



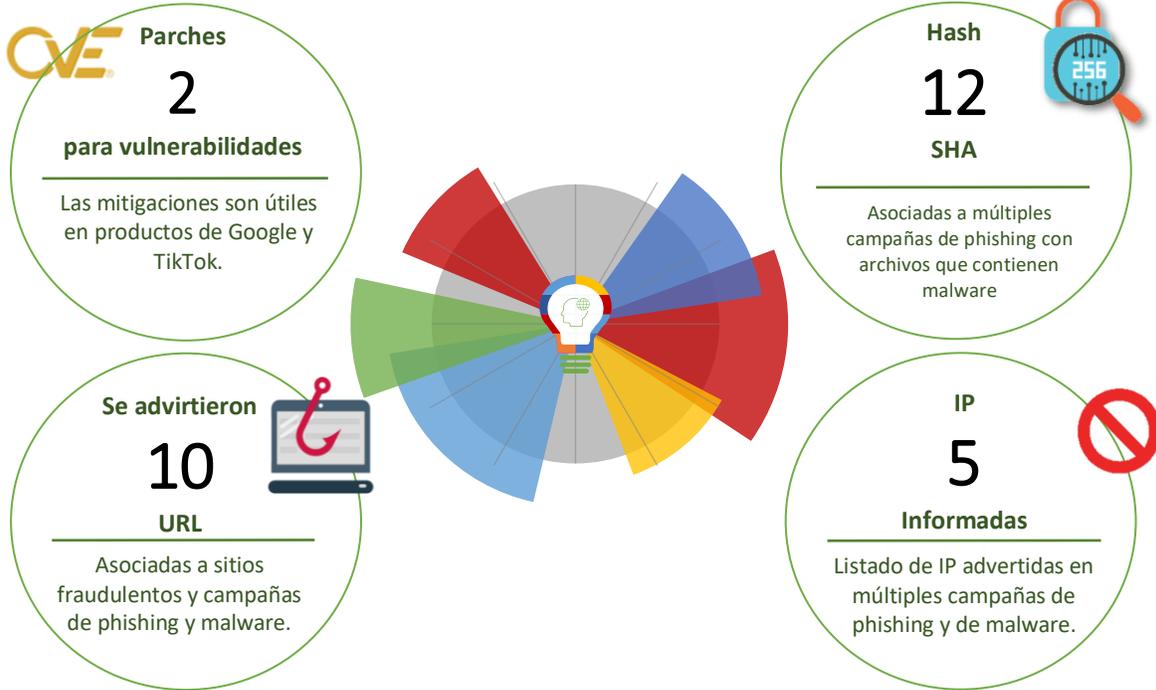
09-09-2022 | Año 4 | N°166

Boletín de Seguridad Cibernética

Semana del 2 al 8 de
septiembre de 2022



La semana en cifras



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

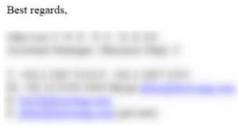
Contenido

Malware.....	2
Phishing	5
Vulnerabilidades	8
Actualidad.....	9
Muro de la Fama	12

Malware

Imagen del mensaje

FM : DOOYANG LIMITED
 RE: PORT INQUIRY - DISCH 13,000 MT SUGAR IN BULK
 GOOD DAY.
 PLEASE NOTE THAT WE ARE STUDYING TO DISCH 13,000 MT SUGAR IN BULK.
 IN THIS REGARDS, IT WOULD BE HIGHLY APPRECIATED TO ADVISE PORT INFORMATION WITH EST PL
 1) DISCH RATE & METHOD - AVERAGE RATE PER DAY - AVERAGE NUMBER OF HOURS ALL UNGED - B
 OR VSL'S GEAR? - WORKING 24 HOURS? * DAYS A WEEK? - ANY OFFICIAL PORT POLICY?
 2) ESTIMATED PORT DISBURSEMENT
 AIMING TONNAGE
 3) PORT RESTRICTION - DRAFT/AIR DRAFT/LOA/BEAM AND ETC - ALLOWANCE FOR NIGHT NAVIGATIO
 OR NOT? (IF YES, PLS PROVIDE TIDE TABLE)
 4) ESTIMATED BERTH CONDITIONS - AVERAGE WAITING TIME TO BERTH THESEDAYS - BERTHING LNS
 TODAY FOR CHECKING CONGESTION. - SHIPPERS & BERTH NAME AND PRIVATE OR PUBLIC OWNED?
 5) ANY HELPFUL INFORMATION FOR SMOOTH/FAST OPERATION. - BUNKER AVAILABILITY AND METH
 BY TRUCK?) - POSSIBLE TO BUNKER DURING CARGO WORKING? OR SHIFTING TO BUNKERING BERTH
 - FRESH WATER AVAILABILITY AND COST. - SHORE CRANE AVAILABILITY AND COST. - WEATHER CO
 THESEDAYS.
 APPRECIATED FOR YOUR PROMPT REPLY.



