



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 192

SEMANA DEL 3 AL 9 DE MARZO 2023

INFORMACION IMPORTANTE

El CSIRT de Gobierno informa que debido a problemas técnicos no ha sido posible publicar las alertas de seguridad cibernéticas y campañas de concientización en nuestro sitio web.

Por lo tanto, los informes e indicadores de compromiso los podrán encontrar en el repositorio de GitHub del CSIRT de Gobierno: www.github.com/csirtcl

LA SEMANA EN CIFRAS

IP INFORMADAS

14

IP advertidas en múltiples campañas de phishing y de malware.



URL ADVERTIDAS

19

asociadas a sitios fraudulentos y campañas de phishing y malware



HASH REPORTADOS

7

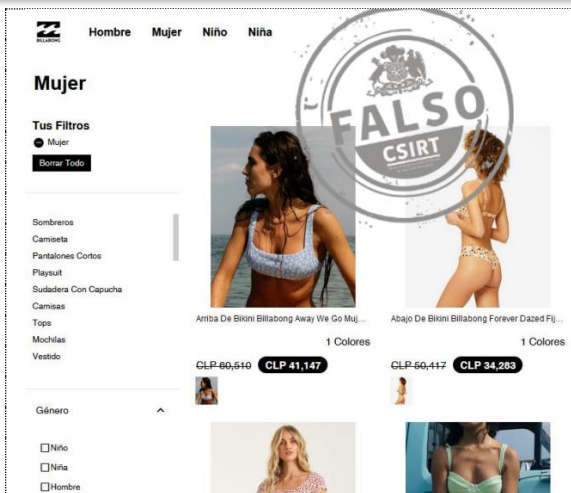
asociadas a múltiples campañas de phishing con archivos que contienen malware



CONTENIDO

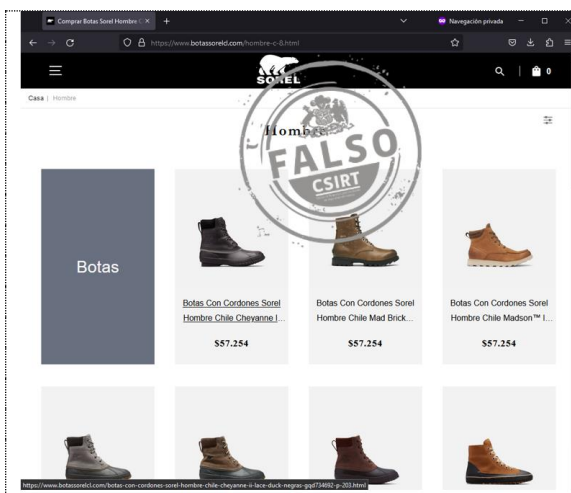
1.	Sitios fraudulentos	4
2.	Phishing	8
3.	Malware.....	10
4.	Concientización.....	11
5.	Recomendaciones y buenas prácticas	14
6.	Muro de la Fama	15

1. Sitios fraudulentos



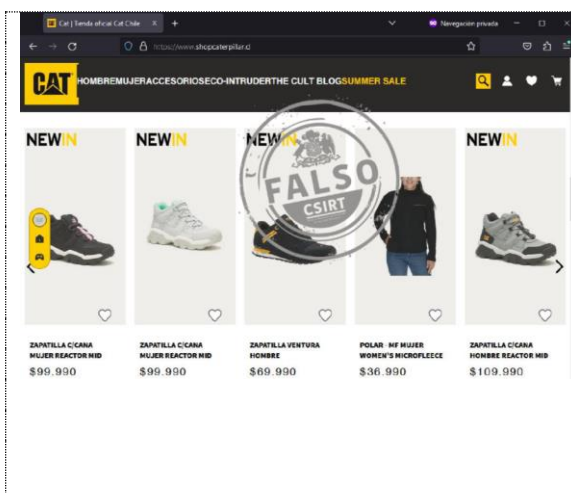
CSIRT advierte sitio que suplanta a Billabong

