15-05-2020 | Año 1 | N°45

Boletín de Seguridad Cibernética

Semana del 7 al 13 de mayo de 2020

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

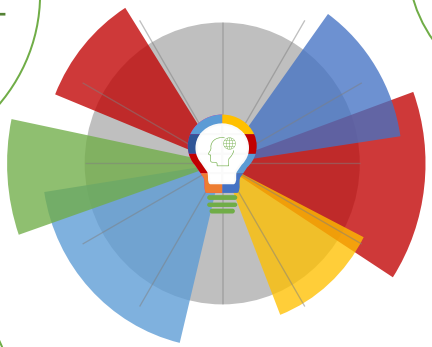
División de Redes y Seguridad Informática. Gobierno de Chile

Ministerio del Interior y Seguridad Pública. Gobierno de Chile

Resumen de la semana en cifras

Parches
126
para vulnerabilidades
Las mitigaciones son útiles para productos de Microsoft, VBulletin, Open VPN, VMware, NGINGX y Mozilla.

Se advirtieron
68
sitios fraudulentos
Asociadas a 39 IP maliciosas



Phishing
8
Campañas
Entre ellos se cuentan phishing bancarios, de servicios de pago y correos corporativos

IPs
183
bloqueadas
Listado de IPs que trataron de realizar escaneos de puertos, DDoS o infectar códigos maliciosos, entre otros.

*Las cifras provienen de información publicada en este boletín y del sitio https://www.csirt.gob.cl

Contenido

Sitios fraudulentos

Imagen del sitio

CSIRT advierte de dos sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00390-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Mayo de 2020
Última revisión	07 de Mayo de 2020
Indicadores de compromiso	
URL	
bancoestado-cl[.]steelresourcesinc[.]ca/	
estado-movils[.]com	
IP	
192[.]185[.]116[.]108	
198[.]54[.]112[.]209	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00390-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00390-01.pdf	

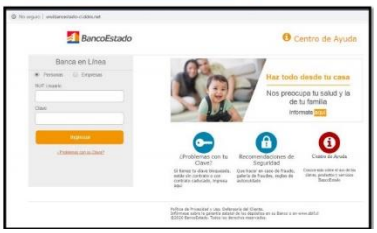
Imagen del sitio

CSIRT advierte de dos sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00391-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Mayo de 2020
Última revisión	07 de Mayo de 2020
Indicadores de compromiso	
URL	
acessobancofalabella[.]com	
IP	
18[.]231[.]106[.]234	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00391-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00391-01.pdf	

Imagen del sitio

CSIRT advierte de dos portales bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00392-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Mayo de 2020
Última revisión	07 de Mayo de 2020
Indicadores de compromiso	
URL	
bancoestado[.]chileaccesso[.]com	
estado[.]chileaccesso[.]com	
IP	
217[.]61[.]121[.]181	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00392-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00392-01.pdf	

Imagen del sitio



CSIRT advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00393-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Mayo de 2020
Última revisión	07 de Mayo de 2020
Indicadores de compromiso	
URL	
wwwibancestado-cl[.]ddns[.]net	
IP	
146[.]71[.]87[.]192	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00393-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00393-01.pdf	

Imagen del sitio

CSIRT advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00394-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Mayo de 2020
Última revisión	08 de Mayo de 2020
Indicadores de compromiso	
URL	
basncoestado[.]ru[.]com/imagenes/comun2008/	
IP	
47[.]245[.]32[.]253	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00394-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR-00394-01.pdf	

Imagen del sitio

CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00395-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Mayo de 2020
Última revisión	08 de Mayo de 2020
Indicadores de compromiso	
URL	
enlineas.baercoichlle.cl.grtdsdf.com/barchille/persona/login/#/login	
IP	
68[.]65[.]122[.]160	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00395-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR-00395-01.pdf	

Imagen del sitio

CSIRT advierte de sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00396-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Mayo de 2020
Última revisión	08 de Mayo de 2020
Indicadores de compromiso	
URL	
www3bancestado-cl[.]ddns.net	
IP	
146[.]71[.]87[.]192	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00396-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR-00396-01.pdf	

