



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 182

SEMANA DEL 23 AL 29 DE DICIEMBRE

# LA SEMANA EN CIFRAS

## PARCHES COMPARTIDOS



1

Las mitigaciones son útiles en productos de GitHub.

## IP INFORMADAS



16

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

## URL ADVERTIDAS



25

Asociadas a sitios fraudulentos y campañas de phishing y malware

# CONTENIDO

1. Sitios fraudulentos .....	3
2. Phishing.....	8
3. Vulnerabilidades .....	12
4. Actualidad .....	13
5. Concientización.....	14
6. Recomendaciones y buenas prácticas.....	16
7. Muro de la Fama .....	17



**CSIRT**

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

## 1. Sitios fraudulentos

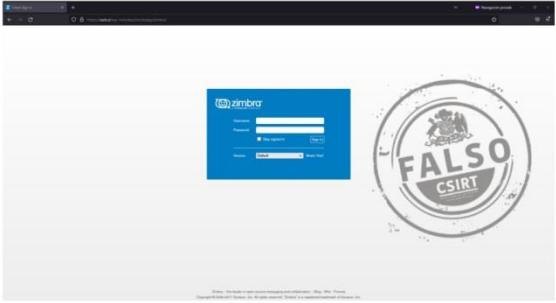
Imagen del sitio		<b>CSIRT alerta de sitio fraudulento que suplanta a Zimbra</b>		
	Alerta de seguridad cibernética	8FFR22-01175-01		
	Clase de alerta	Fraude		
	Tipo de incidente	Falsificación de Registros o Identidad		
	Nivel de riesgo	Alto		
	TLP	Blanco		
	Fecha de lanzamiento original	23 de diciembre de 2022		
	Última revisión	23 de diciembre de 2022		
	<b>Indicadores de compromiso</b>			
	<b>URL sitio falso</b>			
	<a href="https://cark[.]cl/wp-includes/zim/today/zimbra/">https://cark[.]cl/wp-includes/zim/today/zimbra/</a>			
<b>Dirección IP</b>				
[190.13.188.108]				
<b>Enlaces para revisar el informe:</b>				
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01175-01/">https://www.csirt.gob.cl/alertas/8ffr22-01175-01/</a>				
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01175-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01175-01.pdf</a>				

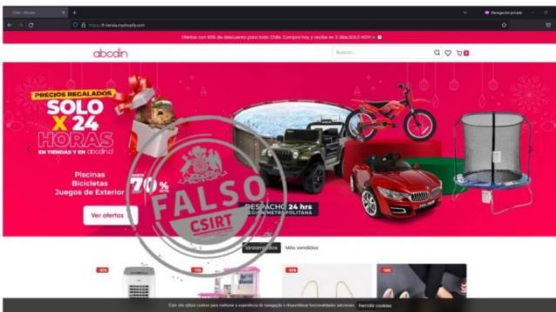

Imagen del sitio		<b>CSIRT alerta de sitio fraudulento que suplanta a ABCDIN</b>		
	Alerta de seguridad cibernética	8FFR22-01176-01		
	Clase de alerta	Fraude		
	Tipo de incidente	Falsificación de Registros o Identidad		
	Nivel de riesgo	Alto		
	TLP	Blanco		
	Fecha de lanzamiento original	23 de diciembre de 2022		
	Última revisión	23 de diciembre de 2022		
	<b>Indicadores de compromiso</b>			
	<b>URL sitio falso</b>			
	<a href="https://fl-tienda.myshopify[.]com/">https://fl-tienda.myshopify[.]com/</a>			
<b>Dirección IP</b>				
[23.227.38.74]				
<b>Enlaces para revisar el informe:</b>				
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01176-01/">https://www.csirt.gob.cl/alertas/8ffr22-01176-01/</a>				
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01176-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01176-01.pdf</a>				