Alerta de seguridad cibernética	8FFR23-01239-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2023
Última revisión	3 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.billabongchile[.]com/	
Dirección IP	
[196.247.61.208]	
Enlace para revisar loC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01239-01.txt	



CSIRT alerta página web que suplanta a Sorel


Alerta de seguridad cibernética	8FFR23-01240-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2023
Última revisión	3 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.botassorelcl[.]com/	
Dirección IP	
[196.242.16.249]	
Enlace para revisar loC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01240-01.txt	



CSIRT alerta página web que suplanta a Caterpillar

Alerta de seguridad cibernética	8FFR23-01241-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo de 2023
Última revisión	6 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.shopcaterpillar[.]cl/	
Dirección IP	
[13.226.22.66]	
Enlace para revisar loC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01241-01.txt	

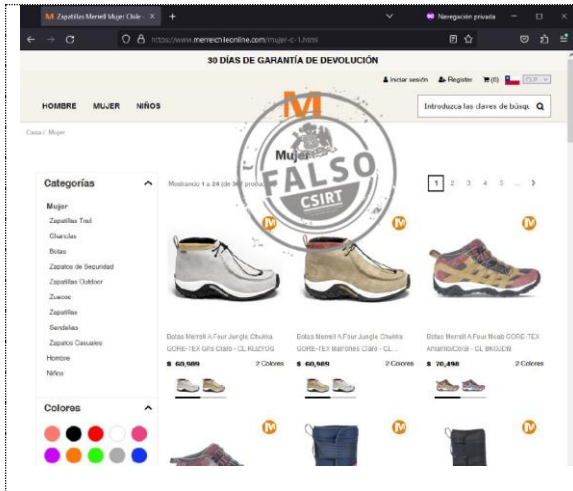
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Boletín de Seguridad Cibernética N° 192

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

BOLETÍN 13BCS23-00201-01 | SEMANA DEL 3 al 9 de MARZO DE 2023



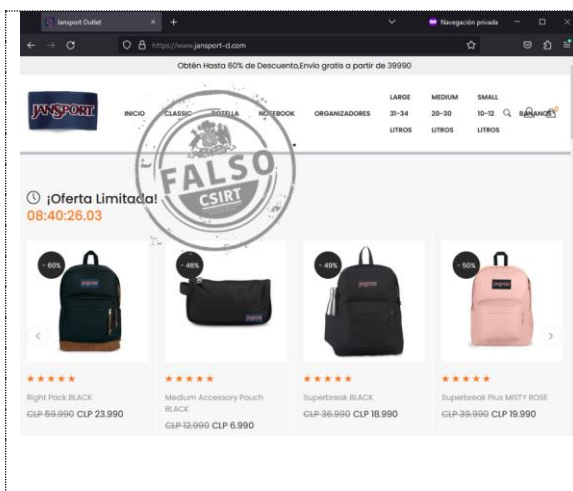
CSIRT advierte sitio que suplanta a Merrell

Alerta de seguridad cibernética	8FFR23-01242-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de marzo de 2023
Última revisión	6 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.merrellchileofertas[.]com/	
Dirección IP	
[196.196.205.239]	
Enlace para revisar loC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01242-01.txt	



CSIRT alerta de página web que suplanta al Banco Falabella

Alerta de seguridad cibernética	8FFR23-01243-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de marzo de 2023
Última revisión	7 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://dev-aceptar-nuevo-aumento4.pantheonsite[.]jio/	
Dirección IP	
[23.185.0.3]	
Enlace para revisar loC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01243-01.txt	



CSIRT alerta sitio web falso de JanSport

Alerta de seguridad cibernética	8FFR23-01244-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de marzo de 2023
Última revisión	7 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.jansport-cl[.]com/	
Dirección IP	
[172.67.175.180]	
Enlace para revisar loC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01244-01.txt	

