



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 18

SEMANA DEL 30 DE DICIEMBRE DE 2022

AL 5 DE ENERO DE 2023

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

66

Las mitigaciones son útiles en productos de Fortinet, IBM, Google (Android) y Zoho.



IP INFORMADAS

13

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

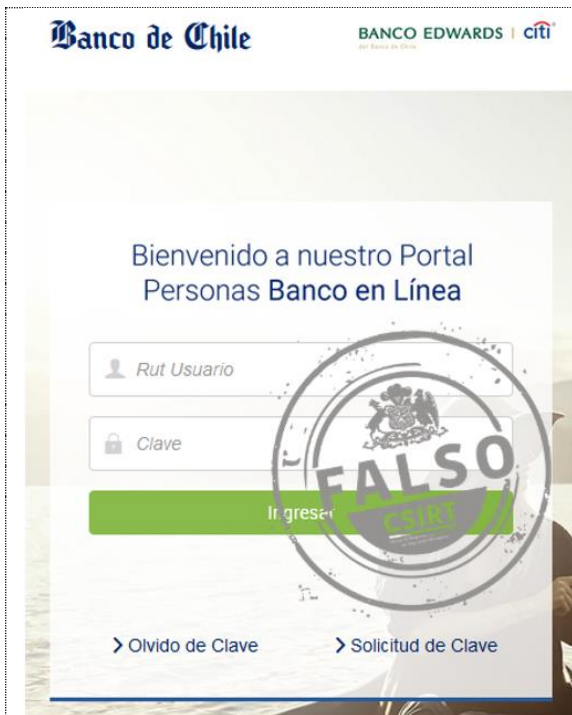
| | |
|--|----|
| 1. Sitios fraudulentos | 3 |
| 2. Phishing..... | 6 |
| 3. Vulnerabilidades | 9 |
| 4. Concientización | 11 |
| 5. Recomendaciones y buenas prácticas..... | 12 |
| 6. Muro de la Fama | 13 |



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

1. Sitios fraudulentos



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

| | |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR22-01184-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 30 de diciembre de 2022 |
| Última revisión | 30 de diciembre de 2022 |

Indicadores de compromiso

URL sitio falso

[https\[:\]//portal-bancochile.cl.townrealstate\[.\]com/1672425960/bchile-web/persona/login/index.html/login](https[:]//portal-bancochile.cl.townrealstate[.]com/1672425960/bchile-web/persona/login/index.html/login)

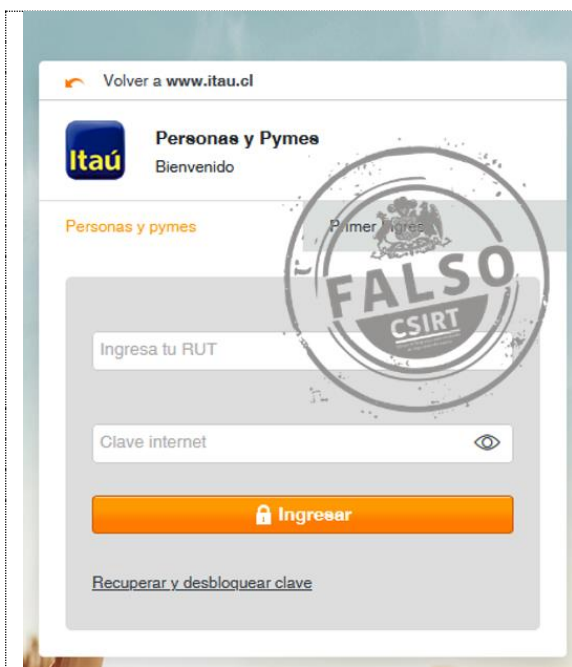
Dirección IP

[185.146.22.242]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01184-01/>

<https://www.csirt.gob.cl/media/2023/01/8FFR22-01184-01.pdf>



CSIRT alerta de nueva página fraudulenta que suplanta al Banco Itaú

| | |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR22-01185-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 30 de diciembre de 2022 |
| Última revisión | 30 de diciembre de 2022 |

Indicadores de compromiso

URL sitio falso

[https\[:\]//www.bnnco.ita.cl.scgfounders\[.\]com/1672426652/bancochile-web/persona/login/index.html/login](https[:]//www.bnnco.ita.cl.scgfounders[.]com/1672426652/bancochile-web/persona/login/index.html/login)

Dirección IP

[162.241.169.18]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr22-01185-01/>