Imagen del sitio		<b>CSIRT alerta de nueva página fraudulenta que suplanta al Banco Santander</b>		
	Alerta de seguridad cibernética	8FFR22-01177-01		
	Clase de alerta	Fraude		
	Tipo de incidente	Falsificación de Registros o Identidad		
	Nivel de riesgo	Alto		
	TLP	Blanco		
	Fecha de lanzamiento original	23 de diciembre de 2022		
	Última revisión	23 de diciembre de 2022		
	<b>Indicadores de compromiso</b>			
	<b>URL sitio falso</b>			
	https[:]//shukuyaratay[.]top/1671819832/portada/personas/home.asp			
<b>Dirección IP</b>				
[172.67.195.69]				
<b>Enlaces para revisar el informe:</b>				
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01177-01/">https://www.csirt.gob.cl/alertas/8ffr22-01177-01/</a>				
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01177-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01177-01.pdf</a>				

Imagen del sitio		<b>CSIRT alerta de página fraudulenta que suplanta a Cencosud Scotiabank</b>		
	Alerta de seguridad cibernética	8FFR22-01178-01		
	Clase de alerta	Fraude		
	Tipo de incidente	Falsificación de Registros o Identidad		
	Nivel de riesgo	Alto		
	TLP	Blanco		
	Fecha de lanzamiento original	27 de diciembre de 2022		
	Última revisión	27 de diciembre de 2022		
	<b>Indicadores de compromiso</b>			
	<b>URL redirección</b>			
	https://is[.]gd/rQMXVk			
<b>URL sitio falso</b>				
https://www.ayuda-cencosud.cl.townrealstate.com/1672153669/login/index.html				
<b>Dirección IP</b>				
[185.146.22.242]				
<b>Enlaces para revisar el informe:</b>				
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01178-01/">https://www.csirt.gob.cl/alertas/8ffr22-01178-01/</a>				
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01178-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01178-01.pdf</a>				

## Imagen del sitio



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

Alerta de seguridad cibernética	8FFR22-01179-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de diciembre de 2022
Última revisión	27 de diciembre de 2022

#### Indicadores de compromiso

##### URL sitio falso

[https://portalpersonas-bancochile.cl.sanhitaphotography\[.\]com/1672154353/bchile-web/persona/login/index.html/login](https://portalpersonas-bancochile.cl.sanhitaphotography[.]com/1672154353/bchile-web/persona/login/index.html/login)

##### Dirección IP

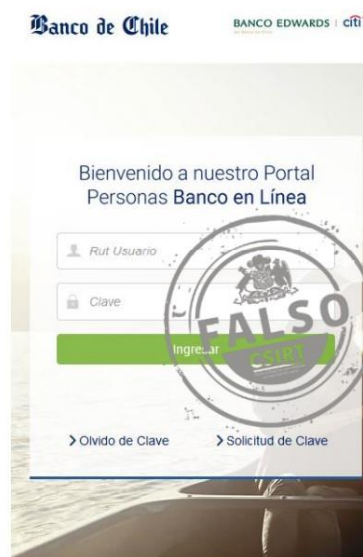
[162.241.85.230]

##### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01179-01/>

<https://www.csirt.gob.cl/media/2022/12/8FFR22-01179-01.pdf>

## Imagen del sitio



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

Alerta de seguridad cibernética	8FFR22-01180-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de diciembre de 2022
Última revisión	27 de diciembre de 2022

#### Indicadores de compromiso

##### URL sitio falso

[https://www.logIn.portal-bancochile.cl.scruma\[.\]xyz/1672154732/bchile-web/persona/login/index.html/login](https://www.logIn.portal-bancochile.cl.scruma[.]xyz/1672154732/bchile-web/persona/login/index.html/login)

##### Dirección IP

[68.66.224.44]

