liberadas por Mozilla	
Alerta de seguridad cibernética	9VSA20-00232-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Junio de 2020
Última revisión	03 de Junio de 2020
CVE	
CVE-2020-12399 - CVE-2020-12405 - CVE-2020-12406 CVE-2020-12407 - CVE-2020-12408 - CVE-2020-12409 CVE-2020-12410 - CVE-2020-12411	
Fabricante	
Mozilla	
Productos afectados	
Mozilla NSS entre las versiones 3.40.x y 3.52.x. Firefox desde la versión 60.0 hasta la 76.0.1. Firefox ESR desde la versión 60.0 hasta la 68.8.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00232-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00232-01.pdf	

CSIRT comparte actualizaciones liberadas por Google para Chrome	
Alerta de seguridad cibernética	9VSA20-00233-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Junio de 2020
Última revisión	03 de Junio de 2020
CVE	
CVE-2020-6493 CVE-2020-6494 CVE-2020-6495 CVE-2020-6496 CVE-2020-6497 CVE-2020-6498	
Fabricante	
Google	
Producto afectado	
Google Chrome desde la versión 83.0.4103.0 hasta la 83.0.4103.96.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00233-01/	
https://www.csirt.gob.cl/media/2020/06/9VSA20-00233-01.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
164.132.91.99	Port Scan	69.162.109.106	Port Scan
80.82.64.127	Port Scan	185.143.75.81	Port Scan
193.187.116.29	Port Scan	51.83.171.11	Port Scan
91.199.118.138	Port Scan	51.83.171.15	Port Scan
181.40.113.250	Port Scan	37.49.226.183	Port Scan
185.200.118.89	Port Scan	181.214.91.29	Port Scan
162.243.136.113	Port Scan	194.180.224.93	Port Scan
178.128.59.172	Port Scan	209.126.10.229	Port Scan
198.108.67.27	Port Scan	45.143.220.233	Port Scan
184.105.139.69	Port Scan	185.200.118.70	Port Scan
216.218.206.82	Port Scan	178.62.47.158	Port Scan
184.105.139.76	Port Scan	103.138.109.221	Port Scan
74.82.47.51	Port Scan	156.96.119.148	Port Scan
74.82.47.39	Port Scan	156.96.58.108	Port Scan
74.82.47.35	Port Scan	185.200.118.72	Port Scan
74.82.47.34	Port Scan	208.100.26.241	Port Scan
185.142.236.35	Port Scan	208.100.26.228	Port Scan
184.105.139.73	Port Scan	60.248.213.66	Port Scan
74.82.47.53	Port Scan	185.200.118.41	Port Scan
164.52.24.182	Port Scan	37.10.127.13	Port Scan
184.105.139.69	Port Scan	23.237.44.122	Port Scan
51.81.137.147	Port Scan	162.243.136.230	Port Scan
185.200.118.80	Port Scan	37.49.226.40	Port Scan
45.220.68.91	Port Scan	185.200.118.89	Port Scan
178.32.70.241	Port Scan	157.52.193.95	Port Scan
206.189.117.83	Port Scan	157.52.193.81	Port Scan
175.183.71.74	Port Scan	157.52.193.121	Port Scan
45.143.220.13	Port Scan	167.172.63.56	Port Scan
198.199.115.134	Port Scan	142.93.150.6	Port Scan
68.183.170.114	Malware	64.225.69.55	Port Scan
93.174.89.20	Port Scan	193.118.53.194	Port Scan
185.153.196.226	Port Scan	128.199.59.238	Port Scan
80.82.77.132	Port Scan	128.199.232.80	Port Scan
94.102.51.95	Port Scan	162.243.136.158	Port Scan
128.14.180.102	Port Scan	162.243.136.194	Port Scan

102.68.86.54	Port Scan	45.143.220.112	Port Scan
162.243.136.169	Port Scan	162.243.136.71	Port Scan
51.255.109.163	Port Scan	62.171.152.76	Port Scan
54.36.149.6	Port Scan	201.149.75.18	Port Scan
92.118.160.37	Port Scan	183.134.104.146	Port Scan
113.161.25.243	Port Scan	45.143.220.112	Port Scan
185.183.107.147	Port Scan	77.247.109.40	Port Scan
54.36.148.89	Port Scan	176.221.123.87	Port Scan
185.153.196.126	Port Scan	159.65.163.234	Port Scan
45.89.175.110	Port Scan	45.56.106.179	Port Scan
45.148.121.42	Port Scan	157.52.193.110	Port Scan
51.68.181.121	Port Scan	157.52.193.91	Port Scan
37.49.226.58	Port Scan	220.158.216.132	Spam
162.243.136.45	Port Scan	103.89.88.109	Port Scan
185.107.80.34	Port Scan	167.99.110.189	DDoS
159.65.106.138	Port Scan	147.75.83.239	Port Scan
162.243.136.216	Port Scan	192.87.30.47	Port Scan
77.247.110.171	Port Scan	5.182.210.97	Port Scan
5.182.210.99	Port Scan	213.186.33.17	Spam
180.214.238.74	Port Scan	162.243.136.62	Port Scan
199.201.110.206	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.