<https://www.csirt.gob.cl/media/2023/01/8FFR22-01185-01.pdf>


CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

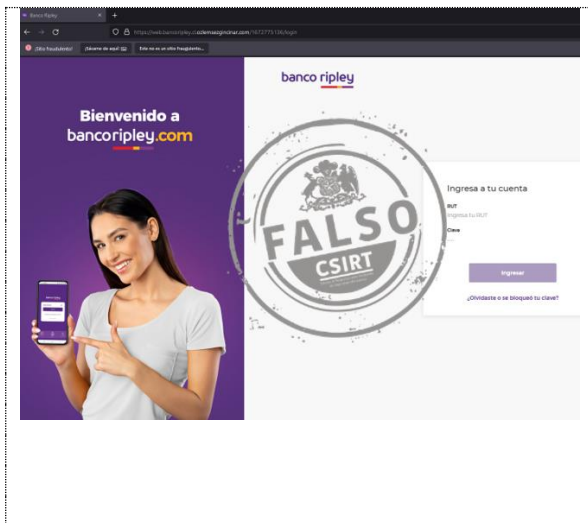
<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

Boletín de Seguridad Cibernética N° 183

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

BOLETÍN 13BCS23-00192-01 | SEMANA DEL 30 DE DICIEMBRE DE 2022 AL 5 DE ENERO DE 2023

| | | | | | | | | | | | | | | | |
|--|---|---------------------------------|-----------------|-----------------|--------|-------------------|--|-----------------|------|-----|--------|-------------------------------|--------------------|-----------------|--------------------|
|  | <p>CSIRT alerta de una página fraudulenta que suplanta al Banco Santander</p> <table border="1"><tr><td>Alerta de seguridad cibernética</td><td>8FFR22-01186-01</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>3 de enero de 2023</td></tr><tr><td>Última revisión</td><td>3 de enero de 2023</td></tr></table> <p>Indicadores de compromiso</p> <p>URL sitio falso https[:]//santanderchile-personas.dmklaws.co[.]ke/1672770309/portada/personas/home.asp</p> <p>Dirección IP [109.106.250.12]</p> <p>Enlaces para revisar el informe: https://www.csirt.gob.cl/alertas/8ffr22-01186-01/ https://www.csirt.gob.cl/media/2023/01/8FFR22-01186-01.pdf</p> | Alerta de seguridad cibernética | 8FFR22-01186-01 | Clase de alerta | Fraude | Tipo de incidente | Falsificación de Registros o Identidad | Nivel de riesgo | Alto | TLP | Blanco | Fecha de lanzamiento original | 3 de enero de 2023 | Última revisión | 3 de enero de 2023 |
| Alerta de seguridad cibernética | 8FFR22-01186-01 | | | | | | | | | | | | | | |
| Clase de alerta | Fraude | | | | | | | | | | | | | | |
| Tipo de incidente | Falsificación de Registros o Identidad | | | | | | | | | | | | | | |
| Nivel de riesgo | Alto | | | | | | | | | | | | | | |
| TLP | Blanco | | | | | | | | | | | | | | |
| Fecha de lanzamiento original | 3 de enero de 2023 | | | | | | | | | | | | | | |
| Última revisión | 3 de enero de 2023 | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | |
|---|--|---------------------------------|-----------------|-----------------|--------|-------------------|--|-----------------|------|-----|--------|-------------------------------|--------------------|-----------------|--------------------|
|  | <p>CSIRT alerta de la activación de una página fraudulenta que suplanta al Banco Ripley</p> <table border="1"><tr><td>Alerta de seguridad cibernética</td><td>8FFR22-01187-01</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>3 de enero de 2023</td></tr><tr><td>Última revisión</td><td>3 de enero de 2023</td></tr></table> <p>Indicadores de compromiso</p> <p>URL sitio falso https[:]//web.bancoripley.cl.ozlemsezgincinar[.]com/1672775136/login</p> <p>Dirección IP [185.179.27.31]</p> <p>Enlaces para revisar el informe: https://www.csirt.gob.cl/alertas/8ffr22-01187-01/ https://www.csirt.gob.cl/media/2023/01/8FFR22-01187-01.pdf</p> | Alerta de seguridad cibernética | 8FFR22-01187-01 | Clase de alerta | Fraude | Tipo de incidente | Falsificación de Registros o Identidad | Nivel de riesgo | Alto | TLP | Blanco | Fecha de lanzamiento original | 3 de enero de 2023 | Última revisión | 3 de enero de 2023 |
| Alerta de seguridad cibernética | 8FFR22-01187-01 | | | | | | | | | | | | | | |
| Clase de alerta | Fraude | | | | | | | | | | | | | | |
| Tipo de incidente | Falsificación de Registros o Identidad | | | | | | | | | | | | | | |
| Nivel de riesgo | Alto | | | | | | | | | | | | | | |
| TLP | Blanco | | | | | | | | | | | | | | |
| Fecha de lanzamiento original | 3 de enero de 2023 | | | | | | | | | | | | | | |
| Última revisión | 3 de enero de 2023 | | | | | | | | | | | | | | |