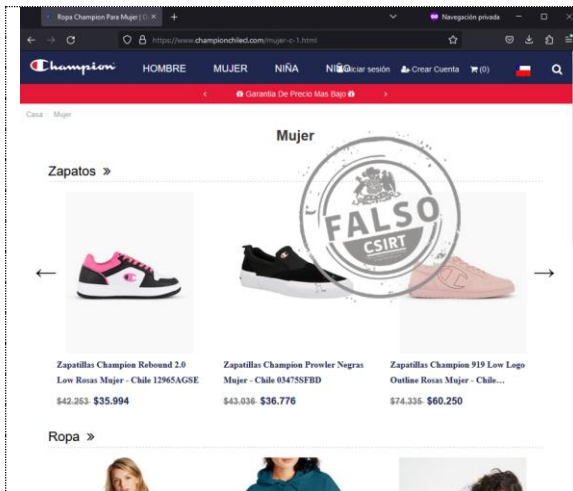
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

Boletín de Seguridad Cibernética N° 192

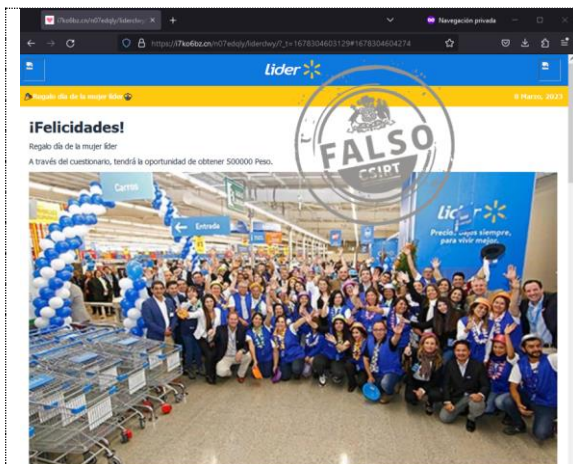
Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

BOLETÍN 13BCS23-00201-01 | SEMANA DEL 3 al 9 de MARZO DE 2023



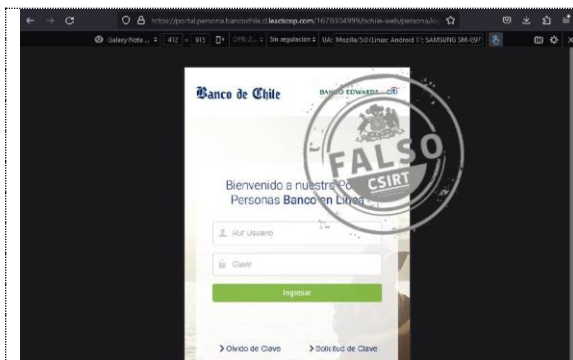
CSIRT advierte página web que suplanta a Champion

Alerta de seguridad cibernética	8FFR23-01245-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2023
Última revisión	8 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.championchilecl[.]com/	
Dirección IP	
[196.245.249.87]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01245-01.txt	



CSIRT alerta de sitio web falso de Líder

Alerta de seguridad cibernética	8FFR23-01246-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2023
Última revisión	8 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
http://w.attractpant[.]cyou/0830aI9_RUBERIRkW31kAxsHbFh9D0lYFQ1BNVIFMA0bXDQmaz4eFI0eEVs6HFMDSakjekUgaAg6VAkgFAtEXR5eIQka?pngw1678303073349	
https://i7ko6bz[.]cn/n07edqyliderclwy/?_t=1678304603129#1678304604274	
Dirección IP	
[104.21.1.9]	
Enlace para revisar IoC:	
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01246-01.txt	



CSIRT informa de página web que suplanta al Banco de Chile

Alerta de seguridad cibernética	8FFR23-01247-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2023
Última revisión	8 de marzo de 2023
Indicadores de compromiso	
URL sitio falso	
https://is.gd/BancoChile	
https://portal.persona.bancochile.cl.leadscop[.]com/1678304999/bchile-web/persona/login/index.html/login	
Dirección IP	
[68.66.216.59]	