##### Enlaces para revisar el informe:

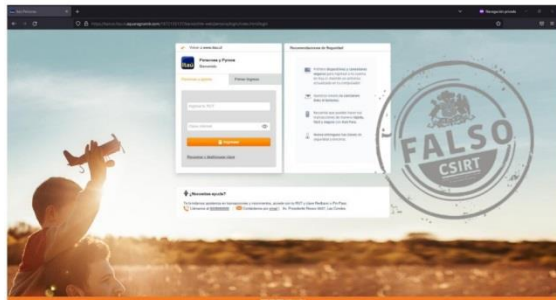
<https://www.csirt.gob.cl/alertas/8ffr22-01180-01/>

<https://www.csirt.gob.cl/media/2022/12/8FFR22-01180-01.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>

## Imagen del sitio



### CSIRT alerta de una página fraudulenta que suplanta a Banco Itaú

Alerta de seguridad cibernética	8FFR22-01181-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de diciembre de 2022
Última revisión	27 de diciembre de 2022

#### Indicadores de compromiso

##### URL sitio falso

[https://banco.itaui.cl/aquaragnarok\[.\]com/1672155137/bancochile-web/persona/login/index.html/login](https://banco.itaui.cl/aquaragnarok[.]com/1672155137/bancochile-web/persona/login/index.html/login)

##### Dirección IP

[103.227.176.25]

##### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01181-01/>

<https://www.csirt.gob.cl/media/2022/12/8FFR22-01181-01.pdf>

## Imagen del sitio



### CSIRT alerta ante página fraudulenta que suplanta al Banco Santander

Alerta de seguridad cibernética	8FFR22-01182-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de diciembre de 2022
Última revisión	27 de diciembre de 2022

#### Indicadores de compromiso

##### URL sitio falso

[https://santanderchile-personas.dmklaws.co\[.\]ke/1672163976/portada/personas/home.asp](https://santanderchile-personas.dmklaws.co[.]ke/1672163976/portada/personas/home.asp)

##### Dirección IP

[109.106.250.12]

##### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01182-01/>

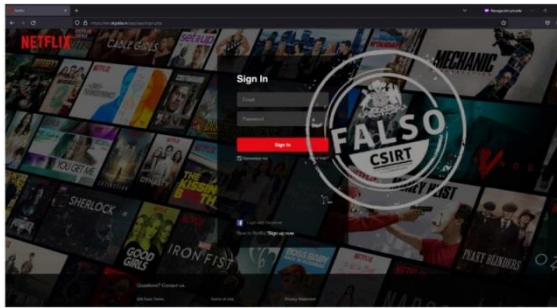
<https://www.csirt.gob.cl/media/2022/12/8FFR22-01182-01.pdf>

# Boletín de Seguridad Cibernética N° 182

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

BOLETÍN 13BCS22-00191-01 | SEMANA DEL 23 AL 29 DE DICIEMBRE DE 2022





## Imagen del sitio



## CSIRT alerta ante página fraudulenta que suplanta a Netflix


Alerta de seguridad cibernética	8FFR22-01183-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de diciembre de 2022
Última revisión	29 de diciembre de 2022
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	
<a href="http://dev.skydda[.]in/app/app/index.php">http://dev.skydda[.]in/app/app/index.php</a>	
<b>Dirección IP</b>	
[150.242.140.198]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01183-01/">https://www.csirt.gob.cl/alertas/8ffr22-01183-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01183-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01183-01.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](mailto:soc-csirt@interior.gob.cl)  
 @csirtgob  
 <https://www.linkedin.com/company/csirt-gob>