Imagen del sitio

CSIRT advierte de un portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00397-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Mayo de 2020
Última revisión	08 de Mayo de 2020
Indicadores de compromiso	
URL	
wwibancestado-chile.ddns.net	
IP	
146[.]71[.]87[.]192	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00397-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00392-01.pdf	

CSIRT advierte de sitio fraudulento que suplanta a servicio de streaming	
Alerta de seguridad cibernética	8FFR20-00398-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de mayo de 2020
Última revisión	08 de mayo de 2020
Indicadores de compromiso	
URL	
netflix-vencido[.]cl	
IP	
162[.]241[.]61[.]68	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00398-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00398-01.pdf	

Imagen del sitio

CSIRT advierte de dominio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00399-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
Indicadores de compromiso	
URL	
estado-alert.com/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
35[.]208[.]103[.]4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00399-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00399-01.pdf	

Imagen del sitio

CSIRT advierte de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00400-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
Indicadores de compromiso	
URL	
chile.chileaccesso.com/mobile/choose.php	
IP	
217[.]61[.]121[.]181	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00400-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00400-01.pdf	

Imagen del sitio

CSIRT advierte de web bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR20-00401-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
Indicadores de compromiso	
URL	
connectionis[.]audison[.]eu/code/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
176[.]223[.]212[.]65	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00401-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00401-01.pdf	

Imagen del sitio

CSIRT comparte información sobre sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00402-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
Indicadores de compromiso	
URL	
estadopromo-cl[.]site	
IP	
139[.]59[.]36[.]248	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00402-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00402-01.pdf	

Imagen del sitio

CSIRT advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00403-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
Indicadores de compromiso	
URL	
bancoestado-cl[.]radiocrossovernetwork[.]com	
IP	
162[.]241[.]95[.]71	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00403-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00403-01.pdf	

Imagen del sitio

CSIRT informa de portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00404-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
Indicadores de compromiso	
URL	
falabella[.]chileaccesso.com	
IP	
217[.]61[.]121[.]181	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00404-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00404-01.pdf	

Imagen del sitio

CSIRT advierte de un sitio fraudulento que suplanta web bancaria	
Alerta de seguridad cibernética	8FFR20-00405-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
Indicadores de compromiso	
URL	
transferenciasscotiabankk-chile-covid[.]gq	
IP	
178[.]159[.]36[.]139	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00405-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00405-01.pdf	

Imagen del sitio

CSIRT advierte tres dominios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00406-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Mayo de 2020
Última revisión	10 de Mayo de 2020
Indicadores de compromiso	
URL	
wwwbancenestado-cl[.]gotdns[.]ch	
www2bancnestado-cl.ddns.net	
elbancnestado-chile.ddns.net	
IP	
146[.]71[.]87[.]192	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00406-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00406-01.pdf	

Imagen del sitio

CSIRT Advierte de un portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00407-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Mayo de 2020
Última revisión	10 de Mayo de 2020
Indicadores de compromiso	
URL	
sklep[.]dlawina[.]pl/classes/www[.]santander[.]cl/pagina/index[.]php	
IP	
185[.]38[.]251[.]214	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00407-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00407-01.pdf	

Imagen del sitio

CSIRT advierte de un sitio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00408-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Mayo de 2020
Última revisión	10 de Mayo de 2020
Indicadores de compromiso	
URL	
bancnestado-chile.ddns.net	
IP	
146[.]71[.]87[.]192	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00408-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00408-01.pdf	

Imagen del sitio

CSIRT advierte de tres dominios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00409-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Mayo de 2020
Última revisión	12 de Mayo de 2020
Indicadores de compromiso	
URL	
bancoestado-cl.instantsolutions[.]com.bd/imagenes/comun2008/banca-en-linea-personas[.]html	
bancoestado-cl[.]bdkhati.com/imagenes/comun2008/banca-en-linea-personas[.]html	
sms-centralestado[.]com/imagenes/comun2008/banca-en-linea-personas[.]html	
IP	
23[.]229[.]104[.]50	
64[.]188[.]2[.]209	
35[.]209[.]89[.]210	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00409-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00409-01.pdf	

