



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 186

Semana del 20 al 26 de enero

## PARCHES COMPARTIDOS

9

Las mitigaciones son útiles en productos de Google y VMware.



## IP INFORMADAS

17

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



## URL ADVERTIDAS

30

Asociadas a sitios fraudulentos y campañas de phishing y malware



## HASH REPORTADOS

9

Asociadas a múltiples campañas de phishing con archivos que contienen malware



# CONTENIDO

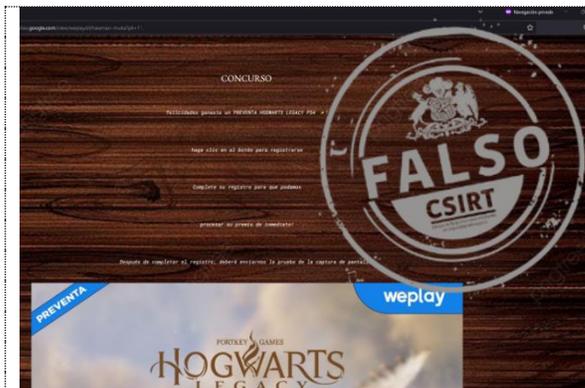
1. Sitios fraudulentos.....	3
2. Phishing.....	5
3. Malware.....	9
4. Vulnerabilidades.....	9
5. Concientización.....	11
6. Recomendaciones y buenas prácticas.....	13
7. Muro de la Fama.....	14



**CSIRT**

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

## 1. Sitios fraudulentos



### CSIRT alerta de página fraudulenta que suplanta a WePlay

Alerta de seguridad cibernética	8FFR23-01201-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2023
Última revisión	23 de enero de 2023

#### Indicadores de compromiso

#### URL sitio falso

[https://sites.google\[.\]com/view/weplaycl/halaman-muka?pli=1%22](https://sites.google[.]com/view/weplaycl/halaman-muka?pli=1%22)

#### Dirección IP

[209.85.145.101]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01201-01/>

<https://www.csirt.gob.cl/media/2023/01/8FFR23-01201-01.pdf>



### CSIRT alerta de sitio fraudulento que suplanta al Banco Falabella

Alerta de seguridad cibernética	8FFR23-01202-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2023
Última revisión	23 de enero de 2023

#### Indicadores de compromiso

#### URL sitio falso

[https://autoservis-cmr.firebaseio\[.\]com/oportunidades?22536528337245feonp](https://autoservis-cmr.firebaseio[.]com/oportunidades?22536528337245feonp)

#### Dirección IP

[199.36.158.100]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01202-01/>

<https://www.csirt.gob.cl/media/2023/01/8FFR23-01202-01-1.pdf>



## CSIRT alerta de una página fraudulenta que suplanta al Banco Santander

Alerta de seguridad cibernética	8FFR23-01203-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2023
Última revisión	24 de enero de 2023

### Indicadores de compromiso

#### URL sitio falso

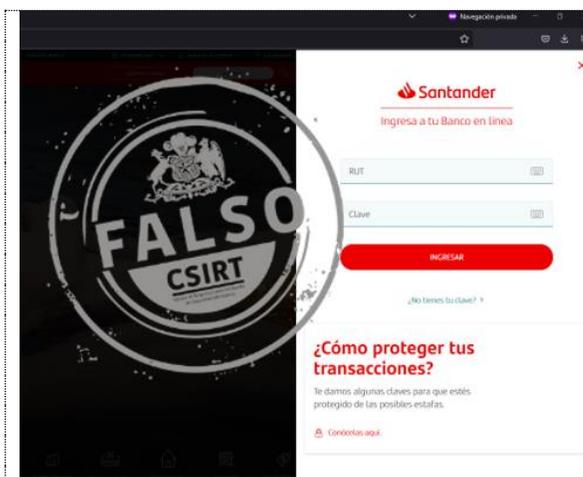
[https://ucmstudio\[.\]info/cuentas/cuenta-test/](https://ucmstudio[.]info/cuentas/cuenta-test/)  
[https://surfsantnder\[.\]info/pagina/login.asp](https://surfsantnder[.]info/pagina/login.asp)

