



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 181

SEMANA DEL 16 AL 22 DE DICIEMBRE

# LA SEMANA EN CIFRAS

## PARCHES COMPARTIDOS

24

Las mitigaciones son útiles en productos de Fortinet y Atlassian.



## IP INFORMADAS

24

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



## HASH REPORTADOS

3

Asociadas a múltiples campañas de phishing con archivos que contienen malware



# CONTENIDO

1. Malware.....
2. Ataques de fuerza bruta.....
3. Sitios fraudulentos.....
4. Phishing.....
5. Vulnerabilidades.....
6. Actualidad.....
7. Concientización.....
8. Recomendaciones y buenas prácticas.....
9. Muro de la Fama.....

## 1. Malware

 <p>RE: Payment</p> <p>"AI Fang" &lt;gerardo@mufftrading.com&gt; Para</p> <p>TT Payment Decap 010 KB</p> <p>Dear:</p> <p>Good Day,</p> <p>We have arranged the remittance of US\$56,475.00 as payment against your invoices# 3000000852.</p> <p>Please find attached herewith a scan copy of the TT application for your reference. Kindly confirm once you receive the payment.</p> <p>Best regards,</p> <p>AI Fang AFNAN PERFUMES LLC P.O. Box 7771 Surf Industrial I Nasser China Mall Ajman, U.A.E. Tel: +971 6 747 4441 Fax: +971 6 747 4114 Mob: +971 522031676 Website: www.afnan.com</p> <p>Virus-free. <a href="http://www.avast.com">www.avast.com</a></p>	<b>CSIRT alerta de campaña de phishing con malware, que suplanta a Muff Trading</b>	
	Alerta de seguridad cibernética	2CMV22-00394-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	19 de diciembre de 2022
	Última revisión	19 de diciembre de 2022
	<b>Indicadores de compromiso</b>	
	<b>Asunto</b>	
RE: Payment		
<b>Correo de salida</b>		
gerardo@mufftrading[.]com		
<b>SHA256</b>		
b375ace043904ca1884316d38124698993ffb28ed27cae8deb3559867d16e7cb589c67cd28abd40173abc9bfe2fb2b80eaa905bc8bd0be9b70d04c73829a7423 TT589c67cd28abd40173abc9bfe2fb2b80eaa905bc8bd0be9b70d04c73829a7423		
<b>URL</b>		
mail.sseximclearing[.]com:587		
<b>Enlaces para revisar el informe:</b>		
<a href="https://www.csirt.gob.cl/alertas/2cmv22-00394-01/">https://www.csirt.gob.cl/alertas/2cmv22-00394-01/</a>		
<a href="https://www.csirt.gob.cl/media/2022/12/2CMV22-00394-01.pdf">https://www.csirt.gob.cl/media/2022/12/2CMV22-00394-01.pdf</a>		

## 2. Ataques de fuerza bruta



Ministerio del Interior y Seguridad Pública

**ALERTA DE Fuerza Bruta**

4IIV22-00058-01

**CSIRT alerta de ataques de fuerza bruta contra SMTP**

PARA REGISTRAR | 562 2486 3850  
UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)

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

### CSIRT alerta de ataques de fuerza bruta contra el protocolo SMTP

Alerta de seguridad cibernética	4IIV22-00058-01
Clase de alerta	Intento de intrusión
Tipo de incidente	Intento de intrusión – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2022
Última revisión	20 de diciembre de 2022

### Indicadores de compromiso

#### Direcciones IP

[80.94.95.206]  
[103.74.103.3]  
[192.227.217.208]  
[141.98.10.236]  
[103.153.78.188]  
[176.111.173.54]

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/4iiv22-00058-01/>  
<https://www.csirt.gob.cl/media/2022/12/4IIV22-00058-01.pdf>

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

## 3. Sitios fraudulentos



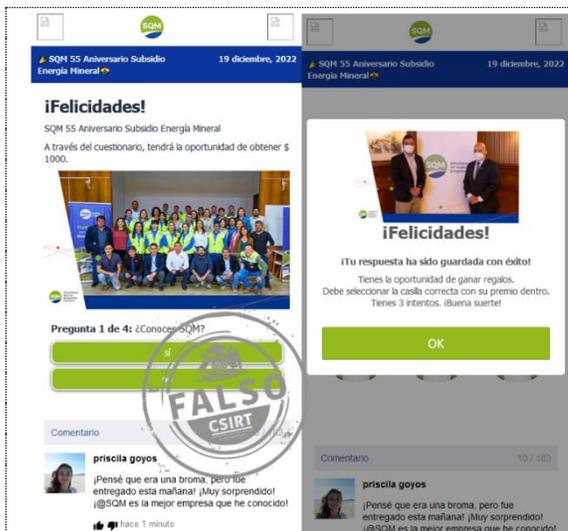
**CSIRT alerta de una página fraudulenta que suplanta a Fonasa**