Imagen del sitio

CSIRT informa de web bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR20-00410-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Mayo de 2020
Última revisión	12 de Mayo de 2020
Indicadores de compromiso	
URL	
scotiabanckcl[.]com	
IP	
144[.]208[.]126[.]171	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00410-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00410-01.pdf	

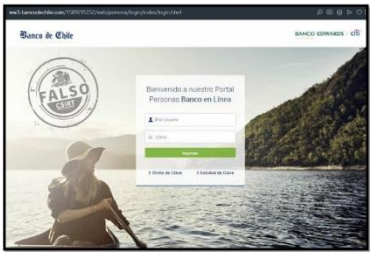
Imagen del sitio

CSIRT informa de dos web fraudulentas	
Alerta de seguridad cibernética	8FFR20-00411-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Mayo de 2020
Última revisión	12 de Mayo de 2020
Indicadores de compromiso	
URL	
falabella[.]securitycl[.]com,	
bancofalabellacmr[.]app/site/choose[.]php	
IP	
217[.]61[.]121[.]181	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00411-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00411-01.pdf	

Imagen del sitio

CSIRT advierte cinco sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00412-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Mayo de 2020
Última revisión	12 de Mayo de 2020
Indicadores de compromiso	
URL	
htlps-wwv-bancaestado-cl[.]comidagourmetchileuti[.]com/personas-cl/ estadoenlineacl[.]aqp[.]red/images/comuncl008/banca-en-linea-personas[.]html	
bancoestado[.]securitycl[.]com/site/index[.]php	
estado-plataforma[.]com/site/imagenes/comun2008/banca-en-linea-personas[.]html	
tecnifer[.]com[.]co/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]htm	
bit[.]ly/35N1Vzu?l	
IP	
217[.]61[.]121[.]181	
162[.]241[.]60[.]178	
198[.]187[.]30[.]108	
92[.]249[.]44[.]58	
92[.]42[.]107[.]131	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00412-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00412-01.pdf	

Imagen del sitio



CSIRT advierte de dos sitios bancarios fraudulentos	
Alerta de seguridad cibernética	8FFR20-00413-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Mayo de 2020
Última revisión	13 de Mayo de 2020
Indicadores de compromiso	
URL	
ww3-bancodechile[.]com	
chile[.]chileacceso[.]app	
IP	
199[.]33[.]112[.]226	
217[.]61[.]122[.]233	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00413-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00413-01.pdf	

Imagen del sitio

CSIRT informa de una web bancaria fraudulenta	
Alerta de seguridad cibernética	8FFR20-00414-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Mayo de 2020
Última revisión	13 de Mayo de 2020
Indicadores de compromiso	
URL	
tarjetacencosud-chile-activa[.]ga	
IP	
178[.]159[.]36[.]139	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00414-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00414-01.pdf	

Imagen del sitio

CSIRT advierte sobre dominio bancario fraudulento	
Alerta de seguridad cibernética	8FFR20-00415-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Mayo de 2020
Última revisión	13 de Mayo de 2020
Indicadores de compromiso	
URL	
bancoestado[.]chileacceso[.]app	
IP	
217[.]61[.]122[.]233	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00415-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00415-01.pdf	

Imagen del sitio

CSIRT informa sobre una web para fraudes bancarios	
Alerta de seguridad cibernética	8FFR20-00416-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Mayo de 2020
Última revisión	13 de Mayo de 2020
Indicadores de compromiso	
URL	
falabella[.]chileacceso[.]app	
IP	
217[.]61[.]122[.]233	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00416-01/	
https://www.csirt.gob.cl/media/2020/05/8FFR20-00416-01.pdf	

