



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 227

semana del 3 al 9 de noviembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

10

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

20

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

7

Las mitigaciones son útiles en productos de Veeam, QNAP y Apache.



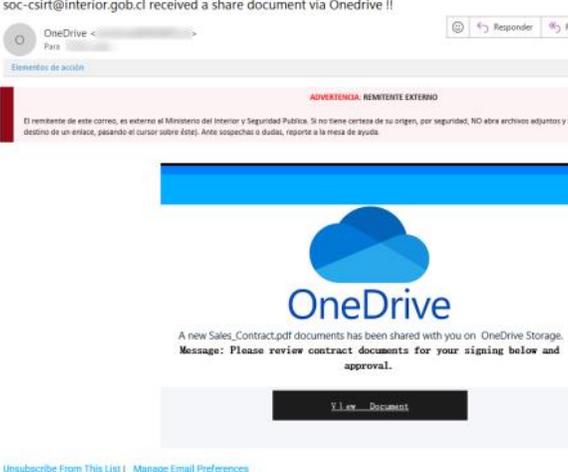
CONTENIDO

| | |
|-------------------------------------|----|
| 1. Phishing | 3 |
| 2. Sitios fraudulentos | 5 |
| 3. Malware..... | 8 |
| 4. Vulnerabilidades | 10 |
| 5. Noticias y concientización | 12 |
| 7. Muro de la Fama | 15 |