Alerta de seguridad cibernética	8FFR22-01163-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de diciembre de 2022
Última revisión	7 de diciembre de 2022
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	
<a href="https://://analystrefuse[.]top/2s4UrH3C/fonasaw/?_t=1671133961633#1671134157104">https://://analystrefuse[.]top/2s4UrH3C/fonasaw/?_t=1671133961633#1671134157104</a>	
<b>Dirección IP</b>	
[172.67.188.84]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01163-01/">https://www.csirt.gob.cl/alertas/8ffr22-01163-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01163-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01163-01.pdf</a>	



**CSIRT alerta de una página fraudulenta que suplanta al Jumbo**

Alerta de seguridad cibernética	8FFR22-01164-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de diciembre de 2022
Última revisión	15 de diciembre de 2022
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	
<a href="https://://analystrefuse[.]top/WD5O9nYJ/jumbo-Christmas/?_t=1671135090835#1671135091839">https://://analystrefuse[.]top/WD5O9nYJ/jumbo-Christmas/?_t=1671135090835#1671135091839</a>	
<b>Dirección IP</b>	
[172.67.188.84]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01164-01/">https://www.csirt.gob.cl/alertas/8ffr22-01164-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01164-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01164-01.pdf</a>	



## CSIRT alerta de página fraudulenta que suplanta a SQM

Alerta de seguridad cibernética	8FFR22-01165-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022

### Indicadores de compromiso

#### URL sitio falso

[https://bpathd\[.\]cyou/H7t7E3fG/sqmw/?\\_t=1671452098934#1671452102428](https://bpathd[.]cyou/H7t7E3fG/sqmw/?_t=1671452098934#1671452102428)

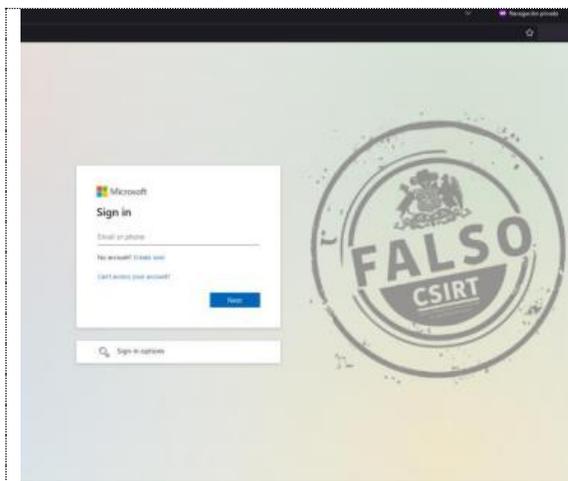
#### Dirección IP

[172.67.219.202]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01165-01/>

<https://www.csirt.gob.cl/media/2022/12/8FFR22-01165-01.pdf>



## CSIRT alerta por página fraudulenta que suplanta a Microsoft

Alerta de seguridad cibernética	8FFR22-01166-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022

### Indicadores de compromiso

#### URL sitio falso

[https://sjcsbm\[.\]ru/ID-63a05f04b8fda](https://sjcsbm[.]ru/ID-63a05f04b8fda)

#### Dirección IP

[172.67.219.202]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01166-01/>

<https://www.csirt.gob.cl/media/2022/12/8FFR22-01166-01.pdf>

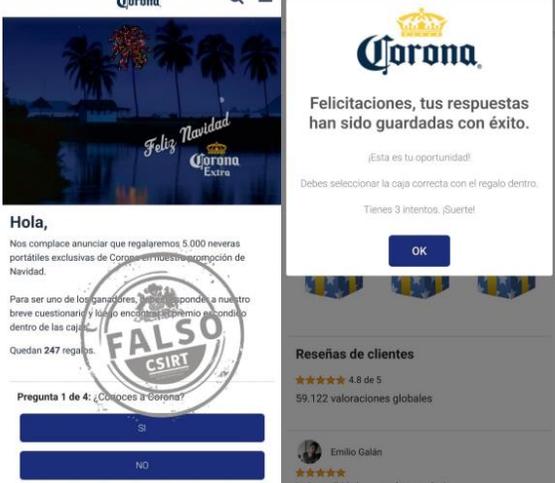
# Boletín de Seguridad Cibernética N° 181

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

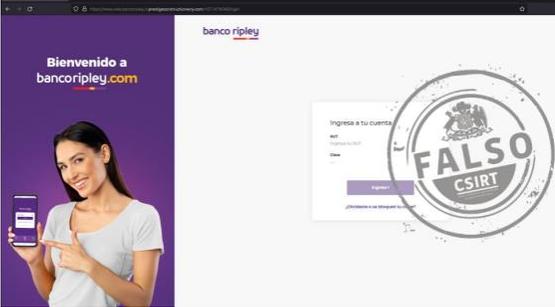
BOLETÍN 13BCS22-00190-01 | SEMANA DEL 16 AL 22 DE DICIEMBRE DE 2022



