23-07-2020 | Año 2 | N°55

Boletín de Seguridad Cibernética

Semana del 16 al 22 de julio 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

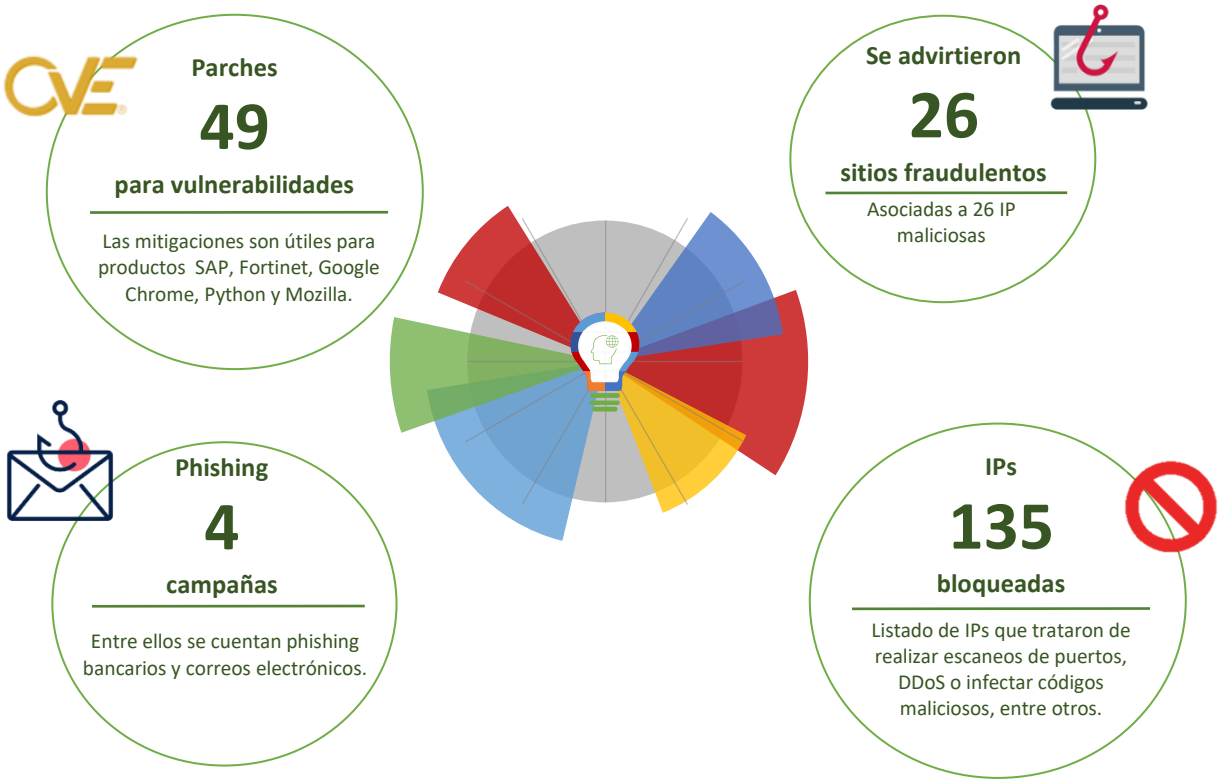
División de Redes y Seguridad Informática.

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 informa de portal fraudulento que suplanta sitio bancario	
Alerta de seguridad cibernética	8FFR20-00508-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Julio de 2020
Última revisión	16 de Julio de 2020
Indicadores de compromiso	
URL	
www-bancoestado-cl[.]bongtannet[.]com	
IP	
185[.]150[.]191[.]224	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00508-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00508-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00509-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Julio de 2020
Última revisión	16 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]www-bancoestado[.]cl[.]k-tech[.]co[.]ke	
IP	
23[.]235[.]198[.]112	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00509-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00509-01.pdf	