#### Dirección IP

[98.142.101.90]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01203-01/>  
<https://www.csirt.gob.cl/media/2023/01/8FFR23-01203-01.pdf>



## CSIRT alerta de una página fraudulenta que suplanta al Banco Santander

Alerta de seguridad cibernética	8FFR23-01204-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2023
Última revisión	25 de enero de 2023

### Indicadores de compromiso

#### URL sitio falso

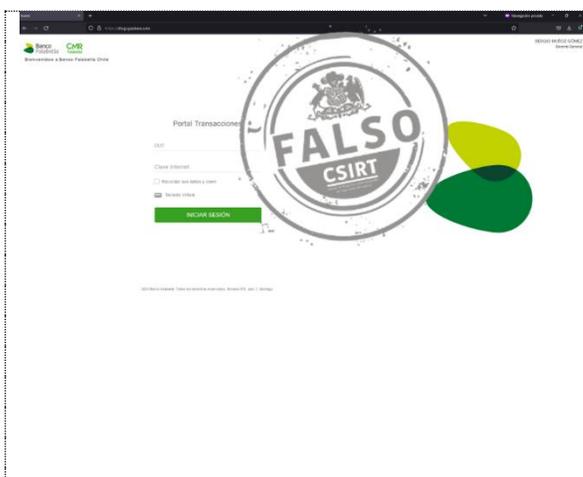
[https://bamco-samtander.cl-sns\[.\]top/1674652583/portada/personas/home.asp](https://bamco-samtander.cl-sns[.]top/1674652583/portada/personas/home.asp)

#### Dirección IP

[104.21.94.40]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01204-01/>  
<https://www.csirt.gob.cl/media/2023/01/8FFR23-01204-01.pdf>



## CSIRT alerta de página fraudulenta que suplanta al Banco Falabella

Alerta de seguridad cibernética	8FFR23-01205-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2023
Última revisión	25 de enero de 2023

### Indicadores de compromiso

#### URL sitio falso

[https://dioguyasbexc\[.\]uno/](https://dioguyasbexc[.]uno/)

#### Dirección IP

[193.84.177.245]

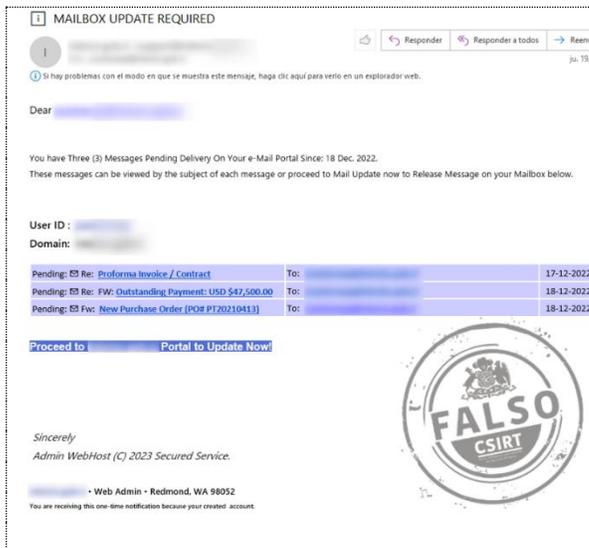
#### Enlaces para revisar el informe:

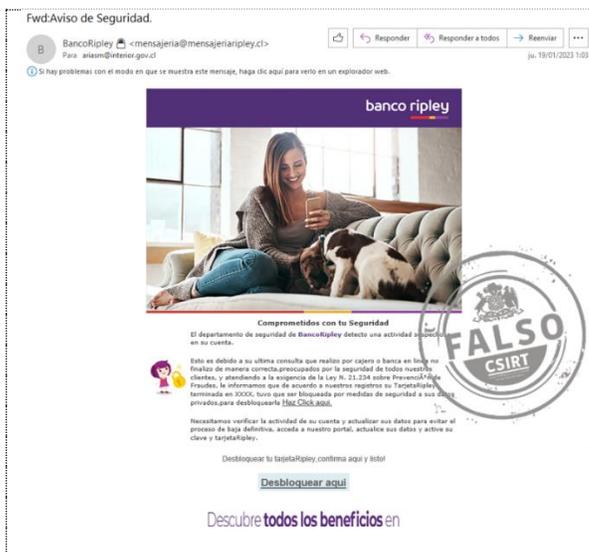
<https://www.csirt.gob.cl/alertas/8ffr23-01205-01/>  
<https://www.csirt.gob.cl/media/2023/01/8FFR23-01205-01.pdf>

