CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 186

Semana del 20 al 26 de enero

PARCHES COMPARTIDOS

9

Las mitigaciones son útiles en productos de Google y VMware.

IP INFORMADAS

17

Listado de IP advertidas en múltiples campañas de phishing y de malware.

URL ADVERTIDAS

30

Asociadas a sitios fraudulentos y campañas de phishing y malware

HASH REPORTADOS

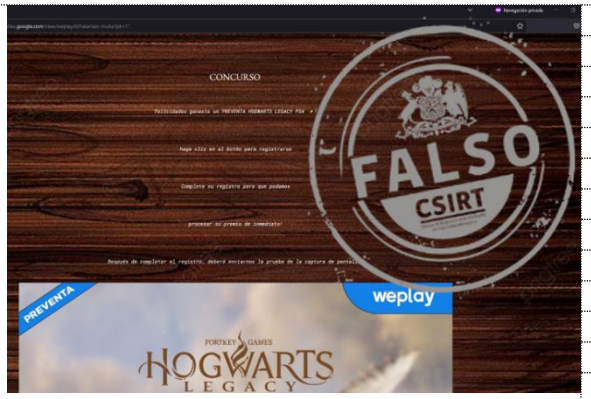
9

Asociadas a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

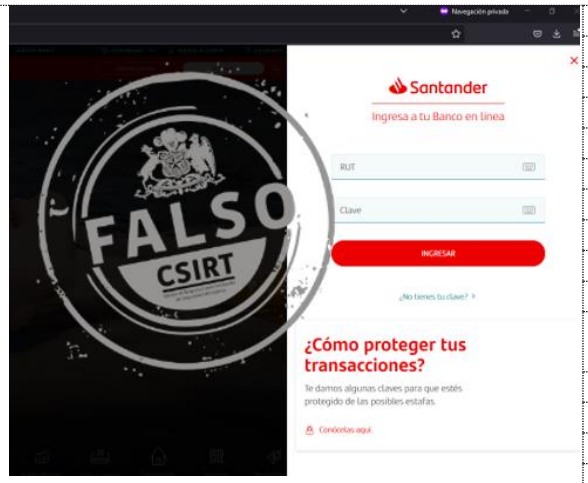
1. Sitios fraudulentos



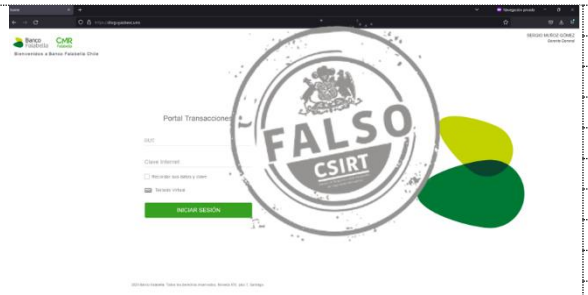
CSIRT alerta de página fraudulenta que suplanta a WePlay	
Alerta de seguridad cibernética	8FFR23-01201-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2023
Última revisión	23 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//sites.google[.]com/view/weplaycll/halaman-muka?pli=1%22	
Dirección IP	
[209.85.145.101]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01201-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01201-01.pdf	

CSIRT alerta de sitio fraudulento que suplanta al Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01202-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2023
Última revisión	23 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//autoservis-cmr.firebaseapp[.]com/oportunidades?22536528337245feonp	
Dirección IP	
[199.36.158.100]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01202-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01202-01-1.pdf	

CSIRT alerta de una página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR23-01203-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2023
Última revisión	24 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//ucmstudio[.]info/cuentas/cuenta-test/ https[:]//surfsantnder[.]info/pagina/login.asp	
Dirección IP	
[98.142.101.90]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01203-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01203-01.pdf	