CSIRT alerta ante campaña de phishing con falso documento de envío de azúcar

Alerta de seguridad cibernética	2CMV22-00339-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de septiembre de 2022
Última revisión	5 de septiembre de 2022

Indicadores de compromiso

Asunto

PORT INQUIRY – DISCH 13,000 MT SUGAR IN BULK

Correo de salida

biz2@dooyang.com

SHA256

Nombre: VESSEL DETAILS.rar

SHA256:

c3884392d9ee916af8672000bb52de3af529eebf3b3db134a8fac666b571ffe8

Nombre: VESSEL DETAILS.exe

SHA256:

36e87dac79bfc21ce7aa9441977aff6b16c3f654685b1000cbf037a90c26d3

Nombre: COVID-19 Instructions to Agents Updated.docx

SHA256:

98219120ee952bdc7b7dbf8e6ce0eff28c42fd5dd4df4e33b582b833fde37101

Command and Control

https://api.telegram.org/bot1897716112:AAEAtOckOV8umHBB93Og24bkilidUKReGK44/sendMessage?chat_id=1745211648

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00339-01/>

<https://www.csirt.gob.cl/media/2022/09/2CMV22-00339-PH-01.pdf>

Imagen del Mensaje



CSIRT alerta ante campaña de phishing que suplanta a la Universidad de Chile

Alerta de seguridad cibernética	2CMV22-00340-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de septiembre de 2022
Última revisión	5 de septiembre de 2022

Indicadores de compromiso	
Asunto	
Re: Solicitud de oferta (UNIVERSIDAD DE CHILE) Proyecto UDC89454/CL4673	
Correo de Salida	
ngsw@unigroup.my	
SHA256	
Nombre:	Solicitud de oferta.rar
SHA256:	e7e2aae9553a22a73d7d60f79cc1e0a42a05dce3d1c93ac3fc0b124ec4079f3d
Nombre:	Solicitud de oferta.exe
SHA256:	09b217e890928c11da68ee319a9af44e3a3078fee93f64bb8a61d94c98dc0051
Nombre:	LpVA.exe
SHA256:	a87606c6b802d9bc7fc4c9c39b3191698b6599f1a7b6336349bf479887448b63
Command and Control	
http://162.213.249[.]190/?Y8nalJQXC4cNDqmmYx1iS34FS7Rj1IspTN8KE5	
http://kbfvzoboss.bid/alien/fre[.]php	
http://alphastand.trade/alien/fre[.]php	
http://alphastand.win/alien/fre[.]php	
http://alphastand.top/alien/fre[.]php	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00340-01/	
https://www.csirt.gob.cl/media/2022/09/2CMV22-00340-PH-01.pdf	

Imagen del mensaje

Estimado amigo,

Según su solicitud de correo electrónico a continuación, encuentre una copia adjunta de la factura proforma, así como nuestra información bancaria para el procesamiento de su pago.

Saludos cordiales.



CSIRT alerta ante campaña de phishing que incluye malware de tipo remcos

Alerta de seguridad cibernética	2CMV22-00341-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de septiembre de 2022
Última revisión	5 de septiembre de 2022

Indicadores de compromiso	
Asunto	
RE: Nota de aviso de pago del 01.09.2022	
Correo de Salida	
sales@g-watches.top	
SHA256	
Nombre:	Proforma y Nota de Aviso de Pago del 09.02.2022.arj

SHA256:
b8e26dae8ebecb68bb5f2321c22fc7e2d8d52af9ccbeb8ab1537ab445c56f2dc

Nombre: Proforma y Nota de Aviso de Pago del 09.02.2022.exe
SHA256:
4d22a6c1435795fa8f394d5c7999a9de0f7eb280b7233f95a17deb46904a7ed4

Nombre: VsDH.exe
SHA256:
f4e4d5dc13f3ef4c2144d41b2cf0f26e7ba59211236e12a75c039e0039621145

Command and Control

65.21.9[.]53:1104

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00341-01/>

<https://www.csirt.gob.cl/media/2022/09/2CMV22-00341-PH-01.pdf>

Imagen del Mensaje

Buenos días.