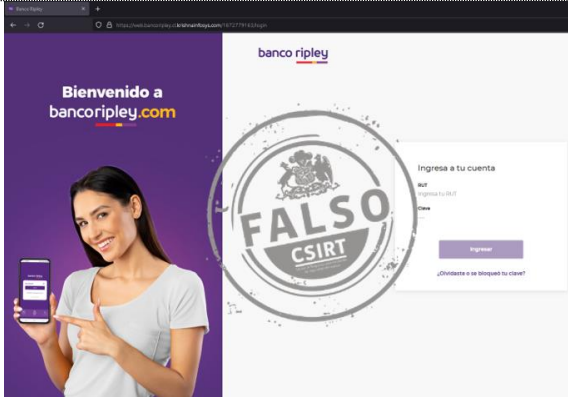
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO


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

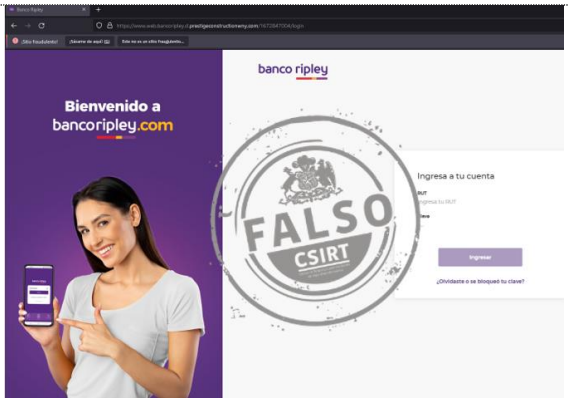
Boletín de Seguridad Cibernética N° 183

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

BOLETÍN 13BCS23-00192-01 | SEMANA DEL 30 DE DICIEMBRE DE 2022 AL 5 DE ENERO DE 2023

| | | |
|---|---|--|
|  | CSIRT alerta de una página fraudulenta que suplanta al Banco Ripley | |
| | Alerta de seguridad cibernética | 8FFR22-01188-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Falsificación de Registros o Identidad |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 4 de enero de 2023 |
| | Última revisión | 4 de enero de 2023 |
| | Indicadores de compromiso | |
| | URL sitio falso https[:]//web.bancoripley.cl.krishnainfosys[.]com/1672779163/login | |
| Dirección IP [78.142.63.93] | | |
| Enlaces para revisar el informe: https://www.csirt.gob.cl/alertas/8ffr22-01188-01/ https://www.csirt.gob.cl/media/2023/01/8FFR22-01188-01.pdf | | |

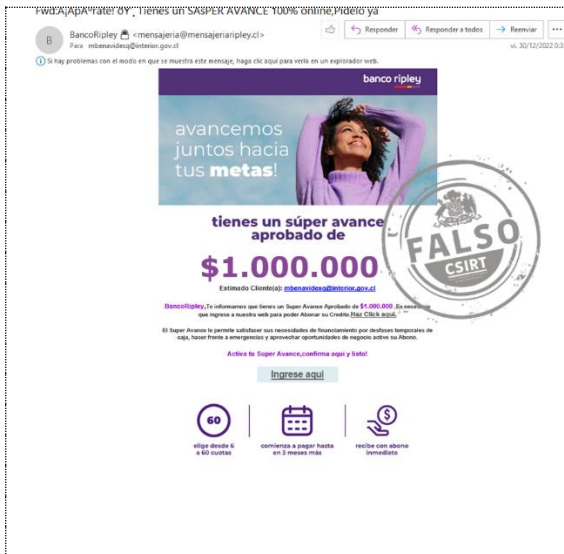
| | | |
|---|---|--|
|  | CSIRT alerta ante página fraudulenta que suplanta al Banco Santander | |
| | Alerta de seguridad cibernética | 8FFR22-01189-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Falsificación de Registros o Identidad |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 4 de enero de 2023 |
| | Última revisión | 4 de enero de 2023 |
| | Indicadores de compromiso | |
| | URL sitio falso https[:]//santanderchile-personas.dmklaws.co[.]ke/1672845677/portada/personas/home.asp | |
| Dirección IP [109.106.250.12] | | |
| Enlaces para revisar el informe: https://www.csirt.gob.cl/alertas/8ffr22-01189-01/ https://www.csirt.gob.cl/media/2023/01/8FFR22-01189-01.pdf | | |

| | | |
|---|---|--|
|  | CSIRT alerta de página fraudulenta que suplanta al Banco Ripley | |
| | Alerta de seguridad cibernética | 8FFR22-01190-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Falsificación de Registros o Identidad |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 4 de enero de 2023 |
| | Última revisión | 4 de enero de 2023 |
| | Indicadores de compromiso | |
| | URL sitio falso https[:]//www.web.bancoripley.cl.prestigeconstructionwny[.]com/1672847004/login | |
| Dirección IP [192.185.21.172] | | |
| Enlaces para revisar el informe: https://www.csirt.gob.cl/alertas/8ffr22-01190-01/ https://www.csirt.gob.cl/media/2023/01/8FFR22-01190-01.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