Imagen del sitio

CSIRT advierte de suplantación de sitio bancario para uso fraudulento	
Alerta de seguridad cibernética	8FFR20-00510-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Julio de 2020
Última revisión	16 de Julio de 2020
Indicadores de compromiso	
URL	
scotiabnakchile[.]cf	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00510-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00510-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00511-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Julio de 2020
Última revisión	16 de Julio de 2020
Indicadores de compromiso	
URL	
login-bancestado[.]tk	
IP	
91[.]234[.]99[.]130	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00511-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00511-01.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta a web de bebida	
Alerta de seguridad cibernética	8FFR20-00512-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Julio de 2020
Última revisión	18 de Julio de 2020
Indicadores de compromiso	
URL	
corlive[.]net/pepsi	
IP	
160[.]153[.]133[.]171	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00512-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00512-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00513-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Julio de 2020
Última revisión	18 de Julio de 2020
Indicadores de compromiso	
URL	
banestado-login[.]gq	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00513-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00513-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario suplantado	
Alerta de seguridad cibernética	8FFR20-00514-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Julio de 2020
Última revisión	18 de Julio de 2020
Indicadores de compromiso	
URL	
banestado-login[.]ml	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00514-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00514-01.pdf	

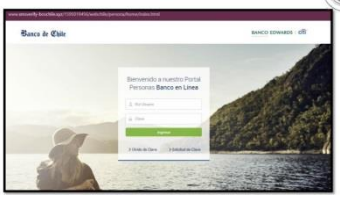
Imagen del sitio

CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00515-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Julio de 2020
Última revisión	18 de Julio de 2020
Indicadores de compromiso	
URL	
banestado-login[.]tk	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00515-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00515-01.pdf	

Imagen del sitio

CSIRT informa sobre sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00516-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Julio de 2020
Última revisión	18 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]verifysms-bchile[.]com	
IP	
162[.]0[.]232[.]43	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00516-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00516-01.pdf	

Imagen del sitio



CSIRT advierte de sitio bancario suplantado	
Alerta de seguridad cibernética	8FFR20-00517-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Julio de 2020
Última revisión	18 de Julio de 2020
Indicadores de compromiso	
URL	
smsverify-bcochile[.]xyz	
IP	
31[.]170[.]161[.]30	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00517-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00517-01.pdf	

Imagen del sitio

CSIRT advierte de un portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00518-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Julio de 2020
Última revisión	21 de Julio de 2020
Indicadores de compromiso	
URL	
norkalimpresiones[.]com/www[.]santander[.]cl/pagina/login[.]asp	
IP	
67[.]225[.]216[.]141	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00518-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00518-01.pdf	

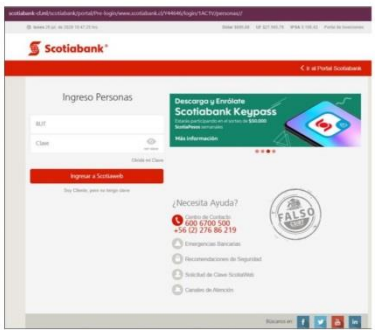
Imagen del sitio

CSIRT informa de portal de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00519-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Julio de 2020
Última revisión	21 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]eelifeinsurance[.]ca/roca/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
107[.]180[.]29[.]18	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00519-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00519-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00520-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Julio de 2020
Última revisión	21 de Julio de 2020
Indicadores de compromiso	
URL	
mechri-ts[.]com/Pensiones/www[.]bancoestado[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
162[.]251[.]80[.]14	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00520-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00520-01.pdf	

Imagen del sitio

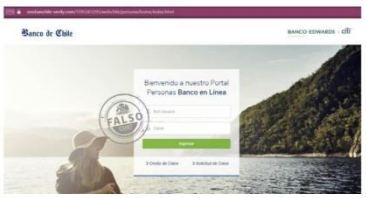


CSIRT advierte sobre sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00521-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Julio de 2020
Última revisión	21 de Julio de 2020
Indicadores de compromiso	
URL	
scotiabank-cl[.]ml	
IP	
178[.]159[.]36[.]76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00521-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00521-01.pdf	