Adjunto una solicitud de cotización para su atención.

Esperamos su respuesta.

Saludos



CSIRT alerta ante nueva campaña de phishing que suplanta a empresa eléctrica

Alerta de seguridad cibernética	2CMV22-00342-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de septiembre de 2021
Última revisión	7 de septiembre de 2021

Indicadores de compromiso

Asunto

SOLICITUD DE COTIZACIÓN

Correo de Salida

mario.medrano@electricadepesa.com

SHA256

Nombre: Solicitud de cotización.zip
SHA256:9f736d4b1ed50c1137307bcc8eb2b29066bd216b6c9ec871fc61dc5033a3ed8

Nombre: UgjfJCiDli0PgJa.exe
SHA256:0874a3e74491ccd057bd23bf3b51b243d35110925f8da42de4277b5209ad36d9

Nombre: ZgVkfQjf.exe
SHA256:ca4428f3d8b491ea334a9f333aa685c1e8221a0be7fa19fd49dc89c65288252

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00342-01/>

<https://www.csirt.gob.cl/media/2022/08/2CMV22-00342-PH-01.pdf>

Phishing

Imagen del mensaje



BancoEstado

Estimado Cliente:

BancoEstado le comunica que su acceso a la banca en línea por internet expiró de manera temporal, por lo que su cuenta procedió a estar **DESHABILITADO** hasta la correcta verificación de sus datos como medida de seguridad.

Realizando este proceso de validación, su cuenta será activada obteniendo los beneficios y el acceso de la banca en línea por internet y de nuestra App BancoEstado.

Recordarle que solo tiene 24 horas de plazo disponible para realizar este proceso de seguridad que le brinda nuestra entidad. De no proceder con la corrección de sus datos, su cuenta será suspendida y tendrá que apersonarse a la sucursal más cercana de nuestra entidad para su verificación respectiva. BancoEstado nos preocupamos por tu Seguridad.

[Verificar Datos](#)

FALSO

CSIRT alerta ante nueva campaña de phishing que suplanta al BancoEstado

Alerta de seguridad cibernética	8FPH22-00583-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de septiembre de 2022
Última revisión	6 de septiembre de 2022

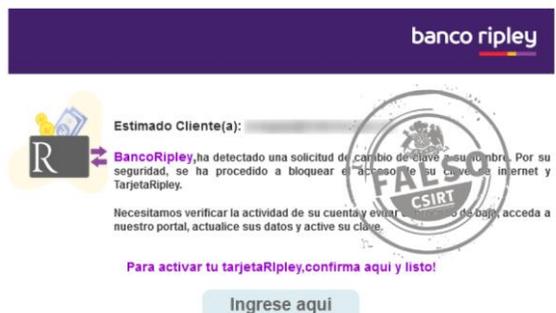
Indicadores de compromiso

URL sitio redirección	https://talkainversiones[.]com/consulta/cuenta-khbq/
URL sitio falso	https://s3rvicu4ck[.]com/mkrbgdh/pagina/imagenes/comun2008/banca-en-linea-personas.html
IP	[138.128.188.146]

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/8fph22-00583-01/
https://www.csirt.gob.cl/media/2022/09/8FPH22-00583-01.pdf

Imagen del mensaje



banco ripley

Estimado Cliente(a):

BancoRipley, ha detectado una solicitud de cambio de clave en su nombre. Por su seguridad, se ha procedido a bloquear el acceso por internet y TarjetaRipley.

Necesitamos verificar la actividad de su cuenta y evitar que alguien más pueda acceder a nuestro portal, actualice sus datos y active su clave.