<b>CSIRT alerta de una página fraudulenta que suplanta a Adobe Acrobat</b>	
Alerta de seguridad cibernética	8FFR22-01167-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	
<a href="https://www.patagonia-nuestra.cl/invioces/inv/index.php">https://www.patagonia-nuestra.cl/invioces/inv/index.php</a>	
<b>Dirección IP</b>	
[186.64.116.35]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01167-01/">https://www.csirt.gob.cl/alertas/8ffr22-01167-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01167-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01167-01.pdf</a>	



<b>CSIRT alerta de una página fraudulenta que suplanta a cerveza Corona</b>	
Alerta de seguridad cibernética	8FFR22-01168-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	
<a href="https://tinyurl4.ru/BRUwjIMy/">https://tinyurl4.ru/BRUwjIMy/</a>	
<a href="https://tinyurl4.ru/BRUwjIMy/#1671463113414">https://tinyurl4.ru/BRUwjIMy/#1671463113414</a>	
<b>Dirección IP</b>	
[104.21.84.153]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01168-01/">https://www.csirt.gob.cl/alertas/8ffr22-01168-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01168-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01168-01.pdf</a>	



<b>CSIRT alerta de página fraudulenta que suplanta a Banco Ripley</b>	
Alerta de seguridad cibernética	8FFR22-01169-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	
<a href="https://www.web.bancoripley.cl/prestigeconstructionwny[.]com/1671474048/ogin">https://www.web.bancoripley.cl/prestigeconstructionwny[.]com/1671474048/ogin</a>	
<b>Dirección IP</b>	
[192.185.21.172]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01169-01/">https://www.csirt.gob.cl/alertas/8ffr22-01169-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01169-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01169-01.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>



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

Alerta de seguridad cibernética	8FFR22-01170-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022

### Indicadores de compromiso

#### URL sitio falso

[https://brancosantander-cl.clavecl\[.\]top/1671474365/portada/personas/home.asp](https://brancosantander-cl.clavecl[.]top/1671474365/portada/personas/home.asp)

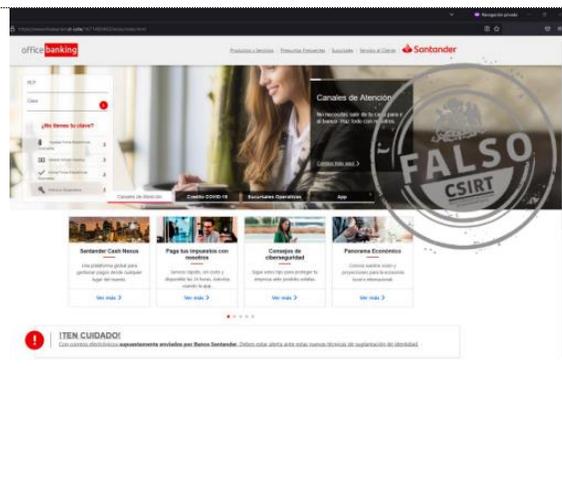
#### Dirección IP

[104.21.17.124]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01170-01/>

<https://www.csirt.gob.cl/media/2022/12/8FFR22-01170-01.pdf>



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

Alerta de seguridad cibernética	8FFR22-01171-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022

### Indicadores de compromiso

#### URL sitio falso

[https://wwwoficebankin-cl-\[.\]site/1671478897/inicio/index.html](https://wwwoficebankin-cl-[.]site/1671478897/inicio/index.html)

#### Dirección IP

[104.21.55.136]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01171-01/>

<https://www.csirt.gob.cl/media/2022/12/8FFR22-01171-01.pdf>



## CSIRT alerta ante sitio fraudulento que suplanta a cerveza Corona

Alerta de seguridad cibernética	8FFR22-01172-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2022
Última revisión	21 de diciembre de 2022

### Indicadores de compromiso

#### URL sitio falso

[https://tinyurl4\[.\]ru/chrcorlat/#1671635678096](https://tinyurl4[.]ru/chrcorlat/#1671635678096)

#### Dirección IP

[172.64.199.36]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01172-01/>

<https://www.csirt.gob.cl/media/2022/12/8FFR22-01172-01.pdf>



## CSIRT alerta de 1.849 sitios fraudulentos que suplantan a populares marcas

Alerta de seguridad cibernética	8FFR22-01173-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2022
Última revisión	21 de diciembre de 2022

### Indicadores de compromiso

#### URL sitio falso

[https://tinyurl4\[.\]ru/](https://tinyurl4[.]ru/)