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

## 2. Phishing

 <p><b>MAILBOX UPDATE REQUIRED</b></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>Dear [redacted]</p> <p>You have Three (3) Messages Pending Delivery On Your e-Mail Portal Since: 18 Dec. 2022. These messages can be viewed by the subject of each message or proceed to Mail Update now to Release Message on your Mailbox below.</p> <p>User ID : [redacted] Domain : [redacted]</p> <p>Pending: <b>Re: Proforma Invoice / Contract</b> To: [redacted] 17-12-2022 Pending: <b>Re: FW: Outstanding Payment: USD \$47,500.00</b> To: [redacted] 18-12-2022 Pending: <b>Re: Fw: New Purchase Order (PO# P120210413)</b> To: [redacted] 18-12-2022</p> <p>Proceed to <a href="#">Portal to Update Now</a></p> <p>Sincerely Admin WebHost (C) 2023 Secured Service.</p> <p>Web Admin - Redmond, WA 98052 You are receiving this one-time notification because your creator added.</p>	<p><b>CSIRT alerta de campaña de phishing que suplanta página de login de servicio de correo electrónico</b></p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00723-01</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>19 de enero de 2023</td></tr> <tr><td>Última revisión</td><td>19 de enero de 2023</td></tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL sitio falso</b> <a href="https://ipfs.io/ipfs/QmYaBZChBefdcjsjopwYGtWL7AewUkPPVdTgWXoFfwTQumE?filename=oglogz113_cham-e.html#test@csirt.gob.cl">https://ipfs.io/ipfs/QmYaBZChBefdcjsjopwYGtWL7AewUkPPVdTgWXoFfwTQumE?filename=oglogz113_cham-e.html#test@csirt.gob.cl</a></p> <p><b>Dirección IP</b> [209.94.90.1]</p> <p><b>Enlaces para revisar el informe:</b> <a href="https://www.csirt.gob.cl/alertas/8fph23-00723-01/">https://www.csirt.gob.cl/alertas/8fph23-00723-01/</a> <a href="https://www.csirt.gob.cl/media/2023/01/8FPH23-00723-01.pdf">https://www.csirt.gob.cl/media/2023/01/8FPH23-00723-01.pdf</a></p>	Alerta de seguridad cibernética	8FPH23-00723-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	19 de enero de 2023	Última revisión	19 de enero de 2023
Alerta de seguridad cibernética	8FPH23-00723-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	19 de enero de 2023														
Última revisión	19 de enero de 2023														