11111<

1. Phishing

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---------------------------------|-----------------|-----------------|--------|-------------------|----------|-----------------|------|-----|--------|-------------------------------|-------------------|-----------------|-------------------|----------------------------------|--|----------------------------|---|---------------------------|---|---------------------------------|-----------------|---------------------------------|---|
|  | <p>CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00904-01</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>7 noviembre, 2023</td> </tr> <tr> <td>Última revisión</td> <td>7 noviembre, 2023</td> </tr> <tr> <td colspan="2">Indicadores de compromiso</td> </tr> <tr> <td>URL del sitio falso</td> <td>https://supportestmstado[.]com/activacion/cuenta-odfp/</td> </tr> <tr> <td>URL de redirección</td> <td>https://serviestadohome.info/1699362047/imagenes/_personas/home/default.asp</td> </tr> <tr> <td>Dirección IP sitio falso</td> <td>[198.27.78.113]</td> </tr> <tr> <td>Enlace para revisar loC:</td> <td>https://www.csirt.gob.cl/alertas/8fph23-00904-01/</td> </tr> </table> | Alerta de seguridad cibernética | 8FPH23-00904-01 | Clase de alerta | Fraude | Tipo de incidente | Phishing | Nivel de riesgo | Alto | TLP | Blanco | Fecha de lanzamiento original | 7 noviembre, 2023 | Última revisión | 7 noviembre, 2023 | Indicadores de compromiso | | URL del sitio falso | https://supportestmstado[.]com/activacion/cuenta-odfp/ | URL de redirección | https://serviestadohome.info/1699362047/imagenes/_personas/home/default.asp | Dirección IP sitio falso | [198.27.78.113] | Enlace para revisar loC: | https://www.csirt.gob.cl/alertas/8fph23-00904-01/ |
| Alerta de seguridad cibernética | 8FPH23-00904-01 | | | | | | | | | | | | | | | | | | | | | | | | |
| Clase de alerta | Fraude | | | | | | | | | | | | | | | | | | | | | | | | |
| Tipo de incidente | Phishing | | | | | | | | | | | | | | | | | | | | | | | | |
| Nivel de riesgo | Alto | | | | | | | | | | | | | | | | | | | | | | | | |
| TLP | Blanco | | | | | | | | | | | | | | | | | | | | | | | | |
| Fecha de lanzamiento original | 7 noviembre, 2023 | | | | | | | | | | | | | | | | | | | | | | | | |
| Última revisión | 7 noviembre, 2023 | | | | | | | | | | | | | | | | | | | | | | | | |
| Indicadores de compromiso | | | | | | | | | | | | | | | | | | | | | | | | | |
| URL del sitio falso | https://supportestmstado[.]com/activacion/cuenta-odfp/ | | | | | | | | | | | | | | | | | | | | | | | | |
| URL de redirección | https://serviestadohome.info/1699362047/imagenes/_personas/home/default.asp | | | | | | | | | | | | | | | | | | | | | | | | |
| Dirección IP sitio falso | [198.27.78.113] | | | | | | | | | | | | | | | | | | | | | | | | |
| Enlace para revisar loC: | https://www.csirt.gob.cl/alertas/8fph23-00904-01/ | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | |
|--|---|---------------------------------|-----------------|-----------------|--------|-------------------|----------|-----------------|------|-----|--------|-------------------------------|-------------------|-----------------|-------------------|----------------------------------|--|----------------------------|---|---------------------------------|---------------|---------------------------------|---|
|  | <p>CSIRT alerta de nueva campaña de phishing que suplanta a Microsoft OneDrive</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00905-01</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>9 noviembre, 2023</td> </tr> <tr> <td>Última revisión</td> <td>9 noviembre, 2023</td> </tr> <tr> <td colspan="2">Indicadores de compromiso</td> </tr> <tr> <td>URL del sitio falso</td> <td>https://pub-f9c256ae09374af7aea1e69a3ba45cc8.r2[.]dev/onedrive-51985623vbndpl0000000plavbnt.html#</td> </tr> <tr> <td>Dirección IP sitio falso</td> <td>[104.18.3.35]</td> </tr> <tr> <td>Enlace para revisar loC:</td> <td>https://www.csirt.gob.cl/alertas/8fph23-00905-01/</td> </tr> </table> | Alerta de seguridad cibernética | 8FPH23-00905-01 | Clase de alerta | Fraude | Tipo de incidente | Phishing | Nivel de riesgo | Alto | TLP | Blanco | Fecha de lanzamiento original | 9 noviembre, 2023 | Última revisión | 9 noviembre, 2023 | Indicadores de compromiso | | URL del sitio falso | https://pub-f9c256ae09374af7aea1e69a3ba45cc8.r2[.]dev/onedrive-51985623vbndpl0000000plavbnt.html# | Dirección IP sitio falso | [104.18.3.35] | Enlace para revisar loC: | https://www.csirt.gob.cl/alertas/8fph23-00905-01/ |
| Alerta de seguridad cibernética | 8FPH23-00905-01 | | | | | | | | | | | | | | | | | | | | | | |
| Clase de alerta | Fraude | | | | | | | | | | | | | | | | | | | | | | |
| Tipo de incidente | Phishing | | | | | | | | | | | | | | | | | | | | | | |
| Nivel de riesgo | Alto | | | | | | | | | | | | | | | | | | | | | | |
| TLP | Blanco | | | | | | | | | | | | | | | | | | | | | | |
| Fecha de lanzamiento original | 9 noviembre, 2023 | | | | | | | | | | | | | | | | | | | | | | |
| Última revisión | 9 noviembre, 2023 | | | | | | | | | | | | | | | | | | | | | | |
| Indicadores de compromiso | | | | | | | | | | | | | | | | | | | | | | | |
| URL del sitio falso | https://pub-f9c256ae09374af7aea1e69a3ba45cc8.r2[.]dev/onedrive-51985623vbndpl0000000plavbnt.html# | | | | | | | | | | | | | | | | | | | | | | |
| Dirección IP sitio falso | [104.18.3.35] | | | | | | | | | | | | | | | | | | | | | | |
| Enlace para revisar loC: | https://www.csirt.gob.cl/alertas/8fph23-00905-01/ | | | | | | | | | | | | | | | | | | | | | | |

CONTACTO Y REDES SOCIALES CSIRT

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

Boletín de Seguridad Cibernética N° 227

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

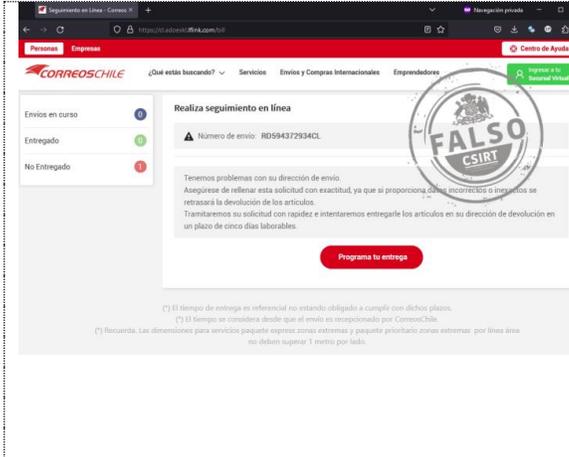
BOLETÍN 13BCS23-00236-01 | Semana del 3 al 9 de noviembre de 2023