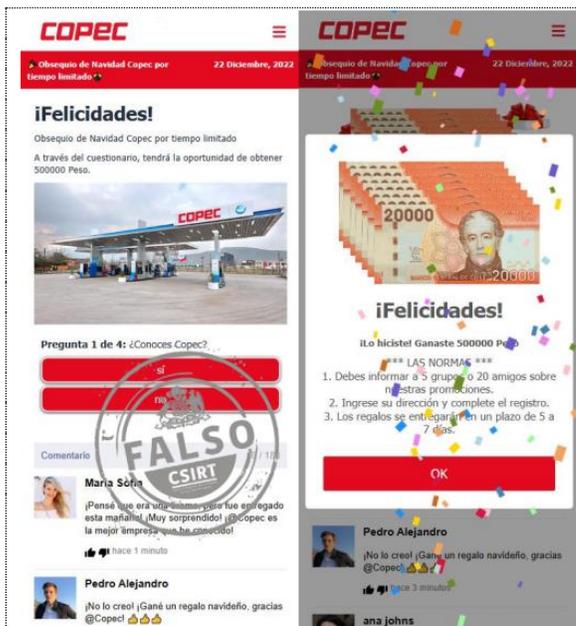
#### Dirección IP

[172.64.199.36]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01173-01/>

<https://www.csirt.gob.cl/media/2022/12/8FFR22-01173-01.pdf>

	<p><b>CSIRT alerta de una página fraudulenta que suplanta a Copec</b></p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FFR22-01174-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Falsificación de Registros o Identidad</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>21 de diciembre de 2022</td> </tr> <tr> <td>Última revisión</td> <td>21 de diciembre de 2022</td> </tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL sitio falso</b></p> <p><a href="https[:]//wldtco[.]cyou/IN8PHMDm/Copecwa/?_t=1671717370065#1671717897263">https[:]//wldtco[.]cyou/IN8PHMDm/Copecwa/?_t=1671717370065#1671717897263</a></p> <p><b>Dirección IP</b></p> <p>[104.21.2.203]</p> <p><b>Enlaces para revisar el informe:</b></p> <p><a href="https://www.csirt.gob.cl/alertas/8ffr22-01174-01/">https://www.csirt.gob.cl/alertas/8ffr22-01174-01/</a></p> <p><a href="https://www.csirt.gob.cl/media/2022/12/8FFR22-01174-01.pdf">https://www.csirt.gob.cl/media/2022/12/8FFR22-01174-01.pdf</a></p>	Alerta de seguridad cibernética	8FFR22-01174-01	Clase de alerta	Fraude	Tipo de incidente	Falsificación de Registros o Identidad	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	21 de diciembre de 2022	Última revisión	21 de diciembre de 2022
Alerta de seguridad cibernética	8FFR22-01174-01														
Clase de alerta	Fraude														
Tipo de incidente	Falsificación de Registros o Identidad														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	21 de diciembre de 2022														
Última revisión	21 de diciembre de 2022														

## 4. Phishing



Esperando el pago.

Hola,  
Está Ud. recibiendo este correo electrónico desde su propia cuenta. Eso se debe a que tengo acceso total a su dispositivo.

Llevo unos meses vigilándole.  
¿No sabe cómo es posible? Usted ha sido infectado con un software mío en un sitio que visitó. Por si no está familiarizado con esto, voy a explicarlo.

Con la ayuda de este software, he obtenido total acceso a un PC o a cualquier otro dispositivo. Eso significa que puedo ver siempre que quiera frente a la pantalla, con solo encender la cámara y el micrófono sin que usted se de cuenta. Además, también tengo acceso a su lista de contactos y a todos sus correos electrónicos.

¿Pero mi equipo tiene un antivirus activo, ¿cómo fue posible? ¿Por qué no he recibido ningún aviso?  
La respuesta es simple: mi software utiliza controladores propios, lo que me permite actualizar sus actividades. Las firmas y el comportamiento no sea detectado, y por ende su antivirus se mantiene inactivo.

Le informo que cuento con un video en el que sale masturbándose, y del lado derecho el video que está en su computadora.  
¿En qué puede perjudicarme esto? Con una sola pulsación de ratón, puedo enviar el video a todas sus redes sociales, correo electrónico.

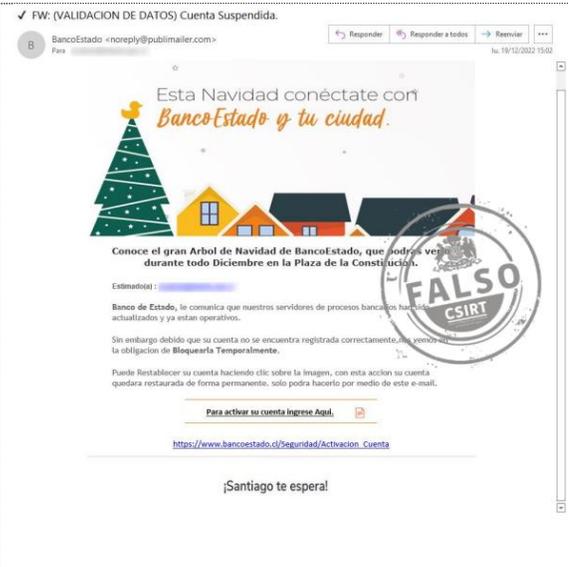
También puedo compartir todos sus mensajes de correo electrónico así como sus conversaciones de messenger y de whatsapp app.