Imagen del sitio

CSIRT informa sobre sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00522-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Julio de 2020
Última revisión	21 de Julio de 2020
Indicadores de compromiso	
URL	
wahat-apps[.]com/cmd/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
198[.]187[.]31[.]223	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00522-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00522-01.pdf	

Imagen del sitio



CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00523-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
smsbanchile-verify[.]com	
IP	
51[.]89[.]232[.]50	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00523-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00523-01.pdf	

Imagen del sitio

CSIRT advierte de web de suplantación bancaria	
Alerta de seguridad cibernética	8FFR20-00524-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
writingpup[.]com/www[.]santander[.]cl/pagina/login[.]asp	
IP	
103[.]53[.]43[.]114	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00524-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00524-01.pdf	

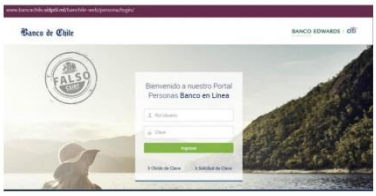
Imagen del sitio

CSIRT informa de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00525-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
wahat-apps[.]com/load/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
198[.]187[.]31[.]223	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00525-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00525-01.pdf	

Imagen del sitio

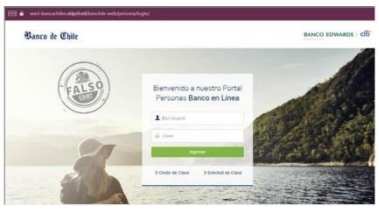
CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00526-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]barcoestado[.]co	
IP	
139[.]59[.]65[.]68	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00526-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00526-01.pdf	

Imagen del sitio



CSIRT advierte de sitio bancario de suplantación	
Alerta de seguridad cibernética	8FFR20-00527-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]bancachile[.]xn--sdpl-vpa2b[.]ml/banchile-web/persona/login/	
IP	
192[.]185[.]35[.]64	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00527-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00527-01.pdf	

Imagen del sitio



CSIRT advierte de sitio de suplantación bancario	
Alerta de seguridad cibernética	8FFR20-00528-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
ww3-bancachiles[.]xn--sdpl-vpa2b[.]ml/banchile-web/persona/login/	
IP	
216[.]239[.]36[.]21	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00528-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00528-01.pdf	

Imagen del sitio

CSIRT advierte de sitio de suplantación de streaming	
Alerta de seguridad cibernética	8FFR20-00529-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
spotifygratis[.]com	
IP	
51[.]89[.]232[.]50	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00535-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00529-01-1.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00530-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]sbiindo[.]com/test/www[.]santander[.]cl/pagina/login[.]asp	
IP	
117[.]54[.]9[.]123	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00530-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00530-01.pdf	

Imagen del sitio

CSIRT advierte sobre sitio que suplanta marca de bebida cola	
Alerta de seguridad cibernética	8FFR20-00531-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
llevate[.]ru/cocacola/lat/	
IP	
31[.]31[.]198[.]75	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00531-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00531-01.pdf	

Imagen del sitio

CSIRT advierte de sitio que suplanta servicio de streaming	
Alerta de seguridad cibernética	8FFR20-00532-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
www[.]netflix[.]clientes-suspendido-pago[.]com	
IP	
37[.]252[.]102[.]163	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00532-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00532-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00533-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Julio de 2020
Última revisión	22 de Julio de 2020
Indicadores de compromiso	
URL	
library[.]thetmm[.]org/www[.]santander[.]cl/pagina/login[.]asp	
IP	
103[.]21[.]59[.]173	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00534-01/	
https://www.csirt.gob.cl/media/2020/07/8FFR20-00533-01-2.pdf	