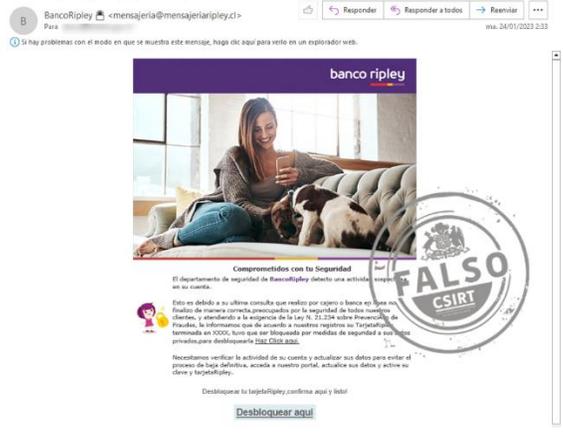
 <p><b>FwdAviso de Seguridad.</b></p> <p>BancoRipley &lt;mensajeria@mensajeriaripley.cl&gt; Para aniam@interior.gob.cl</p> <p>Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.</p> <p><b>banco ripley</b></p> <p>Compremiéndonos con tu Seguridad El departamento de seguridad de BancoRipley detecta una actividad sospechosa en su cuenta.</p> <p>Esto es debido a su última consulta que realizó por cajero o banca en línea no fue posible de manera correcta por razones de seguridad de todos nuestros clientes, y atendiendo a la exigencia de la Ley N. 21.234 sobre Prevención de Fraudes, le informamos que de acuerdo a nuestro registro su TarjetaRipley, terminada en XXXX, tuvo que ser bloqueada por medidas de seguridad a sus datos privados para desbloquearla <a href="#">haga clic aquí</a>.</p> <p>Necesitamos verificar la actividad de su cuenta y actualizar sus datos para evitar el proceso de baja definitiva, acceda a nuestro portal, actualice sus datos y active su clave y tarjetaRipley.</p> <p>Desbloquear tu tarjetaRipley, confirma aquí y listo</p> <p><a href="#">Desbloquear aquí</a></p> <p>Descubre <b>todos los beneficios</b> en</p>	<p><b>CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley</b></p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00724-01</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>24 de enero de 2023</td></tr> <tr><td>Última revisión</td><td>24 de enero de 2023</td></tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b> <a href="https://bit.ly/3HfNI2m?l=www.bancoripley.cl">https://bit.ly/3HfNI2m?l=www.bancoripley.cl</a></p> <p><b>URL sitio falso</b> <a href="http://web.bancoripley.cl.archersbodyworks[.]com.au/1673873742/login">http://web.bancoripley.cl.archersbodyworks[.]com.au/1673873742/login</a></p> <p><b>Dirección IP</b> [185.45.66.125]</p> <p><b>Enlaces para revisar el informe:</b> <a href="https://www.csirt.gob.cl/alertas/8fph23-00724-01/">https://www.csirt.gob.cl/alertas/8fph23-00724-01/</a> <a href="https://www.csirt.gob.cl/media/2023/01/8FPH23-00724-01.pdf">https://www.csirt.gob.cl/media/2023/01/8FPH23-00724-01.pdf</a></p>	Alerta de seguridad cibernética	8FPH23-00724-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	24 de enero de 2023	Última revisión	24 de enero de 2023
Alerta de seguridad cibernética	8FPH23-00724-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	24 de enero de 2023														
Última revisión	24 de enero de 2023														

# Boletín de Seguridad Cibernética N° 186

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

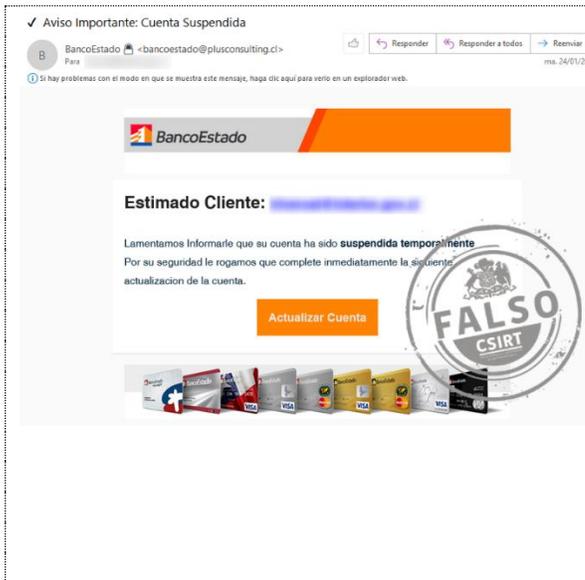
BOLETÍN 13BCS23-00195-01 | SEMANA DEL 20 AL 26 DE ENERO DE 2023