Phishing

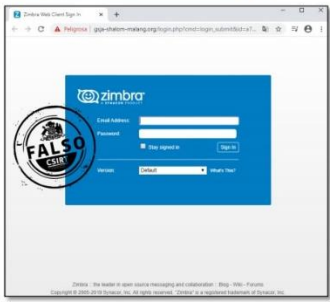
Imagen del mensaje

CSIRT advierte de phishing por bloqueo de cuenta bancaria	
Alerta de seguridad cibernética	8FPH20-00207-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Mayo de 2020
Última revisión	08 de Mayo de 2020
Indicadores de compromiso	
URL	
http://rojitomail[.]site/Activacion/cuenta-wfpd/	
http://rakitys[.]info/crush/	
IP	
[170.239.84.253]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00207-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00207-01.pdf	

IMAGEN DEL MENSAJE

CSIRT advierte sobre campaña de phishing por supuesto premio al azar	
Alerta de seguridad cibernética	8FPH20-00208-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Mayo de 2020
Última revisión	08 de Mayo de 2020
Indicadores de compromiso	
URL	
http://paypalservicegifts[.]com/pp/pp/	
IP	
[168.245.115.183]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00208-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00208-01.pdf	

Imagen del sitio



CSIRT advierte phishing por supuesto mantenimiento de servicio de correo	
Alerta de seguridad cibernética	8FPH20-00209-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Mayo de 2020
Última revisión	08 de Mayo de 2020
Indicadores de compromiso	
URL	
https://correo-zimbra400589.pancakeapps[.]com/zim[.]html?	
IP	
[190.102.147.233]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00209-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00209-01.pdf	

Imagen del mensaje

CSIRT informa sobre campaña de phishing por depósito de pensión	
Alerta de seguridad cibernética	8FPH20-00210-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Mayo de 2020
Última revisión	11 de Mayo de 2020
Indicadores de compromiso	
URL	
https[:]//bit[.]ly/35N1Vzu?l=www[.]bancoestado[.]cl	
https[:]//tecnifer[.]com[.]co/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]htm	
IP	
[92.42.107.131]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00210-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00210-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por bloqueo de cuenta	
Alerta de seguridad cibernética	8FPH20-00211-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Mayo de 2020
Última revisión	12 de Mayo de 2020
Indicadores de compromiso	
URL	
http://torneonet[.]site/Activacion/cuenta-qhtn/	
http://netnt[.]site/natu/imagenes/comun2008/banca-en-linea-personas.html#	
IP	
[170.239.85.165]	
[45.236.131.199]	
Otros IOCs del informe:	
2 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00211-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00211-01.pdf	

Imagen del mensaje

CSIRT advierte campaña de phishing que ofrece aumento de cupo	
Alerta de seguridad cibernética	8FPH20-00212-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Mayo de 2020
Última revisión	12 de Mayo de 2020
Indicadores de compromiso	
URL	
https://d8.gotoproject[.]net/drshiller/wp-content/bancochile.php	
https://banchile-personasss[.]tk/	
IP	
[103.248.146.2]	
[103.248.146.100]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00212-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00212-01.pdf	

Imagen del mensaje

CSIRT advierte de phishing por bloqueo de contraseña bancaria	
Alerta de seguridad cibernética	8FPH20-00213-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Mayo de 2020
Última revisión	12 de Mayo de 2020
Indicadores de compromiso	
URL	
http://novomoskovsk-rada.gov[.]ua/modules/https:/www.scotiabankchile.cl/?cliente=	
https://ingresows-scortiarbarnk-online[.]xyz/AQBM4C/login/0JKTJ/personas//	
IP	
[188.138.70.167]	
Otros IOCs del informe:	
1 sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00213-01/	
https://www.csirt.gob.cl/media/2020/05/8FPH20-00213-01.pdf	

Malware

CSIRT advierte de malware en correo sobre proceso criminal	
Alerta de seguridad cibernética	2CMV20-00061-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
Indicadores de compromiso	
URL	
http[:]//restaurantedoalemao[.]com[.]br/email/0491902	
http[:]//40.89.185[.]52/pela/n9157950df03[.]ret	
IP Servidor Smtp	
[20.36.41.58]	
[23.102.69.175]	
[191.232.181.239]	
[20.36.32.127]	
[52.231.203.97]	
[20.36.34.45]	
[191.232.183.93]	
[20.151.1.196]	
[191.232.181.148]	
Otros IOCs del informe:	
6 Hash SHA256; 22 Sender	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv20-00061-01/	
https://www.csirt.gob.cl/media/2020/05/2CMV20-00061-01.pdf	