Phishing

Imagen del mensaje

CSIRT advierte de phishing por falso bloqueo de cuenta bancaria	
Alerta de seguridad cibernética	8FPH20-00269-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Julio de 2020
Última revisión	17 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://retopop[.]com/Activacion/cuenta-cnoe/	
IP	
[104.47.58.176]	
160.153.128.9	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00269-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00269-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por bloqueo de cuenta	
Alerta de seguridad cibernética	8FPH20-00266-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Julio de 2020
Última revisión	17 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://bit[.]ly/30n7hPw?l=www.santander[.]cl	
hxxp://www[.]invatamimpreuna[.]ro/www[.]santander[.]cl/pagina/login[.]asp	
IP	
[103.74.122.232]	
188.215.250.94	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00270-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00270-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por bloqueo de cuenta	
Alerta de seguridad cibernética	8FPH20-00271-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Julio de 2020
Última revisión	21 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://www.azadiclub[.]ir/cli/enviar.php?l=368641716	
hxxp://nezhalska[.]com/activacion/cuenta-vfdh/	
hxxps://writingpup[.]com/www.santander.cl/pagina/login.asp	
IP	
[103.74.122.232]	
103.53.43.114	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00271-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00271-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por crédito de capital de trabajo	
Alerta de seguridad cibernética	8FPH20-00272-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Julio de 2020
Última revisión	21 de Julio de 2020
Indicadores de compromiso	
URL	
hxxp://www.vitrinesdusablon[.]com/2.php	
hxxps://login-bancestado[.]ml/imagenes/comun2008/banca-en-linea-personas.html	
IP	
178.159.36.76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00272-01/	
https://www.csirt.gob.cl/media/2020/07/8FPH20-00272-01.pdf	

Malware

CSIRT alerta de múltiples campañas de Emotet activas	
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	18 de Julio de 2020
Última revisión	18 de Julio de 2020
Indicadores de compromiso	
URL	
http://tarisfotografi.com/aup/Overview/	
http://movie.cxyw.net/fork/LLC/jj0av1ems/xrgxn858627574n193e6s4zoqd2/	
http://teste.hoonicorns.pt/ddfcn41dj/payment/epwsnm/	
http://demo.xoweb.cn/static/public/yn4g1lj32bix/	
http://www.leonardoenergie.it/media/balance/	
http://watkins.mitchellpwright.com/wp-includes/docs/lg2wm6zn/sxhgff291213969722cb2tpmjwffm/	
http://linhkien36.net.co/wp-admin/browse/	
http://www.mikesar.com/cgi-bin/FILE/9iy3rbp/yc697386432801482480z1o1srx37/	
http://exchangecamp.ir/wp-admin/Documentation/	
http://www.gdstechnologies.co.in/app/eTrac/	
http://akzy.top/h8ioc8/Documentation/	
http://www.ajanews.asia/wp/Document/5r65712504026116389jmyzp09zw2b3sfn63/	
http://www.aumhealings.org/wp-admin/docs/1izhzmhbo/	
http://ulfhorror.com/wp-admin/83279465106718/7fkhh84265327972167057acuknjrmhrfbxz9bdd/	
http://steelworks-students.com/wp-admin/FILE/ype8vbeho2jn/	
http://longphuong.tk/wp-admin/browse/buz7el/	
http://pasca.fapet.ub.ac.id/l/sites/	
http://drive.medisail.fr/lib/INC/	
https://doraflob.com/fef2/Document/	
http://ranks.hoonicorns.pt/comp3/Overview/00giwvmzhy/s040549542 69w9vtvn5tqlan/	
http://www.timelyrain.top/wp-includes/ID3/parts_service/enlbnfk4xl/	
https://koncenful.com/wp-content/lm/hmhj52/ook7ri689941810111164mlk5ffuksnm6anf/	
https://daniwilkinson.co.uk/dup-installer/sites/3u01718046821pkh6l38v42wa3e1eiw/	
https://max-hoffmann-webdesign.de/eTrac/	
http://aarunya.in/wp-admin/swift/3jc4jqgai3rf/98382623658csjsmcfrnnlx032w6e9/	
http://elilaifs.cn/wp-admin/parts_service/jecxwnaz1j/	
https://gayasianporn.men/wp-includes/docs/	