<p>Fwd: Aviso de seguridad - TarjetaRipley Bloqueada</p> <p>BancoRipley &lt;mensajeria@mensajeriaripley.cl&gt;</p> <p>Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.</p> 	<b>CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley</b>	
	Alerta de seguridad cibernética	8FPH23-00725-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	24 de enero de 2023
	Última revisión	24 de enero de 2023
	<b>Indicadores de compromiso</b>	
	<b>URL sitio falso</b>	
<a href="https://t[.]co/wkUrLb38TS">https://t[.]co/wkUrLb38TS</a> <a href="https://sodisiperu[.]com/cl/?index=index">https://sodisiperu[.]com/cl/?index=index</a>		
<b>Dirección IP</b>		
[199.188.200.254]		
<b>Enlaces para revisar el informe:</b>		
<a href="https://www.csirt.gob.cl/alertas/8fph23-00725-01/">https://www.csirt.gob.cl/alertas/8fph23-00725-01/</a> <a href="https://www.csirt.gob.cl/media/2023/01/8FPH23-00725-01.pdf">https://www.csirt.gob.cl/media/2023/01/8FPH23-00725-01.pdf</a>		

<p>Fwd:Aviso.Su tarjetaRipley esta Bloqueada Contactanos.</p> <p>BancoRipley &lt;mensajeria@mensajeriaripley.cl&gt;</p> <p>Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.</p> 	<b>CSIRT alerta de nueva campaña de phishing que suplanta a Banco Ripley</b>	
	Alerta de seguridad cibernética	8FPH23-00726-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	24 de enero de 2023
	Última revisión	24 de enero de 2023
	<b>Indicadores de compromiso</b>	
	<b>URL redirección</b>	
<a href="https://bit.ly/3kzUC9N?l=www.bancoripley.cl">https://bit.ly/3kzUC9N?l=www.bancoripley.cl</a> <a href="https://sam-tech[.]jip/bancoripley/cuenta-ktfs/">https://sam-tech[.]jip/bancoripley/cuenta-ktfs/</a>		
<b>URL sitio falso</b>		
<a href="https://web.bancoripley.cl.gkmayprop[.]com/1674566614/login">https://web.bancoripley.cl.gkmayprop[.]com/1674566614/login</a>		
<b>Dirección IP</b>		
[130.51.180.17]		
<b>Enlaces para revisar el informe:</b>		
<a href="https://www.csirt.gob.cl/alertas/8fph23-00726-01/">https://www.csirt.gob.cl/alertas/8fph23-00726-01/</a> <a href="https://www.csirt.gob.cl/media/2023/01/8FPH23-00726-01.pdf">https://www.csirt.gob.cl/media/2023/01/8FPH23-00726-01.pdf</a>		

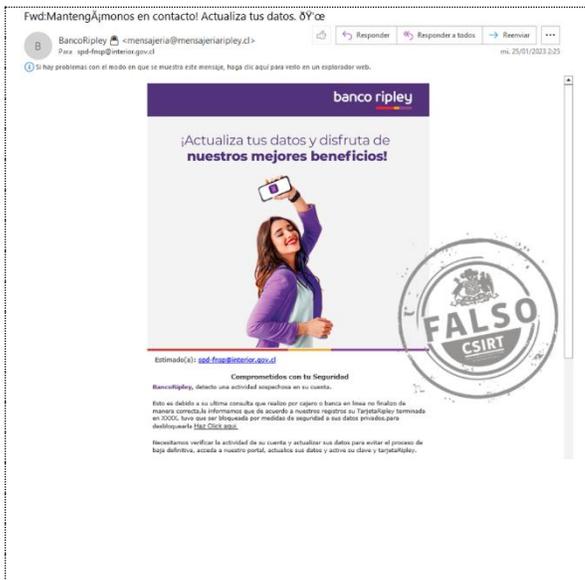
## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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



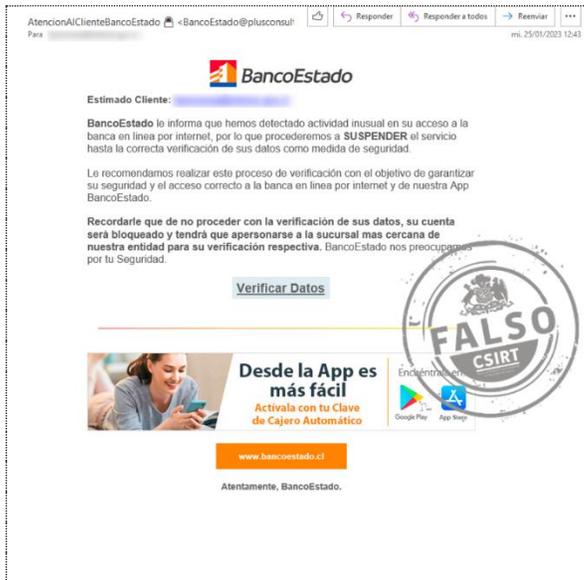
## CSIRT alerta de nueva página de phishing que suplanta a BancoEstado