Vulnerabilidades

CSIRT comparte nueva actualización de VMWare para ESXI y HorizonDaaS	
Alerta de seguridad cibernética	9VSA-00097-002
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Diciembre de 2019
Última revisión	08 de Mayo de 2020
CVE	
CVE-2019-5544	
Fabricante	
VMWare	
Producto afectado	
VMware ESXi, versiones 6.0, 6.5 y 6.7., VMware Horizon Daas, versiones 8.x.	
Informe original (2019):	
https://www.csirt.gob.cl/media/2019/12/9VSA-00097-001.pdf	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa-00097-002/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00097-02.pdf	

CSIRT comparte actualizaciones de Mozilla para Thunderbird	
Alerta de seguridad cibernética	9VSA20-00207-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Mayo de 2020
Última revisión	08 de Mayo de 2020
CVE	
CVE-2020-6831, CVE-2020-12387, CVE-2020-12392, CVE-2020-12393, CVE-2020-12395, CVE-2020-12397	
Fabricante	
Mozilla	
Producto afectado	
Mozilla Thunderbird desde la versión 60.0 hasta la 60.9.1. y desde la versión 68.0 hasta la 68.7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00207-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00207-01.pdf	

CSIRT comparte actualizaciones de NGINX para NGINX Controller	
Alerta de seguridad cibernética	9VSA20-00208-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
CVE	
CVE-2020-5894, CVE-2020-5895	
Fabricante	
NGINX	
Producto afectado	
NGINX Controller	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00208-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00208-01.pdf	

CSIRT comparte actualizaciones de VMware para vRealize Operation Manager	
Alerta de seguridad cibernética	9VSA20-00209-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Mayo de 2020
Última revisión	09 de Mayo de 2020
CVE	
CVE-2020-11651, CVE-2020-11652	
Fabricante	
VMware	
Producto afectado	
VMware vRealize Operations Manager versiones 7.5.0, 8.0.x y 8.1.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00209-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00209-01.pdf	

CSIRT comparte actualizaciones para OpenVPN	
Alerta de seguridad cibernética	9VSA20-00210-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Mayo de 2020
Última revisión	11 de Mayo de 2020
CVE	
CVE-2020-11810	
Fabricante	
OpenVPN	
Producto afectado	
OpenVPN versión 2.4.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00210-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00210-01.pdf	

CSIRT comparte actualizaciones liberadas por vBulletin	
Alerta de seguridad cibernética	9VSA20-00211-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Mayo de 2020
Última revisión	12 de Mayo de 2020
CVE	
CVE-2020-12720	
Fabricante	
vBulletin	
Producto afectado	
vBulletin 5 versión 5.6.1, 5.6.0, 5.5.6 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00211-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00211-01.pdf	