Si desea evitar que todo esto suceda solo debe transferir bitcoins por valor de 7508 USD (setecientos cincuenta dólares americanos) a mi dirección bitcoin (si no tiene ni idea de cómo hacerlo, puede abrir el navegador y simplemente buscar: "Comprar bitcoins").

**CSIRT alerta de campaña de phishing con sextorsión**

Alerta de seguridad cibernética	8FPH22-00681-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022

**Enlaces para revisar el informe:**  
<https://www.csirt.gob.cl/alertas/8fph22-00681-01/>  
<https://www.csirt.gob.cl/media/2022/12/8FPH22-00681-01.pdf>



✓ FW: (VALIDACION DE DATOS) Cuenta Suspendida.

BancoEstado <noreply@publmailier.com>  
Para [redacted] la: 19/12/2022 15:03

Esta Navidad conéctate con BancoEstado y tu ciudad.

Conoce el gran Arbol de Navidad de BancoEstado, que podrás ver durante todo Diciembre en la Plaza de la Construcción.

Estimado(a): [redacted]

Banco de Estado, le comunica que nuestros servidores de procesos bancarios han sido actualizados y ya están operativos.

Sin embargo debido que su cuenta no se encuentra registrada correctamente, usted tiene la obligación de Bloquear su Temporalmente.

Puede Restablecer su cuenta haciendo clic sobre la imagen, con esta acción su cuenta quedará restaurada de forma permanente, solo podrá hacerlo por medio de este e-mail.

[Para activar su cuenta Ingrese Aquí.](https://www.bancoestado.cl/Seguridad/Activacion_Cuenta)

[https://www.bancoestado.cl/Seguridad/Activacion\\_Cuenta](https://www.bancoestado.cl/Seguridad/Activacion_Cuenta)

¡Santiago te espera!

**CSIRT alerta de campaña de phishing que suplanta a BancoEstado**

Alerta de seguridad cibernética	8FPH22-00682-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2022
Última revisión	19 de diciembre de 2022

**Indicadores de compromiso**

**URL redirección**  
[https://ucmstudio\[.\]info/activacion/cuenta-aotq/](https://ucmstudio[.]info/activacion/cuenta-aotq/)

**URL sitio falso**  
[https://newbailando\[.\]com/1671473291/imagenes/\\_personas/home/default.asp](https://newbailando[.]com/1671473291/imagenes/_personas/home/default.asp)

**Dirección IP**  
 [104.21.7.84]

**Enlaces para revisar el informe:**  
<https://www.csirt.gob.cl/alertas/8fph22-00682-01/>  
<https://www.csirt.gob.cl/media/2022/12/8FPH22-00682-01.pdf>



✓ Notificación: Cuenta Deshabilitado

SeguridadBancoEstado <BancoEstado@plusconsulting.cl>  
Para [redacted] ma: 20/12/2022 08:58

**BancoEstado**

Estimado Cliente: [redacted]

BancoEstado le informa que hemos detectado algo inusual en su acceso a la banca en línea por internet, por lo que procederemos a SUSPENDER el servicio hasta la correcta verificación de sus datos como medida de seguridad.

Le recomendamos realizar este proceso de verificación con el objetivo de garantizar su seguridad y el acceso correcto a la banca en línea por internet y de nuestra App BancoEstado.

Recordarle que de no proceder con la verificación de sus datos, su cuenta será bloqueada y tendrá que acercarse a la sucursal más cercana de nuestra entidad para su verificación respectiva. BancoEstado no puede ser responsable por su Seguridad.

[Verificar Datos](#)

Desde la App es más fácil  
Activa con tu Clave de Cajero Automático

[www.bancoestado.cl](https://www.bancoestado.cl)

Atentamente, BancoEstado.

**CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado**

Alerta de seguridad cibernética	8FPH22-00683-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2022
Última revisión	20 de diciembre de 2022

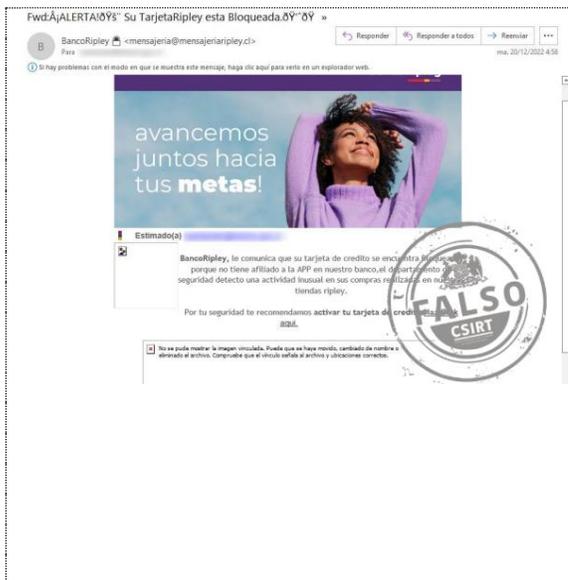
**Indicadores de compromiso**

**URL redirección**  
[https://avengerpati\[.\]com/activacion/cuenta-veqo/](https://avengerpati[.]com/activacion/cuenta-veqo/)

**URL sitio falso**  
[https://nmhpatito\[.\]info/1671548369/imagenes/\\_personas/home/default.asp](https://nmhpatito[.]info/1671548369/imagenes/_personas/home/default.asp)

**Dirección IP**  
 [162.241.60.25]

**Enlaces para revisar el informe:**  
<https://www.csirt.gob.cl/alertas/8fph22-00683-01/>  
<https://www.csirt.gob.cl/media/2022/12/8FPH22-00683-01.pdf>



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

Alerta de seguridad cibernética	8FPH22-00684-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de diciembre de 2022
Última revisión	20 de diciembre de 2022

### Indicadores de compromiso

#### URL redirección

<https://bit.ly/3G5nHSG?l=www.bancoripley.cl>  
<https://worldwidefakenote.com/bancoripley/cuenta-jhpc/>

#### URL sitio falso

<https://web-bancoripley-cl.wonthaggicaravans.com.jau/1671549855/login>

#### Dirección IP

[203.26.41.136]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00684-01/>  
<https://www.csirt.gob.cl/media/2022/12/8FPH22-00684-01.pdf>



## CSIRT alerta de campaña de phishing por WhatsApp, que suplanta a Coca-Cola

Alerta de seguridad cibernética	8FPH22-00685-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de diciembre de 2022
Última revisión	21 de diciembre de 2022

### Indicadores de compromiso

#### URL redirección

<https://tinyurl4.ru/WuBGTYXv/>

#### Dirección IP

[172.64.199.36]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00685-01/>  
<https://www.csirt.gob.cl/media/2022/12/8FPH22-00685-01.pdf>



## CSIRT alerta ante campaña de phishing por Whatsapp que suplanta a Líder

Alerta de seguridad cibernética	8FPH22-00686-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de noviembre de 2022
Última revisión	21 de noviembre de 2022

### Indicadores de compromiso

#### URL sitio falso

<https://lnkshort.ru/ETSbcxBs/#1671627265184>

#### Dirección IP

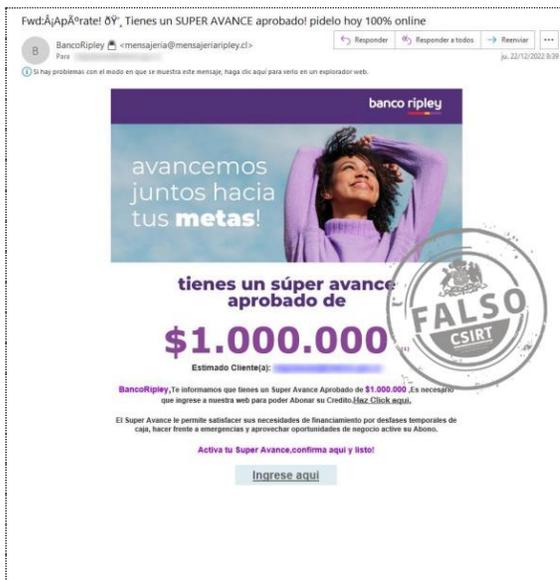
[172.67.190.26]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00686-01/>  
<https://www.csirt.gob.cl/media/2022/12/8FPH22-00686-01.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>



## CSIRT alerta de campaña de phishing que suplanta al Banco Ripley

Alerta de seguridad cibernética	8FPH22-00687-01
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

### Indicadores de compromiso

#### URL sitio falso

[https://web-bancoripley-cl.buckrealty\[.\]net/1671711266/login](https://web-bancoripley-cl.buckrealty[.]net/1671711266/login)

#### URL sitio redirección

[https://bit\[.\]ly/3ChUzFR?l=www.bancoripley.cl](https://bit[.]ly/3ChUzFR?l=www.bancoripley.cl)

[https://web-bancoripley-cl.buckrealty\[.\]net/](https://web-bancoripley-cl.buckrealty[.]net/)