CSIRT alerta de campaña de phishing que suplanta al Banco Ripley

| | |
|---------------------------------|-------------------------|
| Alerta de seguridad cibernética | 8FPH22-00696-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 30 de diciembre de 2022 |
| Última revisión | 30 de diciembre de 2022 |

URL redirección

<https://bit.ly/3FWRqVY?l=www.bancoripley.cl>
<https://mpza.jsk/bancoripley/cuenta-qksa/>

URL sitio falso

[https://web.bancOripleycl.buckrealty\[.\]net/1672404123/login](https://web.bancOripleycl.buckrealty[.]net/1672404123/login)

IP

[64.91.247.208]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00696-01/>
<https://www.csirt.gob.cl/media/2022/12/8FPH22-00696-01.pdf>

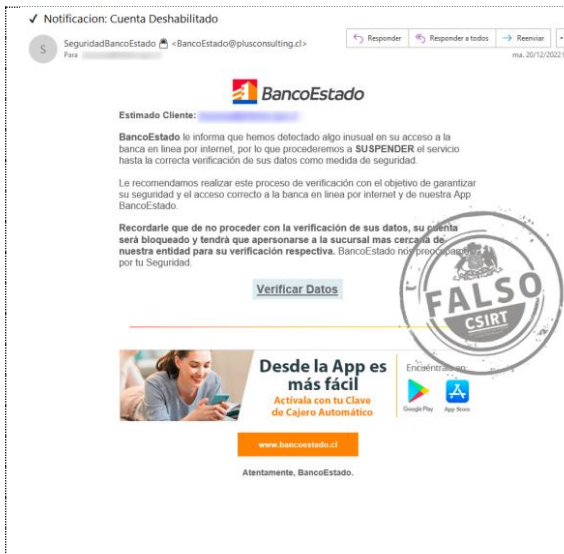


CSIRT alerta de nueva campaña de phishing con sextorsión

| | |
|---------------------------------|-------------------------|
| Alerta de seguridad cibernética | 8FPH22-00697-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 30 de diciembre de 2022 |
| Última revisión | 30 de diciembre de 2022 |

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00697-01/>
<https://www.csirt.gob.cl/media/2022/12/8FPH22-00697-01.pdf>



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

| | |
|---------------------------------|--------------------|
| Alerta de seguridad cibernética | 8FPH22-00698-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 3 de enero de 2023 |
| Última revisión | 3 de enero de 2023 |

Indicadores de compromiso

URL redirección

<https://bit.ly/3Z8OkOn?l=www.bancoripley.cl>

URL sitio falso

[https://web.bancoripley.cl.bluewayeducation\[.\]in/1672748142/login](https://web.bancoripley.cl.bluewayeducation[.]in/1672748142/login)

Dirección IP

[43.225.55.146]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph22-00698-01/>
<https://www.csirt.gob.cl/media/2023/01/8FPH22-00698-01.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>

Fwd:Tienes un SÁSPER AVANCE aprobado8Y, pÁdelo 100% online8Y2Á

BancoRipley <mensaje@mensaje@ripley.cl>

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.



avancemos juntos hacia tus metas!

tienes un súper avance aprobado de **\$1.000.000**

Estimado Cliente:

BancoRipley, te informamos que tienes un Súper Avance Aprobado de \$1.000.000. Es necesario que ingreses a nuestra web para poder Abonar en Crédito. [Click aquí](#).

El Súper Avance te permite satisfacer las necesidades de financiamiento por debetiera temporal de caja, hacer frente a emergencias y aprovechar oportunidades de negocio. Activa tu Súper Avance, confirma aquí y listo!