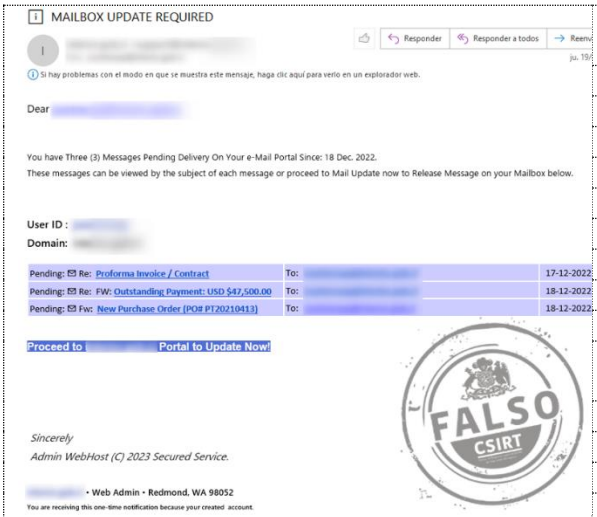


CSIRT alerta de una página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR23-01204-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2023
Última revisión	25 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//bamco-samtander.cl-sns[.]top/1674652583/portada/personas/home.asp	
Dirección IP	
[104.21.94.40]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01204-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01204-01.pdf	

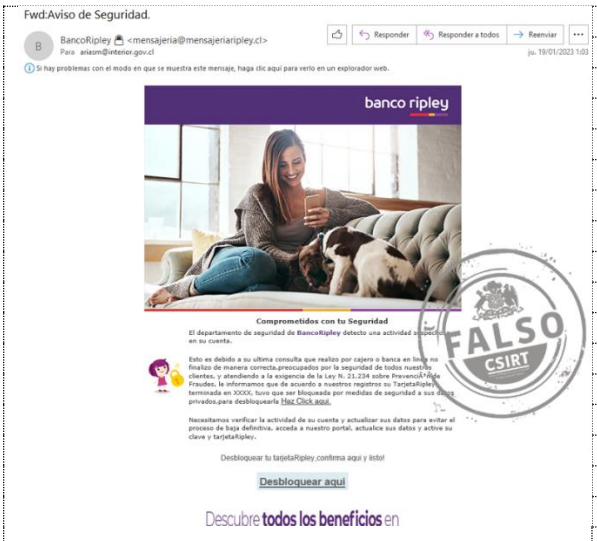


CSIRT alerta de página fraudulenta que suplanta al Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01205-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2023
Última revisión	25 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//dioguyasbexc[.]uno/	
Dirección IP	
[193.84.177.245]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01205-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01205-01.pdf	

2. Phishing

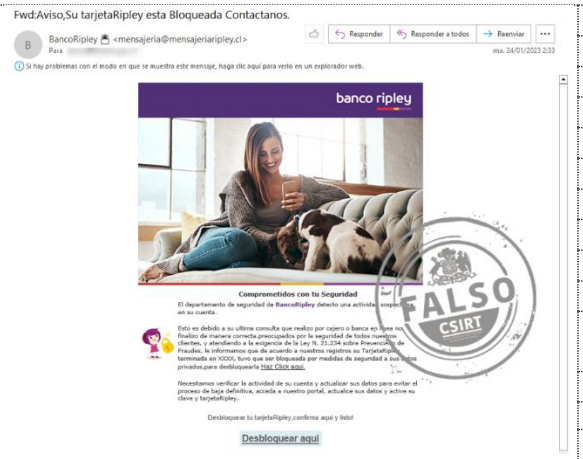


CSIRT alerta de campaña de phishing que suplanta página de login de servicio de correo electrónico	
Alerta de seguridad cibernética	8FPH23-00723-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2023
Última revisión	19 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//ipfs.io/ipfs/QmYaBZcHBefdcsjopwYGtWL7AewUkPPVdTgWXoFfwtQumE?filename=oglogz113_cham-e.html#test@csirt.gob.cl	
Dirección IP	
[209.94.90.1]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00723-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00723-01.pdf	