CSIRT comparte información liberada por Microsoft para sus productos	
Alerta de seguridad cibernética	9VSA20-00212-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Mayo de 2020
Última revisión	13 de Mayo de 2020
CVE	
ADV200004, ADV200007, CVE-2020-0901, CVE-2020-0909, CVE-2020-0963, CVE-2020-1010, CVE-2020-1021, CVE-2020-1023, CVE-2020-1024, CVE-2020-1028, CVE-2020-1035, CVE-2020-1037, CVE-2020-1048, CVE-2020-1051, CVE-2020-1054, CVE-2020-1055, CVE-2020-1056, CVE-2020-1058, CVE-2020-1059, CVE-2020-1060, CVE-2020-1061, CVE-2020-1062, CVE-2020-1063, CVE-2020-1064, CVE-2020-1065, CVE-2020-1066, CVE-2020-1067, CVE-2020-1068, CVE-2020-1069, CVE-2020-1070, CVE-2020-1071, CVE-2020-1072, CVE-2020-1075, CVE-2020-1076, CVE-2020-1077, CVE-2020-1078, CVE-2020-1079, CVE-2020-1081, CVE-2020-1082, CVE-2020-1084, CVE-2020-1086, CVE-2020-1087, CVE-2020-1088, CVE-2020-1090, CVE-2020-1092, CVE-2020-1093, CVE-2020-1096, CVE-2020-1099, CVE-2020-1100, CVE-2020-1101, CVE-2020-1102, CVE-2020-1103, CVE-2020-1104, CVE-2020-1105, CVE-2020-1106, CVE-2020-1107, CVE-2020-1108, CVE-2020-1109, CVE-2020-1110, CVE-2020-1111, CVE-2020-1112, CVE-2020-1113, CVE-2020-1114, CVE-2020-1116, CVE-2020-1117, CVE-2020-1118, CVE-2020-1121, CVE-2020-1123, CVE-2020-1124, CVE-2020-1125, CVE-2020-1126, CVE-2020-1131, CVE-2020-1132, CVE-2020-1134, CVE-2020-1135, CVE-2020-1136, CVE-2020-1137, CVE-2020-1138, CVE-2020-1139, CVE-2020-1140, CVE-2020-1141, CVE-2020-1142, CVE-2020-1143, CVE-2020-1144, CVE-2020-1145, CVE-2020-1149, CVE-2020-1150, CVE-2020-1151, CVE-2020-1153, CVE-2020-1154, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1161, CVE-2020-1164, CVE-2020-1165, CVE-2020-1166, CVE-2020-1171, CVE-2020-1173, CVE-2020-1174, CVE-2020-1175, CVE-2020-1176, CVE-2020-1179, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191, CVE-2020-1192	
Fabricante	
Microsoft	
Producto afectado	
Varios softwares	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00212-01/	
https://www.csirt.gob.cl/media/2020/05/9VSA20-00212-01.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
128.199.185.104	Port Scan	173.249.37.142	Port Scan
192.241.232.135	Port Scan	194.182.88.217	Port Scan
162.243.145.28	Port Scan	94.102.51.17	Port Scan
162.243.145.4	Port Scan	51.159.58.91	Port Scan
192.241.232.48	Port Scan	162.243.140.170	Port Scan
162.243.140.38	Port Scan	156.96.150.87	Port Scan
162.243.144.210	Port Scan	200.2.142.51	Port Scan
162.243.142.210	Port Scan	185.156.73.50	Port Scan
162.243.141.249	Port Scan	107.189.11.127	Port Scan
162.243.137.187	Port Scan	37.49.226.7	Port Scan
162.243.139.150	Port Scan	103.145.12.111	Port Scan
162.243.138.189	Port Scan	185.53.88.252	Port Scan
162.243.141.37	Port Scan	195.154.164.211	Port Scan
162.243.137.74	Port Scan	163.172.82.44	Port Scan
162.243.135.168	Port Scan	162.243.137.14	Port Scan
178.62.50.119	Port Scan	138.68.30.35	Port Scan
162.243.137.209	Port Scan	162.243.137.75	Port Scan
162.243.141.55	Port Scan	176.31.234.222	Port Scan
162.243.136.91	Port Scan	162.243.136.126	Port Scan
67.219.145.50	Port Scan	162.243.144.222	Port Scan
67.219.145.130	Port Scan	209.141.42.26	Port Scan
67.219.148.146	Port Scan	67.229.48.143	Port Scan
67.219.145.2	Port Scan	195.154.199.199	Port Scan
162.243.144.204	Port Scan	94.102.51.28	Port Scan
162.243.137.205	Port Scan	195.231.3.56	Port Scan
162.243.137.28	Port Scan	185.163.45.169	Port Scan
195.154.241.160	Port Scan	45.95.168.85	Port Scan
162.243.144.225	Port Scan	195.54.160.121	Port Scan
162.243.143.240	DDoS	209.90.225.218	Port Scan
45.143.220.20	DDoS	36.83.251.69	Port Scan