Ingrese aquí

60

| | |
|---|--------------------|
| CSIRT alerta de campaña de phishing que suplanta a Banco Ripley | |
| Alerta de seguridad cibernética | 8FPH22-00699-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 4 de enero de 2023 |
| Última revisión | 4 de enero de 2023 |
| Indicadores de compromiso | |
| URL redirección | |
| https://bit.ly/3Qazxyo?l=www.bancoripley.cl | |
| URL sitio falso | |
| https://web-bancoripley-cl.wonhaggicaravans.com/.au/1672836015/login | |
| Dirección IP | |
| [203.26.41.136] | |
| Enlaces para revisar el informe: | |
| https://www.csirt.gob.cl/alertas/8fph22-00699-01/ | |
| https://www.csirt.gob.cl/media/2023/01/8FPH22-00699-01.pdf | |

✓ Alerta De Seguridad: Cuenta Suspendido

SeguridadBancoEstado <BancoEstado@plusconsulting.cl>



Estimado Cliente:

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 comunicarse con la sucursal más cercana de nuestra entidad para su verificación respectiva. BancoEstado nos preocupamos por tu seguridad.

Verificar Datos

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

Encuétrala en Google Play App Store

www.bancoestado.cl

Atentamente, BancoEstado.


| | |
|---|--------------------|
| CSIRT alerta de campaña de phishing que suplanta al BancoEstado | |
| Alerta de seguridad cibernética | 8FPH23-00700-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 4 de enero de 2023 |
| Última revisión | 4 de enero de 2023 |
| Indicadores de compromiso | |
| URL redirección | |
| https://ucmstudio.info/activacion/cuenta-aotq/ | |
| URL sitio falso | |
| https://smscotito.info/1672861250/imagenes/_personas/home/default.asp | |
| Dirección IP | |
| [172.67.133.17] | |
| Enlaces para revisar el informe: | |
| https://www.csirt.gob.cl/alertas/8fph23-00700-01/ | |
| https://www.csirt.gob.cl/media/2023/01/8FPH23-00700-01.pdf | |