| | | |
|--|---|---|
|  | CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado | |
| | Alerta de seguridad cibernética | 8FPH23-00906-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Phishing |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 9 noviembre, 2023 |
| | Última revisión | 9 noviembre, 2023 |
| | Indicadores de compromiso | |
| | URL del sitio falso | https://vcrawford2[.]com/1699535995/imagenes/_personas/home/default.asp |
| | URL de redirección | https://enelvalpa[.]com/activacion/cuenta-wpgk/ |
| | Dirección IP sitio falso | [64.37.50.234] |
| | Enlace para revisar loC: | https://www.csirt.gob.cl/alertas/8fph23-00906-01/ |

CONTACTO Y REDES SOCIALES CSIRT

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

2. Sitios fraudulentos



CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile

| | |
|---------------------------------|-------------------|
| Alerta de seguridad cibernética | 8FFR23-01541-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 7 noviembre, 2023 |
| Última revisión | 7 noviembre, 2023 |

Indicadores de compromiso

URL del sitio falso

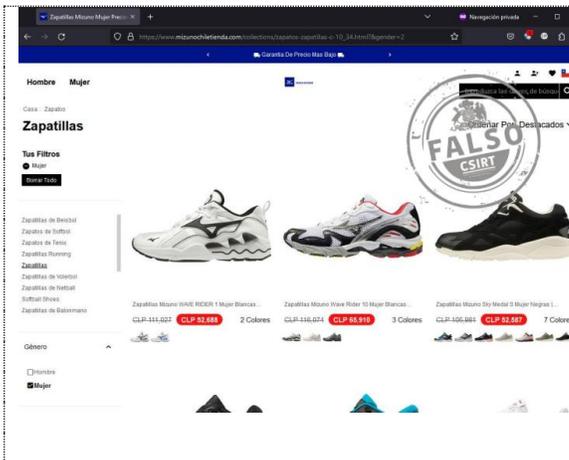
[https://cl.adoexkl.lfink\[.\]com/bill](https://cl.adoexkl.lfink[.]com/bill)

Dirección IP sitio falso

[43.153.106.5]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8ffr23-01541-01/>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Mizuno

| | |
|---------------------------------|-------------------|
| Alerta de seguridad cibernética | 8FFR23-01542-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 8 noviembre, 2023 |
| Última revisión | 8 noviembre, 2023 |

Indicadores de compromiso

URL del sitio falso

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

Dirección IP sitio falso

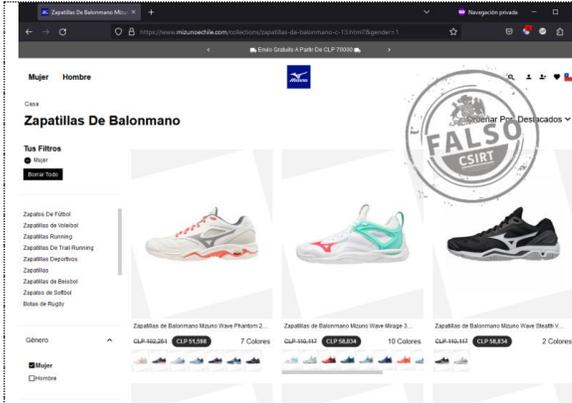
[196.242.179.137]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8ffr23-01542-01/>

CONTACTO Y REDES SOCIALES CSIRT

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



CSIRT alerta de una nueva página fraudulenta que suplanta a Mizuno

| | |
|---------------------------------|-------------------|
| Alerta de seguridad cibernética | 8FFR23-01543-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 8 noviembre, 2023 |
| Última revisión | 8 noviembre, 2023 |