162.222.226.70	Phishing	117.248.248.11	Port Scan
178.159.36.139	Phishing	195.54.160.121	Hacking
213.190.6.50	Phishing	209.90.225.218	Hacking
213.136.95.10	Port Scan	36.83.251.69	Hacking
213.136.95.11	Port Scan	117.248.248.11	Hacking
152.174.157.175	DDoS	173.208.190.186	Port Scan
146.71.87.192	Phishing	185.43.209.119	Port Scan
193.232.128.6	Hacking	103.89.88.140	Port Scan
162.243.136.144	Port Scan	134.73.232.200	Port Scan
162.243.143.216	Port Scan	185.142.236.34	Port Scan
162.243.138.155	Port Scan	49.51.10.24	Port Scan
162.243.138.97	Port Scan	51.255.109.172	Port Scan
162.243.137.77	Port Scan	54.36.149.101	Port Scan
162.243.144.89	Port Scan	114.79.170.228	Port Scan
162.243.139.196	Port Scan	170.106.81.188	Port Scan
162.243.138.32	Port Scan	170.106.84.58	Port Scan
162.243.137.64	Port Scan	185.234.219.28	Port Scan
162.243.136.136	Port Scan	49.51.12.25	Port Scan
162.243.141.59	Port Scan	118.137.162.166	Port Scan
162.243.139.116	Port Scan	124.156.55.167	Port Scan
185.244.150.6	Port Scan	150.109.203.21	Port Scan
193.228.91.107	Port Scan	188.166.26.69	Port Scan
185.212.149.110	Port Scan	104.248.135.111	Port Scan
80.82.65.253	Port Scan	161.35.55.6	Port Scan
94.102.51.16	Port Scan	139.59.7.53	Port Scan
94.102.51.29	Port Scan	12.162.84.2	Malware
195.231.11.144	Port Scan	104.131.41.185	Malware
162.243.142.207	Port Scan	110.145.124.178	Malware
162.243.138.173	Port Scan	175.114.178.83	Malware
162.243.136.20	Port Scan	104.236.161.64	Malware
162.243.144.38	Port Scan	189.19.81.181	Malware
162.243.145.24	Port Scan	103.83.81.141	Malware
162.243.139.233	Port Scan	69.246.151.5	Malware
162.243.145.5	Port Scan	71.69.128.2	Malware
162.243.140.211	Port Scan	216.152.7.12	Malware
162.243.145.89	Port Scan	98.118.156.172	Malware
162.243.135.175	Port Scan	86.127.144.244	Malware
162.243.142.7	Port Scan	79.118.189.100	Malware

162.243.145.49	Port Scan	94.52.220.145	Malware
162.243.145.33	Port Scan	86.108.116.21	Malware
162.243.138.36	Port Scan	190.147.186.58	Malware
162.243.143.75	Port Scan	98.13.0.128	Malware
162.243.139.191	Port Scan	89.137.101.104	Malware
209.141.48.229	Port Scan	72.36.11.22	Malware
107.189.11.185	Port Scan	50.91.171.137	Malware
139.99.114.230	Port Scan	189.128.64.93	Malware
162.243.138.52	Port Scan	71.195.111.107	Malware
162.243.139.192	Port Scan	68.46.142.48	Malware
162.243.138.182	Port Scan	73.226.220.56	Malware
162.243.136.36	Port Scan	96.250.113.218	Malware
162.243.143.225	Port Scan	46.214.62.199	Malware
139.99.114.230	Port Scan	94.176.128.176	Malware
162.243.145.66	Port Scan	24.26.1.14	Malware
162.243.138.27	Port Scan	102.41.125.216	Malware
193.228.91.111	Port Scan	96.37.113.36	Malware
209.141.58.185	Port Scan	65.96.36.157	Malware
104.244.79.145	Port Scan	98.222.23.221	Malware
162.243.136.95	Port Scan	162.243.136.121	Port Scan
209.141.40.23	Port Scan	89.36.213.98	Port Scan
104.144.123.172	Port Scan	45.165.124.15	Port Scan
190.210.166.140	Port Scan	178.62.252.146	Phishing
162.243.144.33	Port Scan		