## 2. Phishing

<p><b>Imagen del mensaje</b></p> 	<p><b>CSIRT alerta una campaña de phishing que suplanta a Líder BCI</b></p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH22-00689-01</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>23 de diciembre de 2022</td> </tr> <tr> <td>Última revisión</td> <td>23 de diciembre de 2022</td> </tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b> https[:]//bit[.]ly/3B7lhCL</p> <p><b>URL sitio falso</b> https[:]//lidereenservicios.filmnanciero[.]com/1671797758/login</p> <p><b>Dirección IP</b> [172.67.130.81]</p> <p><b>Enlaces para revisar el informe:</b> https://www.csirt.gob.cl/alertas/8fph22-00689-01/ https://www.csirt.gob.cl/media/2022/12/8FPH22-00689-01.pdf</p>	Alerta de seguridad cibernética	8FPH22-00689-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	23 de diciembre de 2022	Última revisión	23 de diciembre de 2022
Alerta de seguridad cibernética	8FPH22-00689-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	23 de diciembre de 2022														
Última revisión	23 de diciembre de 2022														

<p><b>Imagen del mensaje</b></p> 	<p><b>CSIRT advierte campaña de phishing que suplanta al Banco Ripley</b></p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH22-00690-01</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 diciembre de 2022</td> </tr> <tr> <td>Última revisión</td> <td>26 de diciembre de 2022</td> </tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b> https[:]//bit[.]ly/3WMxent?l=www.bancoripley.cl</p> <p><b>URL sitio falso</b> https[:]//web-bancoripleycl.buckreality[.]net/1672058924/login</p> <p><b>Dirección IP</b> [64.91.247.208]</p> <p><b>Enlaces para revisar el informe:</b> https://www.csirt.gob.cl/alertas/8fph22-00690-01/ https://www.csirt.gob.cl/media/2022/12/8FPH22-00690-01.pdf</p>	Alerta de seguridad cibernética	8FPH22-00690-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	26 de diciembre de 2022	Última revisión	26 de diciembre de 2022
Alerta de seguridad cibernética	8FPH22-00690-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	26 de diciembre de 2022														
Última revisión	26 de diciembre de 2022														

### 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>

Imagen del mensaje	CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
	Alerta de seguridad cibernética	8FPH22-00691-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	26 de diciembre de 2022
	Última revisión	26 de diciembre de 2022
	<b>Indicadores de compromiso</b>	
	<b>URL redirección</b>	
	<a href="https://bit.ly/3WMxent?l=www.bancoripley.cl">https://bit.ly/3WMxent?l=www.bancoripley.cl</a>	
	<b>URL sitio falso</b>	
	<a href="https://web.bancoripley-cl.buckrealty[.]net/1672083269/login">https://web.bancoripley-cl.buckrealty[.]net/1672083269/login</a>	
	<b>Dirección IP</b>	
	[64.91.247.208]	
	<b>Enlaces para revisar el informe:</b>	
	<a href="https://www.csirt.gob.cl/alertas/8fph22-00691-01/">https://www.csirt.gob.cl/alertas/8fph22-00691-01/</a>	
	<a href="https://www.csirt.gob.cl/media/2022/12/8FPH22-00691-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FPH22-00691-01.pdf</a>	

Imagen del mensaje	CSIRT alerta de nueva campaña de phishing que suplanta al Banco Santander	
	Alerta de seguridad cibernética	8FPH22-00692-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	27 de diciembre de 2022
	Última revisión	27 de diciembre de 2022
	<b>Indicadores de compromiso</b>	
	<b>URL redirección</b>	
	<a href="https://t[.]co/Wg8ni2PMei">https://t[.]co/Wg8ni2PMei</a>	
	<a href="https://grupocantoperu[.]com/es/?index=index">https://grupocantoperu[.]com/es/?index=index</a>	
	<b>URL sitio falso</b>	
	<a href="https://santanderchile-personas.pn-koba.go[.]id/1672144923/portada/personas/home.asp">https://santanderchile-personas.pn-koba.go[.]id/1672144923/portada/personas/home.asp</a>	
	<b>Dirección IP</b>	
	[151.106.118.172]	
	<b>Enlaces para revisar el informe:</b>	
	<a href="https://www.csirt.gob.cl/alertas/8fph22-00692-01/">https://www.csirt.gob.cl/alertas/8fph22-00692-01/</a>	
	<a href="https://www.csirt.gob.cl/media/2022/12/8FPH22-00692-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FPH22-00692-01.pdf</a>	