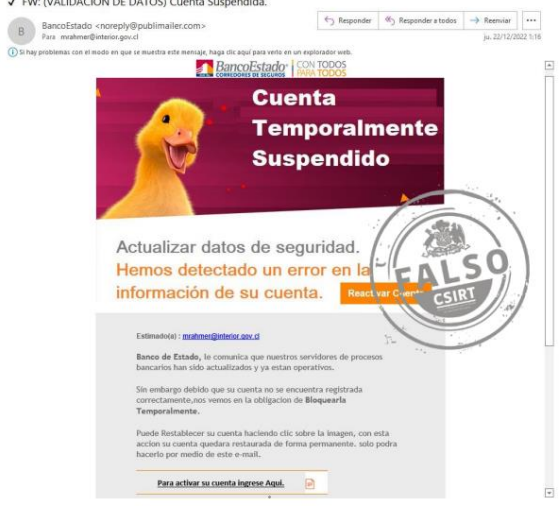
Boletín de Seguridad Cibernética N° 183

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

BOLETÍN 13BCS23-00192-01 | SEMANA DEL 30 DE DICIEMBRE DE 2022 AL 5 DE ENERO DE 2023

| | | | | | | | | | | | | | | | |
|--|--|---------------------------------|-----------------|-----------------|--------|-------------------|----------|-----------------|------|-----|--------|-------------------------------|--------------------|-----------------|--------------------|
|  <p>SeguridadBancoEstado <BancoEstado@plusconsulting.cl> Para: [Redacted]</p> <p>BancoEstado</p> <p>Estimado Cliente:</p> <p>BancoEstado le informa que hemos detectado algo inusual en su acceso a la banca en línea por internet, por lo que procederemos a SUSPENDER servicio hasta la correcta verificación de sus datos como medida de seguridad.</p> <p>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 de nuestra App BancoEstado.</p> <p>Recordarle que de no proceder con la verificación de sus datos, su cuenta será bloqueada y tendrá que acudir a la sucursal más cercana a nuestra entidad para su verificación respectiva. BancoEstado nos preocupamos por tu Seguridad.</p> <p>Verificar Datos</p> <p>Desde la App es más fácil Actívala con tu Clave de Cajero Automático</p> <p>Encuéntrala en Google Play, App Store</p> <p>www.bancoestado.cl</p> <p>Atentamente, BancoEstado.</p> | <p>CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado</p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00701-01</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>4 de enero de 2023</td></tr> <tr><td>Última revisión</td><td>4 de enero de 2023</td></tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección https://xtrailconver[.]com/activacion/cuenta-hkgr/</p> <p>URL sitio falso https://nmhpatito[.]info/1672863063/imagenes/_personas/home/default.asp</p> <p>Dirección IP [162.241.60.24]</p> <p>Enlaces para revisar el informe: https://www.csirt.gob.cl/alertas/8fph23-00701-01/ https://www.csirt.gob.cl/media/2023/01/8FPH23-00701-01.pdf</p> | Alerta de seguridad cibernética | 8FPH23-00701-01 | Clase de alerta | Fraude | Tipo de incidente | Phishing | Nivel de riesgo | Alto | TLP | Blanco | Fecha de lanzamiento original | 4 de enero de 2023 | Última revisión | 4 de enero de 2023 |
| Alerta de seguridad cibernética | 8FPH23-00701-01 | | | | | | | | | | | | | | |
| Clase de alerta | Fraude | | | | | | | | | | | | | | |
| Tipo de incidente | Phishing | | | | | | | | | | | | | | |
| Nivel de riesgo | Alto | | | | | | | | | | | | | | |
| TLP | Blanco | | | | | | | | | | | | | | |
| Fecha de lanzamiento original | 4 de enero de 2023 | | | | | | | | | | | | | | |
| Última revisión | 4 de enero de 2023 | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | |
|---|---|---------------------------------|-----------------|-----------------|--------|-------------------|----------|-----------------|------|-----|--------|-------------------------------|--------------------|-----------------|--------------------|
|  <p>FW: Informacion SII de factura electronica - Protocolo: 3REFUY2STK Para: [Redacted]</p> <p>SII Servicio de Impuestos Internos</p> <p>Estimado contribuyente.</p> <p>Atencion SII, Servicio de Impuestos internos.</p> <p>Advertencia! Encontramos problemas en la Emisión de sus boletas electrónicas, verifique la emisión de sus boletas electrónicas.</p> <p>Información general para Empresas y personas datos informativos operación renta año tributario 2023, para evitar cualquier problema con su Declaración de renta verifique Factura Electrónica.</p> <p>Se adjunta su boletín electrónico con error de información</p> <p>[Descargar adjunto]</p> <p>© 2023 SII Servicio Impuestos Internos. Todos los derechos reservados.</p> | <p>CSIRT alerta de nueva campaña de phishing con malware, que suplanta al SII</p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00702-01</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>5 de enero de 2023</td></tr> <tr><td>Última revisión</td><td>5 de enero de 2023</td></tr> </table> <p>Enlaces para revisar el informe: https://www.csirt.gob.cl/alertas/8fph23-00702-01/ https://www.csirt.gob.cl/media/2023/01/8FPH23-00702-01.pdf</p> | Alerta de seguridad cibernética | 8FPH23-00702-01 | Clase de alerta | Fraude | Tipo de incidente | Phishing | Nivel de riesgo | Alto | TLP | Blanco | Fecha de lanzamiento original | 5 de enero de 2023 | Última revisión | 5 de enero de 2023 |
| Alerta de seguridad cibernética | 8FPH23-00702-01 | | | | | | | | | | | | | | |
| Clase de alerta | Fraude | | | | | | | | | | | | | | |
| Tipo de incidente | Phishing | | | | | | | | | | | | | | |
| Nivel de riesgo | Alto | | | | | | | | | | | | | | |
| TLP | Blanco | | | | | | | | | | | | | | |
| Fecha de lanzamiento original | 5 de enero de 2023 | | | | | | | | | | | | | | |
| Última revisión | 5 de enero de 2023 | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | |
|--|--|---------------------------------|-----------------|-----------------|--------|-------------------|----------|-----------------|------|-----|--------|-------------------------------|--------------------|-----------------|--------------------|
|  <p>FW: (VALIDACION DE DATOS) Cuenta Suspendida. Para: [Redacted]</p> <p>Si hay problemas con el estado en que se muestra esta notificación, haga clic aquí para ir a un navegador web.</p> <p>BancoEstado CON TODOS LOS SERVICIOS</p> <p>Cuenta Temporalmente Suspendida</p> <p>Actualizar datos de seguridad. Hemos detectado un error en la información de su cuenta. Reactivar Cuenta</p> <p>Estimado(a): mgilmo@interior.gov.cl</p> <p>Banco de Estado, la compañía que muestra servidores de procesos bancarios han sido actualizados y ya están operativos.</p> <p>Sin embargo debido que su cuenta no se encuentra registrada correctamente, nos vemos en la obligación de Bloquearla Temporalmente.</p> <p>Puede Reactivar 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.</p> <p>Para activar su cuenta haga clic aquí.</p> | <p>CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley</p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00703-01</td></tr> <tr><td>Clase de alerta</td><td>Fraude</td></tr> <tr><td>Tipo de incidente</td><td>Phishing</td></tr> <tr><td>Nivel de riesgo</td><td>Alto</td></tr> <tr><td>TLP</td><td>Blanco</td></tr> <tr><td>Fecha de lanzamiento original</td><td>6 de enero de 2023</td></tr> <tr><td>Última revisión</td><td>6 de enero de 2023</td></tr> </table> <p>Indicadores de compromiso</p> <p>URL sitio falso https://web-bancoripley-cl.wonhaggicaravans.com[.]au/1673009665/login</p> <p>URL sitio redirección https://bit[.]ly/3CruO5Z?l=www.bancoripley.cl</p> <p>Dirección IP [203.26.41.136]</p> <p>Enlaces para revisar el informe: https://www.csirt.gob.cl/alertas/8fph23-00703-01/ https://www.csirt.gob.cl/media/2023/01/8FPH23-00703-01.pdf</p> | Alerta de seguridad cibernética | 8FPH23-00703-01 | Clase de alerta | Fraude | Tipo de incidente | Phishing | Nivel de riesgo | Alto | TLP | Blanco | Fecha de lanzamiento original | 6 de enero de 2023 | Última revisión | 6 de enero de 2023 |
| Alerta de seguridad cibernética | 8FPH23-00703-01 | | | | | | | | | | | | | | |
| Clase de alerta | Fraude | | | | | | | | | | | | | | |
| Tipo de incidente | Phishing | | | | | | | | | | | | | | |
| Nivel de riesgo | Alto | | | | | | | | | | | | | | |
| TLP | Blanco | | | | | | | | | | | | | | |
| Fecha de lanzamiento original | 6 de enero de 2023 | | | | | | | | | | | | | | |
| Última revisión | 6 de enero de 2023 | | | | | | | | | | | | | | |