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



## CSIRT alerta de nueva campaña de phishing que suplanta a Banco Ripley

Alerta de seguridad cibernética	8FPH23-00728-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2023
Última revisión	25 de enero de 2023
<b>Indicadores de compromiso</b>	
<b>URL sitio redirección</b>	
<a href="https://bit[.]ly/3ZVIO3b?l=www.bancoripley.cl">https://bit[.]ly/3ZVIO3b?l=www.bancoripley.cl</a>	
<a href="https://sam-tech[.]jip/bancoripley/cuenta-tscs/">https://sam-tech[.]jip/bancoripley/cuenta-tscs/</a>	
<b>URL sitio falso</b>	
<a href="https://web.bancoripley.cl/gkmayprop[.]com/1674656207/login">https://web.bancoripley.cl/gkmayprop[.]com/1674656207/login</a>	
<b>Dirección IP</b>	
[130.51.180.17]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8fph23-00728-01/">https://www.csirt.gob.cl/alertas/8fph23-00728-01/</a>	
<a href="https://www.csirt.gob.cl/media/2023/01/8FPH23-00728-01.pdf">https://www.csirt.gob.cl/media/2023/01/8FPH23-00728-01.pdf</a>	

	<p><b>CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado</b></p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00729-01</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>26 de enero de 2023</td></tr> <tr><td>Última revisión</td><td>26 de enero de 2023</td></tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b> <a href="https://cartoonpuzzl3s[.]com/activacion/cuenta-vtva/">https://cartoonpuzzl3s[.]com/activacion/cuenta-vtva/</a></p> <p><b>URL sitio falso</b> <a href="https://xtraillconver[.]com/1674670553/imagenes/_personas/home/default.asp">https://xtraillconver[.]com/1674670553/imagenes/_personas/home/default.asp</a></p> <p><b>Dirección IP</b> [138.128.189.154]</p> <p><b>Enlaces para revisar el informe:</b> <a href="https://www.csirt.gob.cl/alertas/8fph23-00729-01/">https://www.csirt.gob.cl/alertas/8fph23-00729-01/</a> <a href="https://www.csirt.gob.cl/media/2023/01/8FPH23-00729-01.pdf">https://www.csirt.gob.cl/media/2023/01/8FPH23-00729-01.pdf</a></p>	Alerta de seguridad cibernética	8FPH23-00729-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	26 de enero de 2023	Última revisión	26 de enero de 2023
Alerta de seguridad cibernética	8FPH23-00729-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	26 de enero de 2023														
Última revisión	26 de enero de 2023														

	<p><b>CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley</b></p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00730-01</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>26 de enero de 2023</td></tr> <tr><td>Última revisión</td><td>26 de enero de 2023</td></tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b> <a href="https://bit[.]ly/3Jl5gLU?l=www.bancoripley.cl">https://bit[.]ly/3Jl5gLU?l=www.bancoripley.cl</a></p> <p><b>URL sitio falso</b> <a href="https://web-bancoripley-cl.gkmayprop[.]com/1674735680/login">https://web-bancoripley-cl.gkmayprop[.]com/1674735680/login</a></p> <p><b>Dirección IP</b> [130.51.180.17]</p> <p><b>Enlaces para revisar el informe:</b> <a href="https://www.csirt.gob.cl/alertas/8fph23-00730-01/">https://www.csirt.gob.cl/alertas/8fph23-00730-01/</a> <a href="https://www.csirt.gob.cl/media/2023/01/8FPH23-00730-01.pdf">https://www.csirt.gob.cl/media/2023/01/8FPH23-00730-01.pdf</a></p>	Alerta de seguridad cibernética	8FPH23-00730-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	26 de enero de 2023	Última revisión	26 de enero de 2023
Alerta de seguridad cibernética	8FPH23-00730-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	26 de enero de 2023														
Última revisión	26 de enero de 2023														