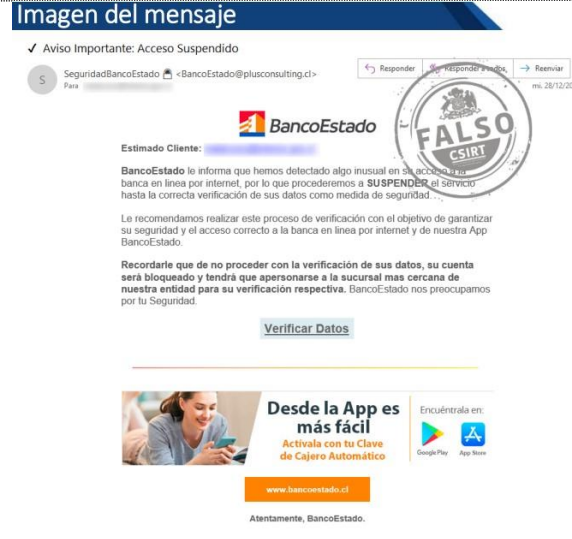
Imagen del mensaje		CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
		Alerta de seguridad cibernética	8FPH22-00693-01
		Clase de alerta	Fraude
		Tipo de incidente	Phishing
		Nivel de riesgo	Alto
		TLP	Blanco
		Fecha de lanzamiento original	22 de noviembre de 2022
		Última revisión	22 de noviembre de 2022
		<b>Indicadores de compromiso</b>	
		<b>URL sitio falso</b>	
		<a href="https://smscotito[.]info/1672163418/imagenes/_personas/home/default.asp">https://smscotito[.]info/1672163418/imagenes/_personas/home/default.asp</a>	
		<b>URL sitio redirección</b>	
		<a href="https://ucmstudio[.]info/activacion/cuenta-aotq/">https://ucmstudio[.]info/activacion/cuenta-aotq/</a>	
		<b>Dirección IP</b>	
		[104.21.13.190]	
		<b>Enlaces para revisar el informe:</b>	
		<a href="https://www.csirt.gob.cl/alertas/8fph22-00693-01/">https://www.csirt.gob.cl/alertas/8fph22-00693-01/</a>	
		<a href="https://www.csirt.gob.cl/media/2022/12/8FPH22-00693-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FPH22-00693-01.pdf</a>	

Imagen del mensaje		CSIRT advierte campaña de phishing que suplanta al BancoEstado	
		Alerta de seguridad cibernética	8FPH22-00694-01
		Clase de alerta	Fraude
		Tipo de incidente	Phishing
		Nivel de riesgo	Alto
		TLP	Blanco
		Fecha de lanzamiento original	28 de diciembre de 2022
		Última revisión	28 de diciembre de 2022
		<b>Indicadores de compromiso</b>	
		<b>URL sitio falso</b>	
		<a href="https://nmhpatito[.]info/1672231561/imagenes/_personas/home/default.asp">https://nmhpatito[.]info/1672231561/imagenes/_personas/home/default.asp</a>	
		<b>URL sitio redirección</b>	
		<a href="https://ibkpatatan[.]com/activacion/cuenta-kbqe/">https://ibkpatatan[.]com/activacion/cuenta-kbqe/</a>	
		<b>Dirección IP</b>	
		[162.241.60.24]	
		<b>Enlaces para revisar el informe:</b>	
		<a href="https://www.csirt.gob.cl/alertas/8fph22-00694-01/">https://www.csirt.gob.cl/alertas/8fph22-00694-01/</a>	
		<a href="https://www.csirt.gob.cl/media/2022/12/8FPH22-00694-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FPH22-00694-01.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>