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

Boletín de Seguridad Cibernética N° 192

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

BOLETÍN 13BCS23-00201-01 | SEMANA DEL 3 al 9 de MARZO DE 2023

Enlace para revisar loC:

https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01247-01.txt

CSIRT advierte sitio web falso que suplanta a Empresas Copec

Alerta de seguridad cibernética	8FFR23-01248-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de marzo de 2023
Última revisión	9 de marzo de 2023

Indicadores de compromiso

URL sitio falso

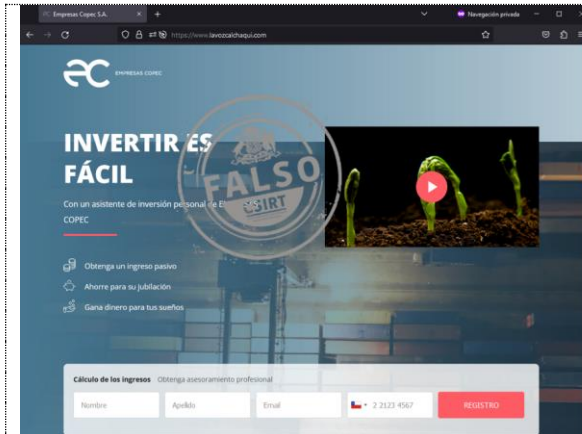
[https://www.lavozcalchaqui\[.\]com/](https://www.lavozcalchaqui[.]com/)

Dirección IP

[172.67.203.208]

Enlace para revisar loC:

https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01248-01.txt





CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>





2. Phishing

 <p>CUENTA SUSPENDIDA</p> <p>BancoEstado <bancocastado@plusconsulting.cl> Para</p> <p>Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.</p> <p>Estimado Cliente:</p> <p>Lamentamos Informarle que su cuenta ha sido suspendida temporalmente Por su seguridad le rogamos que complete inmediatamente la siguiente actualización de la cuenta.</p> <p>Actualizar Cuenta</p>	<p>CSIRT alerta de campaña de smishing que suplanta a BancoEstado</p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00764-01</td></tr> <tr><td>Clase de alerta</td><td>Fraude</td></tr> <tr><td>Tipo de incidente</td><td>Phishing</td></tr> <tr><td>Nivel de riesgo</td><td>Alto</td></tr> <tr><td>TLP</td><td>Blanco</td></tr> <tr><td>Fecha de lanzamiento original</td><td>6 de marzo de 2023</td></tr> <tr><td>Última revisión</td><td>6 de marzo de 2023</td></tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección https://contawebnwm[.]com/activacion/cuenta-wwnq/</p> <p>URL sitio falso https://nwmepsonpatito[.]top/1678107788/imagenes/_personas/home/default.asp</p> <p>Dirección IP [172.67.173.125]</p> <p>Enlace para revisar loC: https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00764-01.txt</p>	Alerta de seguridad cibernética	8FPH23-00764-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	6 de marzo de 2023	Última revisión	6 de marzo de 2023
Alerta de seguridad cibernética	8FPH23-00764-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	6 de marzo de 2023														
Última revisión	6 de marzo de 2023														

 <p>Noticia importante</p> <p>"=7utf-8?q?Administraci=C3=B3n_3Crmolina=40dinaf=2Egob=" Para Recipientes</p> <p>Querido usuario,</p> <p>En nuestro intento de mejorar la seguridad y la calidad de nuestros servicios de correo electrónico, actuali en nuestra base de datos. Esta actualización solo tomará unos minutos y durante la actualización es posi servicio, lo que significa que el envío y la recepción de correos electrónicos podrían retrasarse o ser imposi</p> <p>Se recomienda a los usuarios verificar su correo electrónico a través del siguiente enlace hacer clic en el e y pegar en su URL y seguir las instrucciones para verificar su cuenta. El término límite de este aviso podri de sus mensajes entrantes y también podría conducir al cierre permanente de su cuenta de correo electo</p> <p>Gracias, Apoyo técnico</p>	<p>CSIRT alerta campaña de smishing que suplanta un inicio de sesión de correo electrónico</p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00765-01</td></tr> <tr><td>Clase de alerta</td><td>Fraude</td></tr> <tr><td>Tipo de incidente</td><td>Phishing</td></tr> <tr><td>Nivel de riesgo</td><td>Alto</td></tr> <tr><td>TLP</td><td>Blanco</td></tr> <tr><td>Fecha de lanzamiento original</td><td>6 de marzo de 2023</td></tr> <tr><td>Última revisión</td><td>6 de marzo de 2023</td></tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección https://webcocentricen.wapka[.]co/</p> <p>URL sitio falso https://webcocentricen.wapka[.]co/</p> <p>Dirección IP [173.212.225.42]</p> <p>Enlace para revisar loC: https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00765-01.txt</p>	Alerta de seguridad cibernética	8FPH23-00765-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	6 de marzo de 2023	Última revisión	6 de marzo de 2023
Alerta de seguridad cibernética	8FPH23-00765-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	6 de marzo de 2023														
Última revisión	6 de marzo de 2023														