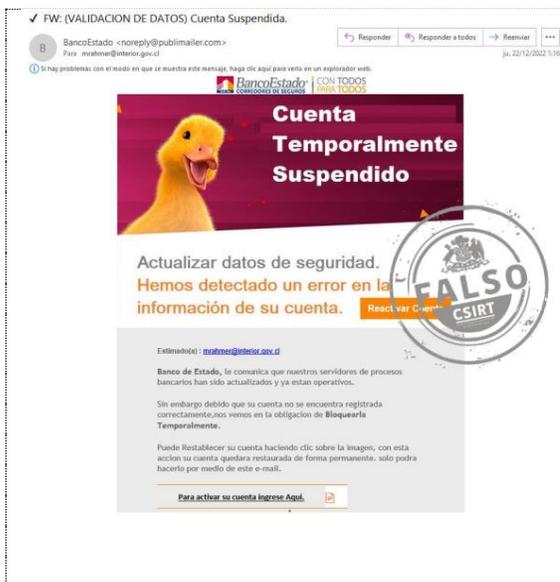
#### Dirección IP

[64.91.247.208]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00687-01/>

<https://www.csirt.gob.cl/media/2022/12/8FPH22-00687-01.pdf>



## CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado

Alerta de seguridad cibernética	8FPH22-00688-01
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

### Indicadores de compromiso

#### URL sitio falso

[https://newbailando\[.\]com/1671712402/imagenes/\\_personas/home/default.asp](https://newbailando[.]com/1671712402/imagenes/_personas/home/default.asp)

#### URL sitio redirección

<https://ucmstudio.info/activacion/cuenta-aotq/>

#### Dirección IP

[173.249.58.117]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00688-01/>

<https://www.csirt.gob.cl/media/2022/12/8FPH22-00688-01.pdf>

## 5. Vulnerabilidades



**INFORME DE Vulnerabilidad**

**9VSA22-00756-01**  
CSIRT alerta vulnerabilidades en productos VMware, incluyendo algunas críticas

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



**CSIRT alerta de varias vulnerabilidades que afectan a diversos productos de VMware**

Alerta de seguridad cibernética	9VSA22-00756-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	19 de diciembre de 2022	
Última revisión	19 de diciembre de 2022	
<b>CVE</b>		
CVE-2021-39144	CVE-2022-31693	CVE-2022-31703
CVE-2022-31678	CVE-2022-31696	CVE-2022-31700
CVE-2022-31685	CVE-2022-31697	CVE-2022-31701
CVE-2022-31686	CVE-2022-31698	CVE-2022-31705
CVE-2022-31687	CVE-2022-31699	CVE-2022-31707
CVE-2022-31688	CVE-2022-31702	CVE-2022-31708
CVE-2022-31689		
<b>Fabricantes</b>	VMware	
<b>Productos afectados</b>	VMware Cloud Foundation VMware Workspace ONE Assist VMware Tools for Windows VMware ESXi and vCenter Server VMware vRealize Network Insight (vRNI) VMware Workspace ONE Access (Access) VMware Identity Manager (vidm) VMware Cloud Foundation (Cloud Foundation)	
<b>Enlaces para revisar el informe:</b>	<a href="https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00756-01/">https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00756-01/</a> <a href="https://www.csirt.gob.cl/media/2022/12/9VSA22-00756-01.pdf">https://www.csirt.gob.cl/media/2022/12/9VSA22-00756-01.pdf</a>	



**INFORME DE Vulnerabilidad**

**9VSA22-00757-01**  
CSIRT alerta de vulnerabilidades en Samba

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



**CSIRT alerta de vulnerabilidades que afectan a Samba**

Alerta de seguridad cibernética	9VSA22-00757-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	20 de diciembre de 2022	
Última revisión	20 de diciembre de 2022	
<b>CVE</b>		
CVE-2022-38023	CVE-2022-37967	
CVE-2022-37966	CVE-2022-45141	
<b>Fabricantes</b>	Samba	
<b>Productos afectados</b>	Versiones de Samba anteriores a 4.17.4, 4.16.8 y 4.15.13.	
<b>Enlaces para revisar el informe:</b>	<a href="https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00757-01/">https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00757-01/</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>