Recomendaciones y Buenas Prácticas

Recomendaciones generales de seguridad

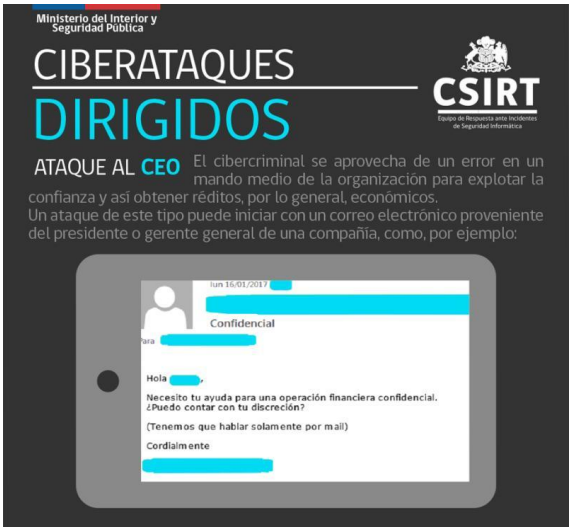
- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- 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.

Campaña sobre compra con ocasión del día de la madre

Se acerca el Día de la Madre y si estás pensando comprarle un regalo a través de Internet, es importante considerar que los riesgos y peligros de internet siempre están presentes. No te expongas a perder tus credenciales comerciales, bancarias o tus datos personales. ¿En qué te debes fijar para asegúrate de no caer en una estafa? Revisa nuestros ciberconsejos en este enlace: https://www.csirt.gob.cl/media/2020/05/Di%CC%81a-de-la-madre.pdf

Campaña para prevenir los ciberataques dirigidos

Suplantar la identidad de forma pública o dentro de las organizaciones es bastante recurrente por parte de los cibercriminales. Las consecuencias de estos ataques son difíciles de cuantificar, muchas veces porque las personas afectadas se enteran muy tarde de la estafa o porque se rehúsan a compartir públicamente que fueron víctimas. Sin embargo, si los mensajes son convincentes, se lamentan pérdidas económicas que pueden llegar a ser cuantiosas. Revisa la campaña en: https://www.csirt.gob.cl/media/2020/05/Suplantacio%CC%81n-de-imagen.pdf



Investigación

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte el siguiente análisis de amenazas cibernéticas que estudia el caso sobre el **Fraude del Príncipe Nigeriano o Phishing 419**, y fue elaborado por Natalia Pérez Muñoz, analista de nivel 2 de CSIRT. Este infame ataque tiene como premisa la personificación del estafador, quien se hace pasar por una persona que necesita recuperar una fortuna en su país pero necesita ayuda de una tercera parte en el extranjero para la transacción, a quien en compensación, ofrece parte del dinero. Este análisis define conceptos como ingeniería social y phishing, expone algunas de las vulnerabilidades que explotan los atacantes, y explorar en la estafa 419 y sus principales consecuencias –especialmente económicas-, además de compartir algunas recomendaciones.

Ver en: https://www.csirt.gob.cl/media/2020/05/AN2-2020-03.pdf

Actualidad

Programa OEA-CISCO ofrece cursos virtuales gratuitos en ciberseguridad

El pasado miércoles 13 de mayo, en el contexto de la reunión del Consejo de Innovación en Ciberseguridad de Latinoamérica, se anunció el lanzamiento de una serie de cursos en ciberseguridad accesible para todos los ciudadanos de los países miembro de la OEA.
El Subsecretario del Interior, Juan Francisco Galli, quien participó en la reunión virtual en representación del Gobierno de Chile, valoró el esfuerzo público-privado que llevan adelante la OEA junto con CISCO, el que permitirá a los ciudadanos desarrollar habilidades técnicas en seguridad informática.

La noticia completa y la información sobre la oferta de cursos están disponibles en el siguiente enlace: https://www.csirt.gob.cl/noticias/programa-oea-cisco-ofrecen-cursos-virtuales-gratuitos-en-ciberseguridad/

Muro de la Fama

Las siguientes personas y organizaciones han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos públicos del Estado, así como a la comunidad en general, al compartir información sobre problemas de seguridad y vulnerabilidades que han descubierto.

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.

- Miguel Ángel Rojas. Twitter @Miguel_Rojas_R
- Bernardo Avilés