Indicadores de compromiso

URL del sitio falso

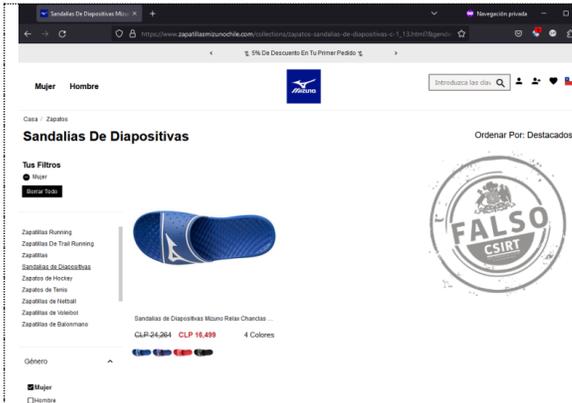
[https://www.mizunochile\[.\]com/](https://www.mizunochile[.]com/)

Dirección IP sitio falso

[165.231.10.33]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8ffr23-01543-01/>



CSIRT alerta de un nuevo sitio fraudulento más que suplanta a Mizuno

| | |
|---------------------------------|-------------------|
| Alerta de seguridad cibernética | 8FFR23-01544-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 8 noviembre, 2023 |
| Última revisión | 8 noviembre, 2023 |

Indicadores de compromiso

URL del sitio falso

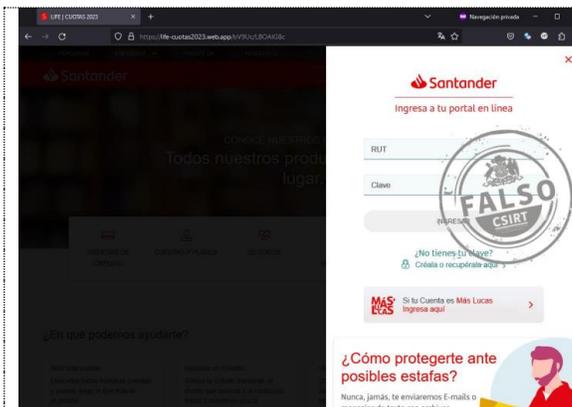
[https://www.zapatillasmizunochile\[.\]com/](https://www.zapatillasmizunochile[.]com/)

Dirección IP sitio falso

[196.196.223.140]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8ffr23-01544-01/>



CSIRT alerta de la activación de un nuevo sitio fraudulento que suplanta a Banco Santander

| | |
|---------------------------------|-------------------|
| Alerta de seguridad cibernética | 8FFR23-01545-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 8 noviembre, 2023 |
| Última revisión | 8 noviembre, 2023 |

Indicadores de compromiso

URL del sitio falso

[https://lfe-cuotas2023\[.\]web.app/bv9Uc/LBOAIG8c](https://lfe-cuotas2023[.]web.app/bv9Uc/LBOAIG8c)

Dirección IP sitio falso

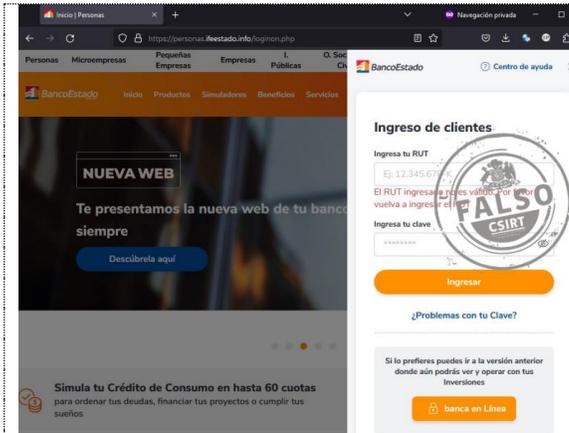
[199.36.158.100]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8ffr23-01545-01/>

CONTACTO Y REDES SOCIALES CSIRT

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



CSIRT alerta de nueva página fraudulenta que suplanta a BancoEstado

| | |
|---------------------------------|-------------------|
| Alerta de seguridad cibernética | 8FFR23-01546-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 9 noviembre, 2023 |
| Última revisión | 9 noviembre, 2023 |

Indicadores de compromiso

URL del sitio falso

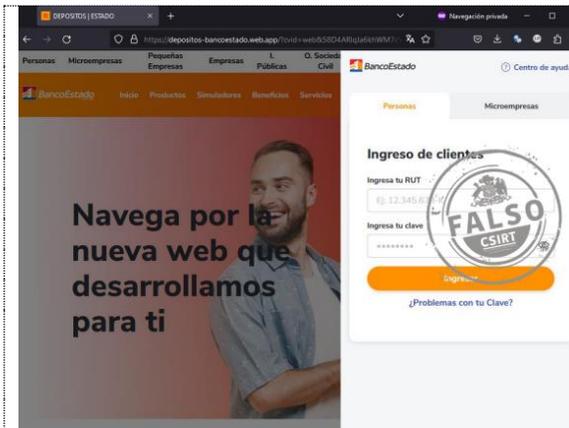
[https://personas.ifeestado\[.\]info/loginon.php](https://personas.ifeestado[.]info/loginon.php)