 <p>Regalo día de la mujer Fonasa Chile</p> <p>Debido a la gran cantidad de personas, las recompensas del día de la mujer se distribuirán dentro de dos días. Espere por favor</p> <p>w.entrepreneurialdevastating.cn</p> <p>http://w.entrepreneurialdevastating.cn/8a44AXl4AFgBwN9ISnZDakdLS10ZFwIAxjd00yJTccLFMHaA0pXAMjNkM3XgdJApp-</p>	<p>CSIRT advierte campaña de phishing que suplanta al Fonasa</p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00766-01</td></tr> <tr><td>Clase de alerta</td><td>Fraude</td></tr> <tr><td>Tipo de incidente</td><td>Phishing</td></tr> <tr><td>Nivel de riesgo</td><td>Alto</td></tr> <tr><td>TLP</td><td>Blanco</td></tr> <tr><td>Fecha de lanzamiento original</td><td>6 de marzo de 2023</td></tr> <tr><td>Última revisión</td><td>6 de marzo de 2023</td></tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección http://w.entrepreneurialdevastating.cn/8a44AXl4AFgBwN9ISnZDakdLS10ZFwIAxjd00yJTccLFMHaA0pXAMjNkM3XgdJApp-</p>	Alerta de seguridad cibernética	8FPH23-00766-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	6 de marzo de 2023	Última revisión	6 de marzo de 2023
Alerta de seguridad cibernética	8FPH23-00766-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	6 de marzo de 2023														
Última revisión	6 de marzo de 2023														

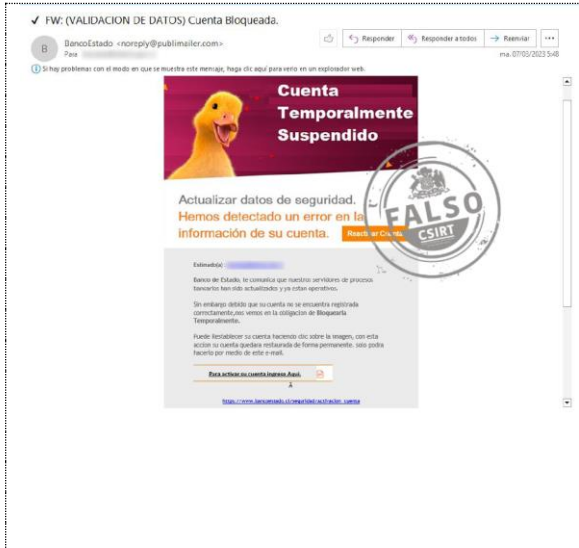
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

ByI1IRBWOH1rAXMAFG80SD4?ttYe1678113459138
URL sitio falso
[https://tmbkkq\[.\]jcyou/ccGhZ80J/fonasawy/?_t=1678122603320#1678122605732](https://tmbkkq[.]jcyou/ccGhZ80J/fonasawy/?_t=1678122603320#1678122605732)
Dirección IP
 [172.64.171.15]
Enlace para revisar loC:
https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00766-01.txt