Imagen del mensaje	CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado		
	Alerta de seguridad cibernética	8FPH22-00695-01	
	Clase de alerta	Fraude	
	Tipo de incidente	Phishing	
	Nivel de riesgo	Alto	
	TLP	Blanco	
	Fecha de lanzamiento original	29 de diciembre de 2022	
	Última revisión	29 de diciembre de 2022	
	<b>Indicadores de compromiso</b>		
	<b>URL sitio falso</b>	<a href="https://nmhpatito[.]info/1672339580/imagenes/_personas/home/default.asp">https://nmhpatito[.]info/1672339580/imagenes/_personas/home/default.asp</a>	
	<b>URL sitio redirección</b>	<a href="https://balarockpop[.]com/activacion/cuenta-vfhh/">https://balarockpop[.]com/activacion/cuenta-vfhh/</a>	
<b>Dirección IP</b>	[162.241.60.24]		
<b>Enlaces para revisar el informe:</b>	<a href="https://www.csirt.gob.cl/alertas/8fph22-00695-01/">https://www.csirt.gob.cl/alertas/8fph22-00695-01/</a>		
	<a href="https://www.csirt.gob.cl/media/2022/12/8FPH22-00695-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FPH22-00695-01.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://twitter.com/csirtgob)
- <https://www.linkedin.com/company/csirt-gob>

## 3. Vulnerabilidades



### CSIRT comparte nueva vulnerabilidad en GitHub

Alerta de seguridad cibernética	9VSA22-00759-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	29 de diciembre de 2022
Última revisión	29 de diciembre de 2022

### CVE

CVE-2022-4848

### Fabricantes

GitHub

### Productos afectados





GitHub, versiones anteriores a 0.9.1.

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00759-01/>

<https://www.csirt.gob.cl/media/2022/12/9VSA22-00759-01.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://www.linkedin.com/company/csirt-gob>

## 4. Actualidad

### CSIRT de Gobierno realiza ejercicio de ciberseguridad para la Asociación del Retail Financiero en coordinación con Kaspersky

Como parte del convenio que la Asociación del Retail Financiero suscribió con el Equipo de Respuesta Ante Incidentes de Seguridad Informática (CSIRT de Gobierno), dependiente del Ministerio del Interior, el lunes 19 de diciembre más de 35 ejecutivos de las empresas que integran el comité de ciberseguridad de la Asociación, participaron en la Kaspersky Interactive Protection Simulation (KIPS).



Al respecto, Carlos Silva, jefe del CSIRT de Gobierno, explicó que “para nosotros es importante llevar la capacitación y concientización en ciberseguridad no solo en el mundo público sino también en el privado, porque nuestro objetivo no es proteger solo a la infraestructura de red si no que fundamentalmente a las personas, al ciudadano que confía en empresas e instituciones para depositar sus datos personales”.





La instancia de capacitación, ya organizada anteriormente con gran éxito para encargados de ciberseguridad de organismos públicos, consta de un juego de simulación virtual e interactivo desarrollado por Kaspersky, conocida compañía de ciberseguridad, en que los ejecutivos de cada empresa se enfrentaron a los ciberataques más comunes en Chile y Latinoamérica, debiendo tomar decisiones para contrarrestar sus efectos y resguardar la seguridad de la operación. Entre las particularidades de este juego figura el hecho que ante cada evento que va ocurriendo, cambia el modo en que se desarrolla la situación, debiendo evaluar constantemente sus decisiones.

Este es el primer ejercicio de esta naturaleza que el CSIRT de Gobierno realiza con entidades del sector privado, iniciando en este caso con un módulo diseñado especialmente para la industria del retail financiero, orientado a proteger frente amenazas avanzadas que pueden afectar a estas instituciones.

Al finalizar la simulación, los ejecutivos cuentan con nuevas herramientas de respuesta ante posibles escenarios de ciberataque, para incorporarlos a sus estrategias de seguridad, como también identificar oportunidades de mejora.