[Para activar tu tarjetaRipley, confirma aquí y listo!](#)

[Ingrese aquí](#)

FALSO

CSIRT alerta ante nueva campaña de phishing que suplanta al Banco Ripley

Alerta de seguridad cibernética	8FPH22-00584-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de septiembre de 2022
Última revisión	6 de septiembre de 2022

Indicadores de compromiso

URL sitio redirección	https://bit[.]ly/3QlxBNh?l=www.bancoripley.cl
URL sitio falso	https://oleificiolama[.]jit/wp-includes/certificates/enviar.php?l=1318458817
URL sitio falso	http://beehive-order.transact.net[.]ru/activacion/cuenta-zsfp/

URL sitio falso	https://web.bancoripleycl.muraridasbabajj[.]org/1661432937/login
IP	[96.127.183.234]

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/8fph22-00584-01/
https://www.csirt.gob.cl/media/2022/09/8FPH22-00584-01.pdf

Imagen del mensaje



BancoEstado

Estimado Cliente:

BancoEstado le comunica que su acceso a la banca en línea por internet expiró de manera temporal, por lo que su cuenta procedió a estar **DESABILITADO** hasta la correcta verificación de sus datos como medida de seguridad.

Realizando este proceso de validación, su cuenta será activada obteniendo los beneficios y el acceso de la banca en línea por internet de nuestro BancoEstado.

Recordarle que solo tiene 24 horas de plazo disponible para realizar este proceso de seguridad que le brinda nuestra entidad bancaria. De no proceder con la corrección de sus datos, su cuenta será suspendido y tendrá que apersonarse a la sucursal más cercana de nuestra entidad para su verificación respectiva. BancoEstado nos preocupamos por tu Seguridad.

[Verificar Datos](#)

Desde la App es más fácil
Actívala con tu Clave de Cajero Automático

Encuétrala en:  

www.bancoestado.cl

Atentamente, BancoEstado.

CSIRT alerta phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00585-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de septiembre de 2022
Última revisión	6 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	https://depart.digitalnoticias.com[.]mx/activacion/cuenta-wzer/
URL sitio falso	https://chictware[.]com/cl0r0xp4/pagina/imagenes/comun2008/banca-en-linea-personas.html
IP	[98.142.102.50]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00585-01/
	https://www.csirt.gob.cl/media/2022/09/8FPH22-00585-01.pdf

Imagen del mensaje

Please find attached confirmation of payment made by our financial department. Kindly check your bank account details and reply to me for confirmation. Please handle accordingly. Regards



CSIRT alerta por campaña de phishing con falso documento de pago	
Alerta de seguridad cibernética	8FPH22-00586-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de septiembre de 2022
Última revisión	6 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	C:\Users\%Usuario%\Desktop\paymentadvise.xml
URL sitio falso	https://ismyschool.net/wp-content/uploads/2017/04/incorrect-username-and-Password.jpg
IP	[145.9.168.106]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00586-01/
	https://www.csirt.gob.cl/media/2022/09/8FPH22-00586-01.pdf

Imagen del mensaje



CSIRT alerta ante una nueva campaña de phishing con falso concurso de Heineken

Alerta de seguridad cibernética	8FPH22-00587-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de septiembre de 2022
Última revisión	7 de septiembre de 2022

Indicadores de compromiso

Texto del mensaje

Sorteo Cerveza Heineken Oktoberfest 2022

URL sitio falso

[https://tinyurl4\[.\]ru/u791760121/](https://tinyurl4[.]ru/u791760121/)

IP

[104.21.84.153]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00587-01/>

<https://www.csirt.gob.cl/media/2022/09/8FPH22-00587-01.pdf>

Vulnerabilidades



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA22-00700-01
CSIRT comparte vulnerabilidad día cero en Google Chrome

PARA REGISTRAR | 1510 UN INCIDENTE | www.csirt.gob.cl



CSIRT comparte vulnerabilidad día cero en Google Chrome	
Alerta de seguridad cibernética	9VSA22-00700-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de septiembre de 2022
Última revisión	5 de septiembre de 2022
CVE	
CVE-2022-3075	
Fabricantes	
Google	
Productos afectados	
Google Chrome anteriores a la versión 105.0.5195.102.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00700-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00700-01.pdf	



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA22-00701-01
CSIRT comparte vulnerabilidad grave en la app de TikTok para Android