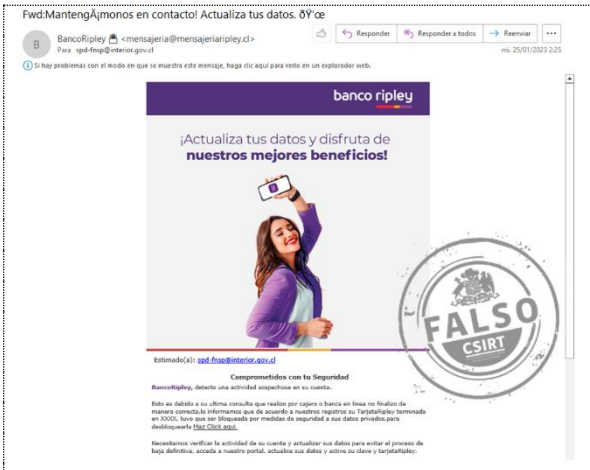
CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00724-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2023
Última revisión	24 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3HfNI2m?l=www.bancoripley.cl	
URL sitio falso	
http[:]//web.bancoripley.cl.archersbodyworks[.]com.au/1673873742/login	
Dirección IP	
[185.45.66.125]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00724-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00724-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00725-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2023
Última revisión	24 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//t[.]co/wkUrLb38TS https[:]//sodisisperu[.]com/cl/?index=index	
Dirección IP	
[199.188.200.254]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00725-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00725-01.pdf	



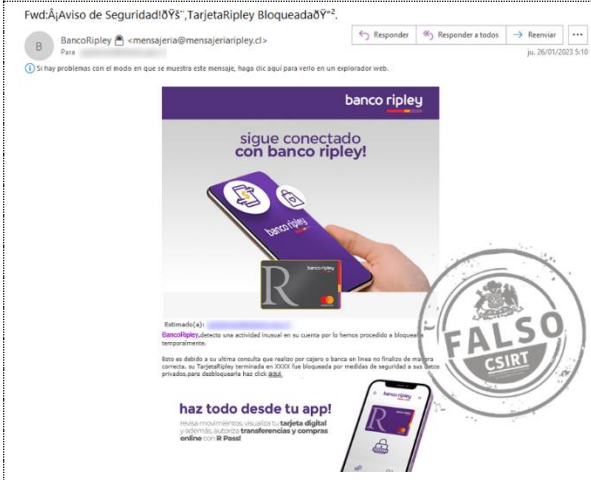
CSIRT alerta de nueva campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00726-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2023
Última revisión	24 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit.ly/3kzUC9N?l=www.bancoripley.cl https[:]//sam-tech[.]jp/bancoripley/cuenta-ktfs/	
URL sitio falso	
https[:]//web.bancoripley.cl.gkmayprop[.]com/1674566614/login	
Dirección IP	
[130.51.180.17]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00726-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00726-01.pdf	

CSIRT alerta de nueva página de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00727-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2023
Última revisión	24 de enero de 2023
Indicadores de compromiso	
URL sitio redirección	
https[:]//contalaserena[.]net/activacion/cuenta-kppf/	
URL sitio falso	
https[:]//xtraillconver[.]com/1674582764/imagenes/_personas/home/default.asp	
Dirección IP	
[138.128.189.154]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00727-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00727-01.pdf	



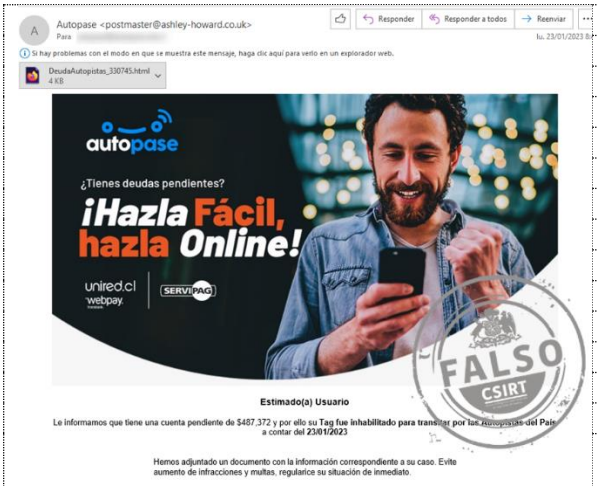
CSIRT alerta de nueva campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00728-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2023
Última revisión	25 de enero de 2023
Indicadores de compromiso	
URL sitio redirección	
https[:]//bit[.]ly/3ZVlO3b?l=www.bancoripley.cl https[:]//sam-tech[.]jp/bancoripley/cuenta-tscs/	
URL sitio falso	
https[:]//web.bancoripley.cl.gkmayprop[.]com/1674656207/login	
Dirección IP	
[130.51.180.17]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00728-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00728-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00729-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de enero de 2023
Última revisión	26 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//cartoonpuzzl3s[.]com/activacion/cuenta-vtvq/	
URL sitio falso	
https[:]//xtraillconver[.]com/1674670553/imagenes/_personas/home/default.asp	
Dirección IP	
[138.128.189.154]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00729-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00729-01.pdf	



CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00730-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de enero de 2023
Última revisión	26 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3Jl5gLU?l=www.bancoripley.cl	
URL sitio falso	
https[:]//web-bancoripley-cl.gkmayprop[.]com/1674735680/login	
Dirección IP	
[130.51.180.17]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00730-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00730-01.pdf	

3. Malware



CSIRT alerta de nueva campaña de phishing con malware, que suplanta a Autopase	
Alerta de seguridad cibernética	2CMV23-00398-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2023
Última revisión	23 de enero de 2023
Indicadores de compromiso	
Asunto	
Su tag está inhabilitado por deuda.	
Correo de Salida	
postmaster@ashley-howard.co.uk	
SHA256	
f669aba8e7621d7c21ad4553d6899311ecdff561fda86261a496a46c7604d4cc d016b039526f23dcddeeac7c511bd7ef439177541504e2998e19d7892481aa7d b753a9dc95ffc2fde9e31d8cbf7b44b59d25e393e7ad6a1effff6122011b4fef ~~ 593d0e89345ac495b7ab40fb789a51fd68c4f2f582de7c17c96f52ffa21e00e1 ~~ bb2a3bbc876eb671233d6980826be466464e7026fd3e2f71c8a825c0de2fa106 206a789ac6eaca1d44d4d89fa77d7e0407cfc9c9fcf5917ce4fc2a947328a8f 98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b b3ce811fb696b94f9117ee7fe725ae6b907d695636beceeb1672d5d5eeb81df4 https://facturasnet[.]store/?uQNaBDB6VMlMEOBOuKU4UTuOJAvdL36I6gJMHTG D	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00398-01/	
https://www.csirt.gob.cl/media/2023/01/2CMV23-00398-01.pdf	

CSIRT comparte información de vulnerabilidades parchadas por VMware para vRealize Log Insight	
Alerta de seguridad cibernética	9VSA23-00776-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de enero de 2023
Última revisión	26 de enero de 2023
CVE	
CVE-2022-31703 CVE-2022-31704 CVE-2022-31706 CVE-2022-31710 CVE-2022-31711	
Fabricantes	
VMware	
Productos afectados	
VMware vRealize Log Insight 8.x VMware Cloud Foundation (VMware vRealize Log Insight) 4.x, 3.x	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00776-01/	
https://www.csirt.gob.cl/media/2022/12/9VSA22-00776-01.pdf	

CSIRT comparte vulnerabilidades en varios productos de Juniper Networks	
Alerta de seguridad cibernética	9VSA23-00777-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	26 de enero de 2023
Última revisión	26 de enero de 2023
CVE	
CVE-2023-0471 CVE-2023-0472 CVE-2023-0473 CVE-2023-0474	
Fabricantes	
Juniper Networks	
Productos afectados	
Google Chrome, versiones anteriores a la 109	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00777-01/	
https://www.csirt.gob.cl/media/2023/01/9VSA23-00777-01.pdf	

5. Concientización

Ciberconsejos | Día de la Protección de Datos Personales

Cada 28 de enero se celebra el Día de la Protección de los Datos Personales, y en anticipación a esta fecha, esta semana como CSIRT de Gobierno les contamos por qué es importante y cómo podemos proteger nuestra información, como parte de nuestros tradicionales #ciberconsejos.

Pueden encontrar la campaña y todas las anteriores que hemos hecho, en nuestro sitio web oficial: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-proteccion-datos-personales/.

Ciberdiccionario Volumen 27

Con los conceptos buzoneo, criptoestafa, datos abiertos e infostealer, presentamos la edición 27 de nuestro Ciberdiccionario. Esperemos que les sea útil y junto con los anteriores volúmenes de este compendio de definiciones en continua expansión les permita relacionarse con mayor facilidad con el mundo de la tecnología y la ciberseguridad.

Enlace: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-27/

6. 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 que los sitios web a los que se ingrese sean los oficiales.

7. 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.

- Daniza Irene Mesa Vega
- Cristián Venegas