http://www.calzadosyaccesorios.com/wp-content/plugins/wp-optimize/cache/balance/6uum399349075e49y7zg5lmhju/
http://misuperpodereslaprogramacion.com/wp-includes/459766/f9bk24443570nsfmvcorb3d0fs0/
http://hyundailamdong.com.vn/wp-content/LLC/z9uf09t/pf4c2866715286295d0poxdviz16wlsy8/
http://elnasr-co.com/b36ybn/parts_service/81mv7870218z8fosnwspopk3th53i4/
http://batdongsanthanhhoa.xyz/wp-admin/esp/syx8t7sa7pn/
http://benjamin-jauernig.de/bilder/parts_service/
http://mikesar.com/cgi-bin/rqag0gz/
https://kettaravision.com/wp-includes/Reporting/1g899748783160327 19mibv1xp63/
https://computerfamilie.com/wp-admin/sites/5zbl583454520034794wvuqb80aka/
https://letu8888.com/wp-admin/report/ck165923294108833875trpu7qznfted/
https://jacksinspiration.com/wp-admin/sites/2fipqcb/
http://www.joycareu.com/9re/payment/luv7f9hd/
http://zeing-kor.com/b/common_array/open_12aprkbzsnv01y_4uawa/87933126050098_FOkxEXj/
https://kompenas.org/wp-admin/open_disk/corporate_portal/ffn_tytwu1u928t/
https://kettaravision.com/wp-includes/Reporting/1g899748783160327 19mibv1xp63/
https://jacksinspiration.com/wp-admin/sites/2fipqcb/
https://www.ziyuan.tech/wp-admin/Documentation/
https://qrtalk.nl/wp-content/docs/f6k3vrc0/
http://www.mikesar.com/cgi-bin/rqag0gz/
https://hightea.tk/wp-admin/LLC/uxblj70750248131jyb5yjz51vq9r3zg0yo/
https://steer2vision.com/recurringo/Overview/t8oku994412361893ciornz3iuaysczvm/
http://akzy.top/h8ioc8/Documentation/
http://cleardristi.com/cleardristi.com_WP_INSTALL/g84oq8lq9ek_d0qdnl3l0gkrr_module/corporate_wkg55rof6x_cf5kxjphwqyz/who5_06y576/
https://ideanetsolutions.com/wp-admin/multifunctional-zone/guarded-mglbz8f9qqm-77foumy8y423bo/ZqnWyCb1ePV-yhG1xbpjL/
http://cellstore.net.br/wp-admin/protected-zone/interior-zgirj9bvpgy5ef1-0z7d5cqgj949/KL4SoBjA0s-nGbvgduN/
https://www.chinavok.com/wv7kv/multifunctional-gmgtAcb-XzR6tiFghuo/additional-gN3u1-JPwnriOV0YM/wg7hzo1jit-0sus2x/
84 tipos de hash
Otros IOCs del informe:
60 sender
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv20-00068-01/
https://www.csirt.gob.cl/media/2020/07/2CMV20-00068-01-1.pdf

Vulnerabilidades

CSIRT comparte vulnerabilidad crítica y mitigación obtenida de SAP	
Alerta de seguridad cibernética	9VSA20-00271-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Julio de 2020
Última revisión	16 de Julio de 2020
CVE	
CVE-2020-6287	
Fabricante	
SAP	
Productos afectados	
Esta vulnerabilidad está presente de forma predeterminada en las aplicaciones de SAP que se ejecutan sobre SAP NetWeaver AS Java 7.3 y cualquier versión más reciente (hasta SAP NetWeaver 7.5). Las soluciones empresariales de SAP potencialmente vulnerables incluyen cualquier solución basada en Java de SAP como (pero no limitado a): SAP Enterprise Resource Planning, SAP Product Lifecycle Management, SAP Customer Relationship Management, SAP Supply Chain Management, Gestión de relaciones con proveedores de SAP, SAP NetWeaver Business Warehouse, SAP Business Intelligence, Infraestructura móvil SAP NetWeaver, SAP Enterprise Portal, SAP Process Orchestration / Process Integration), SAP Solution Manager, Infraestructura de desarrollo de SAP NetWeaver, SAP Central Process Scheduling, SAP NetWeaver Composition Environment, y SAP Landscape Manager.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00271-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00271-01-1.pdf	