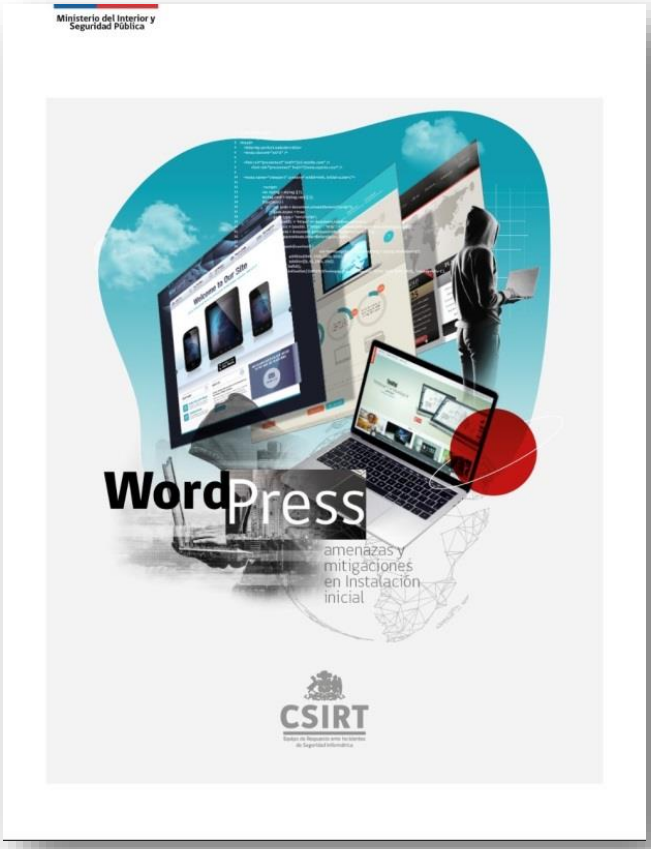
Investigación

WordPress: Amenazas y mitigaciones en instalación inicial

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la sexta edición de su publicación sobre amenazas cibernéticas el que analiza algunos riesgos y mitigaciones en el sistema de gestión de contenidos WordPress. Este artículo que fue elaborado por Juan Moraga Andrades, analista de nivel 2 de CSIRT.

Este gestor de contenido o CMS, es una aplicación de software diseñado para que una persona pueda crear y administrar contenidos en sitios web sin la necesidad de tener conocimientos previos en programación.

WordPress es el CMS más utilizado a nivel global. Este artículo examina este aplicativo desde el punto de vista de las amenazas que puede enfrentar en su instalación, así como las respectivas medidas de mitigación.



Ver en: https://www.csirt.gob.cl/reportes/an2-2020-06/

Actualidad

Los resultados de la Encuesta Nacional Urbana de Seguridad Ciudadana (ENUSC) mide, entre otras cosas, la criminalidad, violencia e inseguridad en el ciberespacio. La reciente muestra revela un incremento del 0,4% en delitos de estafa por internet, situándola en un 2% ocurrencia. El mismo porcentaje de aumento presentaron los casos de suplantación de identidad, llegando al 1,6%.

CSIRT coparte algunos ciberconsejos para evitar ser víctima de estos delitos informáticos a través de la siguiente campaña.

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.

- Manuel González
  Linkedin:
  https://www.linkedin.com/in/manuel-gonz%C3%A1lez-mart%C3%ADnez-04009676/
- Eduardo Flores
  Linkedin:
  https://www.linkedin.com/in/eduardo-flores-saavedra-4ab82142/
- Guillermo Ortiz
  Linkedin:
  https://www.linkedin.com/in/guillermo-ortiz-2456a9113/
- Joaquín Morales
  Twitter: @Joaquin11802683
- Sebastián Romero
  Linkedin:
  https://www.linkedin.com/in/sebastian-r-data-integrity/