PARA REGISTRAR | 1510 UN INCIDENTE | www.csirt.gob.cl



CSIRT comparte vulnerabilidad grave en la app de TikTok para Android	
Alerta de seguridad cibernética	9VSA22-00698-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de septiembre de 2022
Última revisión	5 de septiembre de 2022
CVE	
CVE-2022-28799	
Fabricantes	
TikTok	
Productos afectados	
App de TikTok para Android.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00701-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00701-01.pdf	

Actualidad

Inscripciones abiertas para la quinta edición del Cyberwomen Challenge Chile 2022

La Organización de los Estados Americanos (OEA), en conjunto con el Ministerio del Interior, a través del CSIRT de Gobierno, y Trend Micro, realizará una nueva versión del Cyberwomen Challenge en Chile el próximo 27 de septiembre.

En relación con este evento, el subsecretario del Interior, Manuel Monsalve, asegura: “Como Gobierno estamos comprometidos con las mujeres en mejorar los distintos aspectos de su vida, y en ese contexto el ámbito profesional es, por supuesto, un aspecto extremadamente relevante. Por eso, este año volvemos a llevar a cabo este Cyberwomen Challenge en conjunto con la OEA, una competencia de ciberseguridad exclusivamente para mujeres, donde tendrán la oportunidad de profundizar ciertos conocimientos y ponerlos en práctica. Con esto, esperamos motivar a más mujeres a estudiar y formar parte de esta industria”.



The graphic features logos for Trend Micro, OEA, Canada, Citi, Chile, and CSIRT at the top. The main text reads "OEA CYBERWOMEN CHALLENGE" in large white letters, with "5ta EDICIÓN ONLINE 2022" in a red banner below it. Underneath, it says "CHILE". The event date and time are listed as "27 de septiembre 2022" and "9:30 am a 4:00 pm". At the bottom, it states "Con el apoyo de" followed by logos for AWS and WOMCY.

El reto consiste en un taller técnico online de 6 horas estilo “captura la bandera”, en el que las participantes deberán analizar y procesar incidentes de seguridad a través de casi 49 banderas en equipos para lograr el mayor número de aciertos. La actividad es organizada por la OEA y Trend Micro, con el apoyo de Amazon Web Services y Womcy.

Más información e inscripciones:

https://resources.trendmicro.com/CyberwomenChallenge_2022.html

Ciberdiccionario Volumen 16

Tras una semana sin un nuevo volumen del Ciberdiccionario, volvemos hoy con más términos relacionados de cerca con la labor de ciberseguridad. Esperamos que les sean de utilidad. Pueden ver la campaña también aquí: csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-16/.



Ciber diccionario

Máquina virtual (virtual machine o VM): Recurso que se comporta como un computador tradicional, pero no cuenta con su propio hardware, existiendo solo como código. Así, se pueden tener varias VM (llamadas "guests") en una misma máquina física (o "host"), usando, por ejemplo, distintos sistemas operativos.



Ciber diccionario

Command and Control (C&C): El equipo de un ciberdelincuente que controla a otros distancia de forma no autorizada. Desde estos servidores C&C, los atacantes pueden ejecutar acciones en los equipos de sus víctimas, como robar información confidencial, incluso manejar una red de equipos infectados (conocida como botnet).



Ciber diccionario

Indicadores de compromiso (IoC): En ciberseguridad, se les llama así a indicios de un acceso no autorizado a un sistema, como pueden ser códigos específicos o actividades sospechosas. Si una entidad sufre un ataque, es útil que comparta con la comunidad los IoC que logra obtener, para así facilitar que otras organizaciones mejoren sus defensas.



Ciber diccionario

"pwn": Concepto proveniente del mundo de los videojuegos, se usa como verbo para describir cuando alguien es absolutamente derrotado o engañado. Viene de "owned", en inglés, ser dominado por alguien más. Así, también se usa informalmente al lograr acceso no autorizado a un sistema (cuyos dueños fueron "pwnd" o "pwn3d" por el atacante).



Recomendaciones y buenas prácticas

- 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.



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 del Estado, **al informar campañas de phishing, malware y/o sitios fraudulentos.**

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (<https://www.csirt.gob.cl> o al teléfono **1510** siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Juan Patricio Correa Poblete
- Francisco Flefil
- Mathias Roco Fernández
- Mauricio Hanglin
- Jair Palma
- Jorge Garrido
- Mathias Dannenberg