CSIRT comparte vulnerabilidades y mitigaciones obtenidas de Fortinet	
Alerta de seguridad cibernética	9VSA20-00272-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Julio de 2020
Última revisión	17 de Julio de 2020
CVE	
CVE-2004-1653 - CVE-2019-17655 - CVE-2019-9193 CVE-2019-6693 - CVE-2020-9289 - CVE-2020-12812	
Fabricante	
Fortinet	
Productos afectados	
FortiAnalyzer desde la versión 6.2.0 hasta la 6.2.3, la 6.0.8 y anteriores. FortiManager desde la versión 6.2.0 hasta la 6.2.3, 6.0.8 y anteriores. FortiAP-S/W2 versión 6.2.3 y anteriores. FortiAP-U versión 6.0.1 y anteriores. FortiOS desde la versión 6.2.0 hasta la 6.2.2, 6.0.9 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00272-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00272-01.pdf	

CSIRT comparte actualizaciones para Google Chrome	
Alerta de seguridad cibernética	9VSA20-00273-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Julio de 2020
Última revisión	17 de Julio de 2020
CVE	
CVE-2020-6510 - CVE-2020-6511 - CVE-2020-6512 CVE-2020-6513 - CVE-2020-6514 - CVE-2020-6515 CVE-2020-6516 - CVE-2020-6517 - CVE-2020-6518 CVE-2020-6519 - CVE-2020-6520 - CVE-2020-6521 CVE-2020-6522 - CVE-2020-6523 - CVE-2020-6524 CVE-2020-6525 - CVE-2020-6526 - CVE-2020-6527 CVE-2020-6528 - CVE-2020-6529 - CVE-2020-6530 CVE-2020-6531 - CVE-2020-6533 - CVE-2020-6534 CVE-2020-6535 - CVE-2020-6536	
Fabricante	
Google Chrome	
Producto afectado	
Actualizar a la versión 84.0.4147.89 de Google Chrome.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00273-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00273-01.pdf	

CSIRT comparte información obtenida de Python por vulnerabilidad tipo DDoS	
Alerta de seguridad cibernética	9VSA20-00274-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Julio de 2020
Última revisión	18 de Julio de 2020
CVE	
CVE-2020-14422	
Fabricante	
Python	
Productos afectados	
Python desde la versión 3.8.0 hasta la 3.8.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00274-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00274-01.pdf	

CSIRT comparte actualizaciones de Mozilla para Firefox y Thunderbird	
Alerta de seguridad cibernética	9VSA20-00275-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Julio de 2020
Última revisión	18 de Julio de 2020
CVE	
CVE-2020-15648 - CVE-2020-12415 - CVE-2020-12416 CVE-2020-12417 - CVE-2020-12418 - CVE-2020-12419 CVE-2020-12420 - CVE-2020-12402 - CVE-2020-12421 CVE-2020-12422 - CVE-2020-12423 - CVE-2020-12424 CVE-2020-12425 - CVE-2020-12426	
Fabricante	
Juniper	
Producto afectado	
Mozilla Firefox versiones 78 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00275-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00275-01.pdf	

CSIRT comparte vulnerabilidades y mitigaciones obtenidas de VMWare

Alerta de seguridad cibernética	9VSA20-00276-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Julio de 2020
Última revisión	18 de Julio de 2020
CVE	
CVE-2020-3973 - CVE-2020-3974	
Fabricante	
Zoom	
Producto afectado	
VeloCloud Orchestrador versiones 3.x para Linux. Fusion versiones 11.x para OS X. VMRC versiones 11.x y anteriores para OS X. Horizon Client versiones 5.x y anteriores para OS X.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00276-01/	
https://www.csirt.gob.cl/media/2020/07/9VSA20-00276-01.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:

IP	Motivo	IP	Motivo
45.148.120.31	Malware	167.71.186.157	Port Scan
59.96.244.37	Malware	45.143.223.113	Port Scan
37.228.117.90	Malware	176.126.175.20	Port Scan
107.172.141.10	Malware	37.49.224.57	Port Scan
74.207.230.187	Malware	192.241.234.207	Port Scan
107.6.183.226	Malware	192.241.233.64	Port Scan
113.160.180.109	Malware	192.241.236.232	Port Scan
46.229.168.163	Malware	23.83.129.2	Port Scan
124.156.241.52	Malware	192.241.233.180	Port Scan
207.246.99.156	Malware	192.241.211.196	Port Scan
172.67.154.24	Malware	207.180.201.180	Port Scan
122.114.105.25	Malware	156.96.156.136	Port Scan
80.82.77.4	Port Scan	192.241.234.66	Port Scan
192.241.236.169	Port Scan	198.98.62.87	Port Scan
192.241.227.179	Port Scan	134.73.71.15	Port Scan
192.241.214.107	Port Scan	23.95.50.202	Port Scan
185.53.88.113	Port Scan	161.97.87.68	Port Scan
162.243.169.57	Port Scan	192.241.233.249	Port Scan
192.241.236.86	Port Scan	108.59.0.103	Port Scan
45.143.223.114	Port Scan	192.241.222.112	Port Scan
78.138.98.6	Port Scan	176.126.175.13	Port Scan
93.174.93.45	Port Scan	67.205.160.159	Port Scan
160.153.137.99	Port Scan	198.199.94.238	Port Scan
178.32.196.220	Port Scan	192.241.236.32	Port Scan
23.90.145.34	Port Scan	94.102.56.151	Port Scan
156.96.156.142	Port Scan	108.62.103.209	Port Scan
176.126.175.12	Port Scan	95.211.120.71	Port Scan
94.102.51.209	Port Scan	138.117.99.25	Port Scan
192.241.234.103	Port Scan	37.187.146.73	Port Scan
192.241.207.236	Port Scan	45.143.220.18	Port Scan

185.153.180.203	Port Scan	39.109.233.44	Port Scan
83.97.20.164	Port Scan	91.199.118.137	Port Scan
187.198.19.70	Port Scan	88.218.17.183	Port Scan
141.164.35.240	Port Scan	149.56.164.195	Port Scan
185.153.180.172	Port Scan	37.49.230.132	Port Scan
192.241.234.43	Port Scan	62.210.83.32	Port Scan
192.241.233.115	Port Scan	158.69.6.192	Port Scan
185.132.249.232	Port Scan	77.243.191.26	Port Scan
192.241.214.102	Port Scan	185.200.118.76	Port Scan
103.145.12.2	Port Scan	46.161.27.75	Port Scan
54.39.51.192	Port Scan	94.102.56.231	Port Scan
192.227.144.226	Port Scan	193.142.146.203	Port Scan
192.241.216.210	Port Scan	46.166.148.123	Port Scan
192.241.217.52	Port Scan	64.31.8.50	Port Scan
179.189.2.210	Port Scan	64.31.33.134	Port Scan
185.53.88.22	Port Scan	64.31.33.62	Port Scan
185.53.88.63	Port Scan	80.82.68.63	Port Scan
212.83.135.137	Port Scan	51.210.139.3	Port Scan
107.189.11.114	Port Scan	185.59.51.71	Port Scan
103.145.12.5	Port Scan	192.241.212.44	Port Scan
145.239.11.116	Port Scan	192.241.222.72	Port Scan
128.14.141.99	Port Scan	129.227.129.163	Port Scan
192.241.234.101	Port Scan	5.226.137.138	Port Scan
192.241.236.161	Port Scan	103.81.87.132	Port Scan
85.209.40.45	Port Scan	192.241.233.169	Port Scan
23.90.145.35	Port Scan	185.238.242.31	Port Scan
77.247.108.17	Port Scan	144.91.93.197	Port Scan
162.241.75.116	Port Scan	31.201.227.12	Port Scan
163.172.4.45	Port Scan	118.185.35.101	Port Scan
31.211.191.107	Port Scan	37.49.224.57	Port Scan
23.83.129.11	Port Scan	203.119.15.144	Port Scan
192.241.234.161	Port Scan	203.119.15.143	Port Scan
198.98.62.87	Port Scan	156.154.180.144	Port Scan
180.163.194.16	Port Scan	156.154.180.143	Port Scan
207.148.68.143	Port Scan	202.76.225.74	Port Scan
180.163.194.13	Port Scan	180.153.232.13	Port Scan
192.241.227.154	Port Scan	192.241.236.80	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.