## 3. Malware



### CSIRT alerta de nueva campaña de phishing con malware, que suplanta a Autopase

Alerta de seguridad cibernética	2CMV23-00398-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2023
Última revisión	23 de enero de 2023
<b>Indicadores de compromiso</b>	
<b>Asunto</b>	
Su tag está inhabilitado por deuda.	
<b>Correo de Salida</b>	
postmaster@ashley-howard.co.uk	
<b>SHA256</b>	
f669aba8e7621d7c21ad4553d6899311ecdff561fda86261a496a46c7604d4cc d016b039526f23dcddeec7c511bd7ef439177541504e2998e19d7892481aa7d b753a9dc95ffc2fde9e31d8cbf7b44b59d25e393e7ad6a1e66f6122011b4fef ~~~ 593d0e89345ac495b7ab40fb789a51fd68c4f2f582de7c17c96f52ffa21e00e1 ~~~ bb2a3bbc876eb671233d6980826be466464e7026fd3e2f71c8a825c0de2fa106 206a789ac6eaca1d44d4d89fa77d7e0407cfc9c9cf5917ce4fc2a947328a8f 98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b b3ce811fb696b94f9117ee7fe725ae6b907d695636beceeb1672d5d5eeb81df4 https://facturasnet[.]store/?uQNaBDB6VMIMEOBOuKU4UTuOJAvdL36l6gJMHTG D	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/2cmv23-00398-01/">https://www.csirt.gob.cl/alertas/2cmv23-00398-01/</a>	
<a href="https://www.csirt.gob.cl/media/2023/01/2CMV23-00398-01.pdf">https://www.csirt.gob.cl/media/2023/01/2CMV23-00398-01.pdf</a>	



**INFORME DE Vulnerabilidad**

**9VSA23-00776-01**  
CSIRT comparte vulnerabilidades parchadas por VMware para vRealize Log Insight

PARA REGISTRAR | 15 10  
UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)

**CSIRT**  
Equipo de Respuesta ante Incidentes de Seguridad Informática

## CSIRT comparte información de vulnerabilidades parchadas por VMware para vRealize Log Insight

Alerta de seguridad cibernética	9VSA23-00776-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de enero de 2023
Última revisión	26 de enero de 2023

### CVE

CVE-2022-31703  
CVE-2022-31704  
CVE-2022-31706  
CVE-2022-31710  
CVE-2022-31711

### Fabricantes

VMware

### Productos afectados

VMware vRealize Log Insight 8.x  
VMware Cloud Foundation (VMware vRealize Log Insight) 4.x, 3.x

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00776-01/>  
<https://www.csirt.gob.cl/media/2022/12/9VSA22-00776-01.pdf>



**INFORME DE Vulnerabilidad**

**9VSA23-00777-01**  
CSIRT comparte vulnerabilidades parchadas en Google Chrome 109

PARA REGISTRAR | 15 10  
UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)

**CSIRT**  
Equipo de Respuesta ante Incidentes de Seguridad Informática

## CSIRT comparte vulnerabilidades en varios productos de Juniper Networks

Alerta de seguridad cibernética	9VSA23-00777-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	26 de enero de 2023
Última revisión	26 de enero de 2023

### CVE

CVE-2023-0471  
CVE-2023-0472  
CVE-2023-0473  
CVE-2023-0474

### Fabricantes

Juniper Networks

### Productos afectados

Google Chrome, versiones anteriores a la 109

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00777-01/>  
<https://www.csirt.gob.cl/media/2023/01/9VSA23-00777-01.pdf>

## 5. Concientización

### Ciberconsejos | Día de la Protección de Datos Personales

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

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



**#Ciberconsejos**  
**Día de la Protección de nuestros Datos Personales**

Según la ley chilena, datos personales son "cualquier información concerniente a personas naturales, identificadas o identificables".