 <p>Ministerio del Interior y Seguridad Pública</p> <p><b>INFORME DE Vulnerabilidad</b></p> <p><b>9VSA22-00758-01</b> CSIRT comparte información de vulnerabilidad CVE-2022-42821 en macOS</p> <p>PARA REGISTRAR   15 10 UN INCIDENTE   <a href="http://www.csirt.gob.cl">www.csirt.gob.cl</a></p> 	<a href="https://www.csirt.gob.cl/media/2022/12/9VSA22-00757-01.pdf">https://www.csirt.gob.cl/media/2022/12/9VSA22-00757-01.pdf</a>	
	<b>CSIRT alerta de vulnerabilidad de riesgo medio en macOS</b>	
	Alerta de seguridad cibernética	9VSA22-00758-01
	Clase de alerta	Vulnerabilidad
	Tipo de incidente	Sistema y/o Software Abierto
	Nivel de riesgo	Medio
	TLP	Blanco
	Fecha de lanzamiento original	20 de diciembre de 2022
	Última revisión	20 de diciembre de 2022
	<b>CVE</b>	
CVE-2022-42821		
<b>Fabricantes</b>		
Apple		
<b>Productos afectados</b>		
Versiones anteriores a macOS Monterey 12.6.2, macOS Big Sur 11.7.2 y macOS Ventura 13.		
<b>Enlaces para revisar el informe:</b>		
<a href="https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00758-01/">https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00758-01/</a>		
<a href="https://www.csirt.gob.cl/media/2022/12/9VSA22-00758-01.pdf">https://www.csirt.gob.cl/media/2022/12/9VSA22-00758-01.pdf</a>		

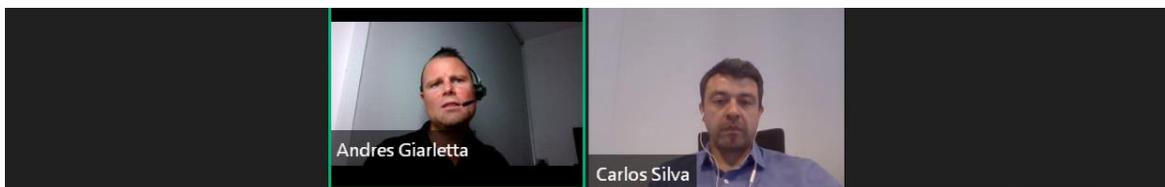
## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <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>

## 6. Actualidad

### Simulación de entrenamiento para el Retail Financiero

El lunes 19 de diciembre, como parte del convenio que la Asociación del Retail Financiero suscribió con el CSIRT de Gobierno, más de 35 ejecutivos de las empresas que integran el comité de ciberseguridad de la Asociación, participaron en la Kaspersky Interactive Protection Simulation (KIPS). La instancia de capacitación consta de un juego de simulación virtual e interactivo desarrollado por Kaspersky, instancia en que los participantes 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.



### La interfaz de la consola



### 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. Concientización

### Ciberconsejos para evitar caer en concursos falsos

Durante diciembre, y a días de la Navidad, este tipo de fraudes han comenzado a propagarse de forma más recurrente. Delincuentes difunden a través de WhatsApp o mensajes de texto un falso sorteo y solicitan difundir la falsa campaña entre sus amigos. Quienes hagan clic son redirigidas a sitios web maliciosos que solicitan sus datos de tarjeta de crédito. Además, existe la posibilidad que los delincuentes secuestren el WhatsApp de la víctima.

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



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

### CIBERCONSEJOS PARA EVITAR CAER EN CONCURSOS FALSOS

#### TÉCNICAS UTILIZADAS PARA DIFUNDIR CONCURSOS FALSOS

- **PHISHING:** Correo electrónico que suplanta la identidad de una institución o persona.
- **SMISHING:** Estafa que circula por mensajes de texto (SMS) o WhatsApp.

**EN AMBOS CASOS, LAS PERSONAS SON REDIRIGIDAS A SITIOS WEB FALSOS.**



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

### CIBERCONSEJOS PARA EVITAR CAER EN CONCURSOS FALSOS

#### ALGUNOS RIESGOS

- Robo de contraseña.
- Pérdidas económicas.
- Secuestro de WhatsApp.
- Redirección a sitios web maliciosos.
- Pérdida de datos personales.
- Descarga de malware.



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

### CIBERCONSEJOS PARA EVITAR CAER EN CONCURSOS FALSOS

#### CARACTERÍSTICAS DE LOS CONCURSOS FALSOS

- Promociones demasiado buenas.
- Solicita realizar un pago.
- Tiene remitente desconocido y no proviene de la empresa aludida.
- Los comentarios pueden provenir de bots o son imágenes.



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

### CIBERCONSEJOS PARA EVITAR CAER EN CONCURSOS FALSOS

#### RECOMENDACIONES

- 1 **SOSPECHA** de los enlaces y archivos en mensajes o e-mails.
- 2 **DESCONFÍA** de ofertas, promociones o premios increíbles.
- 3 **CONFIRMA** que el sitio web al que eres redirigido corresponda a la empresa.
- 4 **NUNCA** ingreses los datos de tus tarjetas bancarias.



## 8. 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>

## 9. 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.

- David Soto
- Sebastián Muñoz
- Gonzalo Andrés Araya Navarrete
- Rodrigo Javier Machado Villegas
- Rodrigo Patricio Velásquez Córdoba
- Héctor Andrés Verdejo Morales
- Edison Rodríguez

### 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>