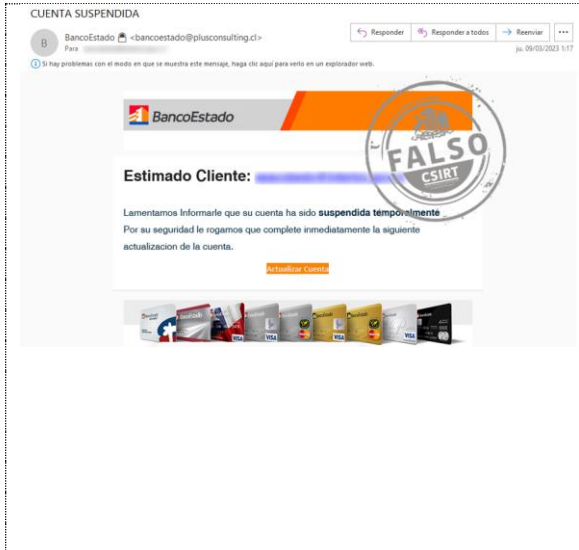
CSIRT informa campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética | 8FPH23-00767-01
Clase de alerta | Fraude
Tipo de incidente | Phishing
Nivel de riesgo | Alto
TLP | Blanco
Fecha de lanzamiento original | 9 de marzo de 2023
Última revisión | 9 de marzo de 2023
Indicadores de compromiso
URL redirección
[https://apply.mituniversity.edu\[.\]jin/activacion/banca-en-linea/](https://apply.mituniversity.edu[.]jin/activacion/banca-en-linea/)
URL sitio falso
[https://underfilehomesteado\[.\]top/1678193232/imagenes/_personas/home/default.asp](https://underfilehomesteado[.]top/1678193232/imagenes/_personas/home/default.asp)
Dirección IP
 [202.89.39.2]
Enlace para revisar loC:
https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00767-01.txt



CSIRT alerta campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética | 8FPH23-00768-01
Clase de alerta | Fraude
Tipo de incidente | Phishing
Nivel de riesgo | Alto
TLP | Blanco
Fecha de lanzamiento original | 9 de marzo de 2023
Última revisión | 9 de marzo de 2023
Indicadores de compromiso
URL redirección
[https://containd3structible\[.\]com/activacion/cuenta-ffca/](https://containd3structible[.]com/activacion/cuenta-ffca/)
URL sitio falso
[https://nwmeponpatito\[.\]club/1678367363/imagenes/_personas/home/default.asp](https://nwmeponpatito[.]club/1678367363/imagenes/_personas/home/default.asp)
Dirección IP
 [172.67.131.190]
Enlace para revisar loC:
https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00768-01.txt



3. Malware

<p>Factura digital</p> <p>JR Jesus Rivera <facturaenlinea@network.org> Para [Redacted]</p> <p>Buenos días.</p> <p>Se adjunta la factura pendiente de pago del servicio con fecha 02/03/2023</p> <p>FACTURA ADJUNTA</p> <p>Favor de revisar a la brevedad.</p> <p>Saludos Cordiales</p> 	<h3>CSIRT advierte campaña de phishing con malware que suplanta a Servipag</h3> <table border="1"><tr><td>Alerta de seguridad cibernética</td><td>2CMV23-00403-01</td></tr><tr><td>Clase de alerta</td><td>Fraude</td></tr><tr><td>Tipo de incidente</td><td>Malware</td></tr><tr><td>Nivel de riesgo</td><td>Alto</td></tr><tr><td>TLP</td><td>Blanco</td></tr><tr><td>Fecha de lanzamiento original</td><td>8 de marzo de 2023</td></tr><tr><td>Última revisión</td><td>8 de marzo de 2023</td></tr></table> <p>Indicadores de compromiso</p> <p>Asunto</p> <p>Factura digital</p> <p>Correo de Salida</p> <p>facturaenlinea@network.org</p> <p>SHA256</p> <pre>69e8f969f539a7673b1378aada96812cf0d53549c54a235934defcee7bd273569cf7217cbd0273f3a37595f7b7c4bb4991391e9932cf90745022e26907e768e743692365c8c951e8929283a345ecfc13a58356add60439bf4e7d103a6be2c2c50fee513762149b1a3f82dca25a5ef05ec542d1cda15891c5eb766c6466542e155f833d1638fb64058d7f968914255a9c90c8479e94512e152949b3cc6b8421be4fc4833ed0036469d258c5d7fbfda93e19fa9a18cb1ddd601a22bc961de0076598e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b</pre> <p>Enlace para revisar IoC:</p> <p>https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00403-01.txt</p>	Alerta de seguridad cibernética	2CMV23-00403-01	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	8 de marzo de 2023	Última revisión	8 de marzo de 2023
Alerta de seguridad cibernética	2CMV23-00403-01														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	8 de marzo de 2023														
Última revisión	8 de marzo de 2023														