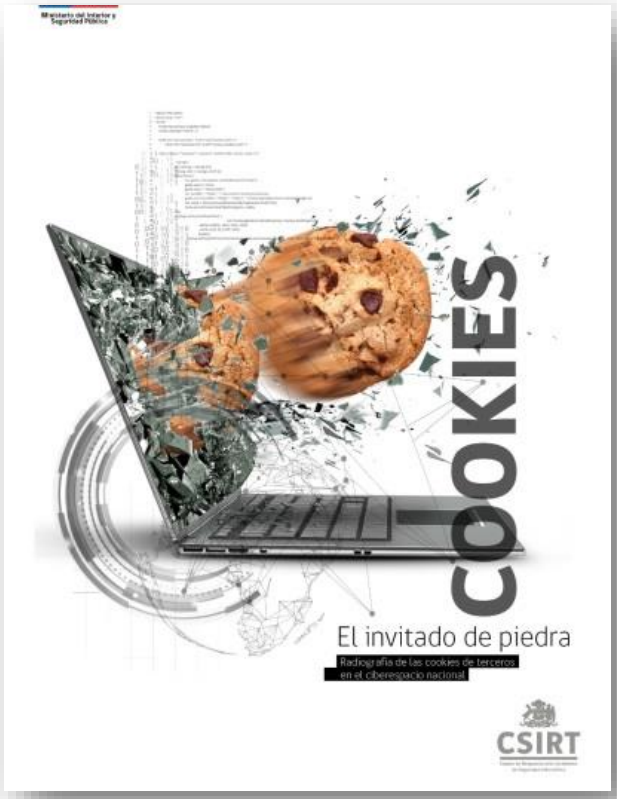
Investigación

El invitado de piedra. Radiografía de las cookies de terceros en el ciberespacio nacional

CSIRT, comparte la undécima edición de su publicación sobre amenazas cibernéticas el que analiza el rol de las cookies de terceros en el ciberespacio chileno. Este artículo fue elaborado por Carlos Silva Caffi y Patricio Quezada Andaur.

Las cookies son generalmente utilizadas para mejorar la navegación en los sitios web. Pero cuando no pertenecen a un desarrollo del sitio, son normalmente utilizadas con fines comerciales. Estas cookies son denominadas como cookies de terceros. En su gran mayoría, se caracterizan por permanecer almacenadas en los equipos de los usuarios por meses o años, hasta su caducidad, lo que se conoce como persistencia.

El objetivo de esta investigación es representar una aproximación al panorama de las cookies en el ciberespacio chileno. Para ello se realizaron dos muestras, en enero y julio de 2020, en un número limitado de sitios, los que fueron segmentados por diferentes rubros para su análisis y posterior comparación. Las muestras, realizadas manualmente, midieron la cantidad y tipos de cookies utilizadas en las navegaciones de estas webs comerciales, informativos y de servicios.



Ver más en: https://www.csirt.gob.cl/reportes/an2-2020-11/

Actualidad

Resultados Encuesta Nacional sobre el Acoso Sexual en Chile

Los resultados de la primera Encuesta Nacional sobre el Acoso Sexual en Chile, realizada por la plataforma Observatorio Contra el Acoso Chile (OCAC), dan como resultado que casi la mitad de los encuestados fueron víctimas de ciberacoso sexual, el cual se define como una práctica con connotación sexual implícita o explícita ejercida por una o más personas a través de internet y/o aparatos electrónicos, ejercida sin el consentimiento de quien la sufre.

Ver en: https://www.csirt.gob.cl/recomendaciones/resultados-encuesta-nacional-sobre-el-acoso-sexual-en-chile/

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.

- Matia Cornejo
  Linkedin:
  https://www.linkedin.com/in/matia-cornejo/
- Leonardo Paredes
  Twitter:
  https://twitter.com/Leonard69121673