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



INFORME DE Vulnerabilidad

9VSA22-00760-01
CSIRT comparte información de vulnerabilidades en FortiADC y FortiTester

PARA REGISTRAR | 15 10
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte vulnerabilidades que afectan a FortiADC y FortiTester

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA22-00760-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Crítico |
| TLP | Blanco |
| Fecha de lanzamiento original | 4 de enero de 2023 |
| Última revisión | 4 de enero de 2023 |

CVE

CVE-2022-39947
CVE-2022-35845

Fabricantes

Fortinet

Productos afectados

| | |
|--------------------------------|-----------------------------------|
| FortiADC versión 7.0.0 a 7.0.2 | FortiTester versión 7.1.0 |
| FortiADC versión 6.2.0 a 6.2.3 | FortiTester versión 7.0 todas |
| FortiADC versión 6.1.0 a 6.1.6 | FortiTester versión 4.0.0 a 4.2.0 |
| FortiADC versión 6.0.0 a 6.0.4 | FortiTester versión 2.3.0 a 3.9.1 |
| FortiADC versión 5.4.0 a 5.4.5 | |

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00760-01/>
<https://www.csirt.gob.cl/media/2023/01/9VSA22-00760-01.pdf>



INFORME DE Vulnerabilidad

9VSA23-00761-01
CSIRT comparte información de vulnerabilidades parchadas por Android en Enero 2023

PARA REGISTRAR | 15 10
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información sobre vulnerabilidades en actualización de seguridad de Android para enero 2023

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA22-00761-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 4 de enero de 2023 |
| Última revisión | 4 de enero de 2023 |

CVE

| | | |
|----------------|----------------|----------------|
| CVE-2022-20456 | CVE-2022-42720 | CVE-2022-44437 |
| CVE-2022-20489 | CVE-2022-42721 | CVE-2022-44438 |
| CVE-2022-20490 | CVE-2022-2959 | CVE-2022-22088 |
| CVE-2022-20492 | CVE-2022-41674 | CVE-2022-33255 |
| CVE-2022-20493 | CVE-2023-20928 | CVE-2021-35097 |
| CVE-2023-20912 | CVE-2022-20235 | CVE-2021-35113 |
| CVE-2023-20916 | CVE-2022-32635 | CVE-2021-35134 |
| CVE-2023-20918 | CVE-2022-32636 | CVE-2022-23960 |
| CVE-2023-20919 | CVE-2022-32637 | CVE-2022-25725 |
| CVE-2023-20920 | CVE-2022-44425 | CVE-2022-25746 |
| CVE-2023-20921 | CVE-2022-44426 | CVE-2022-33252 |
| CVE-2022-20494 | CVE-2022-44427 | CVE-2022-33253 |
| CVE-2023-20908 | CVE-2022-44428 | CVE-2022-33266 |
| CVE-2023-20922 | CVE-2022-44429 | CVE-2022-33274 |
| CVE-2022-20461 | CVE-2022-44430 | CVE-2022-33276 |
| CVE-2023-20904 | CVE-2022-44431 | CVE-2022-33283 |
| CVE-2023-20905 | CVE-2022-44432 | CVE-2022-33284 |
| CVE-2023-20913 | CVE-2022-44434 | CVE-2022-33285 |