4. Concientización

Ciberguía: Cómo protegerse en el mundo digital

Como parte de la conmemoración del Día Internacional de la Mujer compartimos una nueva ciberguía con consejos para protegernos al interactuar con el mundo digital. Puede ser vista en nuestro LinkedIn: <https://www.linkedin.com/feed/update/urn:li:activity:7039317403607957504>.



CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

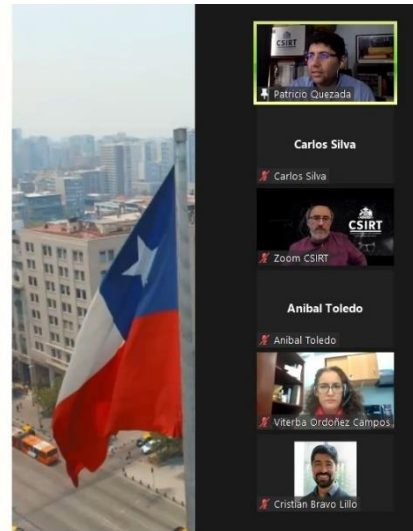
Exitosa charla interactiva para funcionarios públicos sobre efectos del Decreto 273

Especialistas del CSIRT de Gobierno y la Unidad de Coordinación Nacional de Ciberseguridad compartieron ayer las implicancias del Decreto 273 sobre notificación de Incidentes de ciberseguridad con más de 150 encargados de diversos organismos públicos.



DECRETO 273

Artículo 1°	Información sobre amenazas a los órganos de la administración del Estado.
Artículo 2°	Los jefes de servicio establecidos en el artículo 1, dentro del ámbito de sus facultades, y respecto de los contratos que se celebren con posterioridad a la entrada en vigencia del presente decreto, deberán exigir a los proveedores de servicios de tecnologías de la información, que compartan la información sobre las amenazas y vulnerabilidades que puedan afectar a las redes, plataformas y sistemas informáticos de los órganos de la administración del Estado, al igual que las medidas de mitigación aplicadas a éstas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados.
Artículo 3°	
Artículo 4°	



CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

El CSIRT de Gobierno invita a charla de la Fundación Katy Summer este 14 de marzo

El CSIRT de Gobierno y la Fundación Katy Summer invitan a toda la comunidad a una charla online gratuita para hablar sobre el ciberacoso este 14 de marzo, en el marco del Día Nacional Contra el Ciberacoso, a las 9:30 horas.

Inscripciones: <https://registro.interior.gob.cl/charla-ciberacoso>



CHARLA: CÓMO IDENTIFICAR EL CIBERACOSO Y CÓMO ABORDARLO



¿Qué es el ciberacoso o cyberbullying?, ¿qué hacer si mi hijo(a) es víctima?, ¿qué hacer si soy testigo?

Para responder estas y más preguntas, te invitamos a una **charla online gratuita para conversar sobre el ciberacoso.**



Martes 14 de marzo



9:30 horas

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

5. 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.

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>


6. 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.

- Margarita Hermosilla Henríquez
- Jaime
- Leyla Mendoza
- Julián Arias Maetschl
- Bárbara Palacios Cabezas
- Fernando Flores Tobar
- Elizabeth Viviana Parra Cortez

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>