Entre los datos personales más relevantes están:

- RUT, teléfono, dirección.
- Datos bancarios.
- Información comercial.
- Usuarios y contraseñas.
- Fotos e información íntima.



**#Ciberconsejos**  
**Día de la Protección de nuestros Datos Personales**

Es importante proteger nuestros datos personales porque:

- Permiten identificarnos y seguir nuestras acciones o desplazamientos.
- Su uso por terceros puede perjudicar nuestra reputación, involucrarnos en delitos y robarnos dinero.
- Pueden ser usados para chantajear.
- Saber qué compramos o buscamos en internet permite desarrollar publicidad dirigida y discriminar a algunas personas.



**#Ciberconsejos**  
**Día de la Protección de nuestros Datos Personales**

Los ciudadanos tienen derechos sobre cómo tratan sus datos empresas y gobiernos (Ley 19.628 de 1999, actualizada en 2020)

Cómo proteger nuestros datos personales

- Verifica la identidad de quien pide datos personales. Nunca los entregues a menos que sea estrictamente necesario.
- No des contraseñas o códigos a terceros.
- Compra solo en páginas web oficiales.
- Activa doble factor de autenticación en todas tus apps.



**#Ciberconsejos**  
**Día de la Protección de nuestros Datos Personales**

Cómo proteger nuestros datos personales

- No utilices wifi públicas para realizar transacciones bancarias o comerciales.
- Actualiza tu software, incluyendo apps.
- Crea distintas contraseñas para cada cuenta.
- Ten cuidado con la información que compartes en las redes sociales. Evita publicar dónde vives, tu RUT, fotos de carnet o dónde estudian tus hijos.
- Si te ves obligado a entregar una fotocopia de tu carnet, tapa su número de documento.
- Revisa los ajustes de privacidad en cada app.

### CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

## Ciberdiccionario Volumen 27

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

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



**CSIRT** | Ciberdiccionario  
Equipo de Respuesta ante Incidentes de Seguridad Informática

### DATOS ABIERTOS

De "open data", en inglés, se refiere a datos que están disponibles para todo público, de forma libre y gratuita, para usar de cualquier manera, sin requerir permiso del autor. Existe un movimiento que promueve la puesta a disposición del público de este tipo de datos. En Chile contamos con [datos.gob.cl](https://datos.gob.cl) como portal de datos abiertos del Estado.



**CSIRT** | Ciberdiccionario  
Equipo de Respuesta ante Incidentes de Seguridad Informática

### INFOSTEALER

Tipo de programa malicioso (malware) dedicado a robar información. Son usados principalmente por delincuentes para hacerse de la información privada, como usuarios y contraseñas del banco u otra institución de pagos de la víctima. Un ejemplo de infostealer son los key-loggers, que copian y filtran la información de lo marcado en el teclado del equipo.



**CSIRT** | Ciberdiccionario  
Equipo de Respuesta ante Incidentes de Seguridad Informática

### BUZONEO

Táctica de los delincuentes para tomar control de una cuenta de WhatsApp. Si logra que el código de recuperación de la víctima llegue al buzón de voz de la misma, y la clave del buzón no es robusta, pueden adivinarla y conseguir el código. Sugerimos activar el 2do factor de autenticación en WhatsApp y considerar pedir a la compañía telefónica desactivar el buzón de voz.



**CSIRT** | Ciberdiccionario  
Equipo de Respuesta ante Incidentes de Seguridad Informática

### CRIPTOSTAFA

También llamadas cryptoscams, son engaños basados en las denominadas criptomonedas (y similares activos digitales) para robar el dinero de sus víctimas. Muchas veces las estafas en sí mismas no son nada nuevo, pero al exigir pago en criptomonedas, se dificulta recuperar los fondos y perseguir a los delincuentes. ¡Nunca creas en ofertas o concursos no solicitados ni hagas clic en enlaces desconocidos!



## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

## 6. Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar que los sitios web a los que se ingrese sean los oficiales.

### CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

## 7. Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar campañas de phishing, malware y/o sitios fraudulentos.

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

- Daniza Irene Mesa Vega
- Cristián Venegas

### CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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