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

| | | |
|---|----------------|----------------|
| CVE-2023-20915 | CVE-2022-44435 | CVE-2022-33286 |
| CVE-2022-42719 | CVE-2022-44436 | |
| Fabricantes | | |
| Google | | |
| Productos afectados | | |
| Android, todas las versiones. | | |
| Enlaces para revisar el informe: | | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00761-01/ | | |
| https://www.csirt.gob.cl/media/2023/01/9VSA23-00761-01.pdf | | |



INFORME DE Vulnerabilidad

9VSA23-00762-01
CSIRT comparte información de vulnerabilidades parchadas para IBM Cloud Pak for Business Automation

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de vulnerabilidades parchadas para IBM Cloud Pak for Business Automation

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00762-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Medio |
| TLP | Blanco |
| Fecha de lanzamiento original | 5 de enero de 2023 |
| Última revisión | 5 de enero de 2023 |

CVE

| | |
|----------------|----------------|
| CVE-2017-10355 | CVE-2022-42435 |
| CVE-2022-42920 | CVE-2022-2047 |

Fabricantes

IBM

Productos afectados

IBM Cloud Pak for Business Automation anteriores a 21.0.3-IF016 y 22.0.1-IF006, las que corrigen las presentes vulnerabilidades.

Enlaces para revisar el informe:

| |
|---|
| https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00762-01/ |
| https://www.csirt.gob.cl/media/2023/01/9VSA23-00762-01.pdf |



INFORME DE Vulnerabilidad

9VSA23-00763-01
CSIRT comparte información de vulnerabilidades para varios productos de Zoho

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte vulnerabilidades informadas para distintos productos de Zoho

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00763-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Crítico |
| TLP | Blanco |
| Fecha de lanzamiento original | 4 de enero de 2023 |
| Última revisión | 4 de enero de 2023 |

CVE

CVE-2022-47523

Fabricantes

Fortinet

Productos afectados

Access Manager Plus 12200 y anteriores.
PAM360 5800 y anteriores,
Password Manager Pro 4308 y anteriores.

Enlaces para revisar el informe:

| |
|---|
| https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00763-01/ |
| https://www.csirt.gob.cl/media/2023/01/9VSA23-00763-01.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>

4. Concientización

Ciberconsejos: ¿Cómo protegerse de los fraudes de verano?

Cada vez son más las personas que arriendan alguna propiedad para sus vacaciones de verano a través de un sitio web. Sin embargo, así como incrementa esta tendencia también aparecen los avisos falsos que buscan obtener un beneficio económico.

Para evitar caer en este tipo de estafas, el CSIRT de Gobierno entregó esta semana las siguientes recomendaciones, disponibles también en nuestro sitio web oficial: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-estafas-verano/>



CIBERCONSEJOS
¿Cómo protegerse de los fraudes de verano?

Algunos fraudes de verano:

- Anuncios falsos en el que se utilizan fotografías robadas de otros avisos con una descripción y un precio muy atractivo.
- También existen avisos falsos en sitios especializados como Tripadvisor y Airbnb.
- Campañas de phishing con enlaces a webs falsas para robar datos bancarios, información personal u otros datos sensibles.



CIBERCONSEJOS
¿Cómo protegerse de los fraudes de verano?

Recomendaciones:

1. Desconfía de anuncios muy atractivos y demasiado económicos.
2. Sospecha si el anuncio está mal redactado o tiene faltas de ortografía.



CIBERCONSEJOS
¿Cómo protegerse de los fraudes de verano?

Recomendaciones:

3. Intenta comprobar la identidad del anunciante, la titularidad y existencia del inmueble, mediante herramientas como Google Street View.
4. Sospecha si piden un adelanto o proponen formas alternativas de pago.



CIBERCONSEJOS
¿Cómo protegerse de los fraudes de verano?





Si fuiste víctima de una estafa:

- 1 Denuncia la falsa oferta a los responsables de la plataforma.
- 2 Recopila todas las pruebas que puedas de la estafa e información sobre el anunciante.
- 3 Denuncia con las autoridades pertinentes, como la Policía de Investigaciones (PDI), llamando al +562 2708 0658.

5. Recomendaciones y buenas prácticas

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








CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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





6. Muro de la Fama

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

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

-  Cristián Figueroa Valenzuela
-  Rodrigo Machado Villegas
-  Gerardo Andrés Hernández Rodríguez
-  David Soto
-  Christopher Provoste Álvarez
-  Juan Pablo Andrés Garrido Lara
-  Rodrigo Andrés Cáceres Valdés.

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>