Entre las empresas que participaron figuran Banco Falabella, Cencosud- Scotiabank, Banco Ripley, Líder BCI, SBPay, Hites y ABCDin.

#### 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>

## 5. Concientización

### Ciberconsejos para el uso seguro de Whatsapp

WhatsApp es una de las plataformas de mensajería más utilizada en el mundo, con más de 2.000 millones de usuarios activos. Esto lo hace un blanco atractivo para los ciberdelincuentes que a través de distintas técnicas buscan obtener algún tipo de beneficio, suplantando la identidad de los usuarios. Para usar de forma segura esta red social, el CSIRT de Gobierno preparó los consejos de esta semana.

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



**CIBERCONSEJOS para el uso seguro de WhatsApp**

**1 NUNCA ENTREGUES TU CÓDIGO DE VERIFICACIÓN**

Una técnica que utilizan los ciberdelincuentes para robar las cuentas de WhatsApp es solicitando el código que te llega a través de un SMS, suplantando la identidad de un amigo o conocido.



**CIBERCONSEJOS para el uso seguro de WhatsApp**

**2 CONFIGURA LA AUTENTICACIÓN EN DOS PASOS**

Para activar el doble factor de autenticación, sigue estos pasos:

- Ingresa al menú ajustes de WhatsApp.
- Cuenta.
- Verificación en dos pasos.
- Activar.



**CIBERCONSEJOS para el uso seguro de WhatsApp**

**3 ACTIVA DESBLOQUEO CON RECONOCIMIENTO FACIAL**

En caso de que tu smartphone lo permita, puedes activar esta medida de seguridad ingresando al menú de ajustes ➤ **cuenta** ➤ **privacidad** ➤ **activar bloqueo** de pantalla y reconocimiento facial.



**CIBERCONSEJOS para el uso seguro de WhatsApp**

**4 CIERRA WHATSAPP WEB SI NO LO ESTÁS USANDO**

Evita que otras personas accedan a tu WhatsApp. Para cerrarlo de forma correcta, puedes ir a:

- Configuración desde la app.
- Dispositivos vinculados.
- Cerrar sesión utilizada.



## Ciberdiccionario Volumen 26

Esta semana en el ciberdiccionario del CSIRT de Gobierno explicamos los conceptos: spoofing, actor de amenazas, SMTP y sitio web falso: <https://csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-26/>.



### Ciberdiccionario

**SPOOFING:**

Acción de los ciberdelincuentes de ocultar su identidad haciéndose pasar por otras personas o instituciones. Este término se usa principalmente para cuando se envía un email que aparenta venir de una fuente confiable, como puede ser un jefe, con el objetivo de engañar al receptor y robar dinero a él o su empresa.



### Ciberdiccionario

**ACTOR DE AMENAZAS:**

Personas o entidades que provocan incidentes de seguridad digital, lo hagan voluntariamente o no. Este concepto a su vez se divide en cuatro tipos: cibercriminales, hacktivistas, amenazas internas (dentro de la organización amenazada) y grupos estatales o apoyados por Estados.



### Ciberdiccionario

**SMTP:**

Sigla de "Protocolo de Transporte Simple de Correo", es un estándar de comunicación de correo electrónico proveniente de los años setenta y actualizado en numerosas ocasiones. Siendo el protocolo más usado, también es el más atacado por ciberdelincuentes.



### Ciberdiccionario

**SITIO WEB FALSO:**

Es un sitio web no legítimo. Por lo general, son creados con el objetivo de engañar a las personas para robar información confidencial, dinero, vender falsos productos, etc. En algunos casos, suplantan la identidad de una marca reconocida.









## 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

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

## 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.

Carlos Escalona

Fernando Flores





Juan Berrios

Martin Cevallos

Michael Hudson

Sebastian Muñoz

### 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://twitter.com/csirtgob)  
 <https://www.linkedin.com/company/csirt-gob>