Dirección IP sitio falso

[172.67.179.69]

Enlace para revisar IoC:

<https://www.csirt.gob.cl/alertas/8ffr23-01546-01/>



CSIRT alerta de un nuevo sitio fraudulento que suplanta a BancoEstado

| | |
|---------------------------------|-------------------|
| Alerta de seguridad cibernética | 8FFR23-01547-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 9 noviembre, 2023 |
| Última revisión | 9 noviembre, 2023 |

Indicadores de compromiso

URL del sitio falso

[https://depositos-bancoestado\[.\]web.app/?cvid=web&58D4ARlqJa6khWM7cV1jIdwylGzLufNEoHepSb9QmKCYvTPZ200xtnU3FSrgXB](https://depositos-bancoestado[.]web.app/?cvid=web&58D4ARlqJa6khWM7cV1jIdwylGzLufNEoHepSb9QmKCYvTPZ200xtnU3FSrgXB)

Dirección IP sitio falso

[199.36.158.100]

Enlace para revisar IoC:

<https://www.csirt.gob.cl/alertas/8ffr23-01547-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

3. Malware

| | | | | | | | | | | | | | | | |
|---|--|---------------------------------|-----------------|-----------------|--------|-------------------|---------|-----------------|------|-----|--------|-------------------------------|-------------------|-----------------|-------------------|
| <p>FACTURA DE PROFORMA</p> <p>Jorge <...> Para</p> <p>Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.</p> <p>Factura de proforma_xks.7z 45 KB</p> <p>Estimado señor,</p> <p>Buenos días</p> <p>Perdón por el retraso, adjunto lo siguiente para su referencia.</p> <ul style="list-style-type: none"> Certificado de origen Factura de proforma Lista de embalaje <p>Documentos autorizados por usted. Gracias de antemano por su amable cooperación.</p> <p>¡Gracias y Saludos cordiales!</p> | <p>CSIRT alerta de nueva campaña de phishing con malware Agent Tesla</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>2CMV23-00431-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Malware</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>3 noviembre, 2023</td> </tr> <tr> <td>Última revisión</td> <td>3 noviembre, 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL-Dominio</p> <p>https://telemas[.]com.co/cdi/Djphbrnppqe.pdf https://api.telegram[.]org/bot6548288330:AAGA-b1ojgiCCinc5YQor8R1kxgez4hPFpM/sendDocument</p> <p>SHA256</p> <p>510771c843a856eb15d763d0931002f6f297aed35b0ed9aac509d3bd6e7b964a b0b873b46d9e024e7d59de49d506637f2bb31632465ccf88424ca1ab3c457b38</p> <p>Enlaces para revisar el informe:</p> <p>https://www.csirt.gob.cl/alertas/2cmv23-00431-01/</p> | Alerta de seguridad cibernética | 2CMV23-00431-01 | Clase de alerta | Fraude | Tipo de incidente | Malware | Nivel de riesgo | Alto | TLP | Blanco | Fecha de lanzamiento original | 3 noviembre, 2023 | Última revisión | 3 noviembre, 2023 |
| Alerta de seguridad cibernética | 2CMV23-00431-01 | | | | | | | | | | | | | | |
| Clase de alerta | Fraude | | | | | | | | | | | | | | |
| Tipo de incidente | Malware | | | | | | | | | | | | | | |
| Nivel de riesgo | Alto | | | | | | | | | | | | | | |
| TLP | Blanco | | | | | | | | | | | | | | |
| Fecha de lanzamiento original | 3 noviembre, 2023 | | | | | | | | | | | | | | |
| Última revisión | 3 noviembre, 2023 | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | |
|---|--|---------------------------------|-----------------|-----------------|--------|-------------------|---------|-----------------|------|-----|--------|-------------------------------|-------------------|-----------------|-------------------|
| <p>Re: Solicitud de Aprobación Nota de Crédito</p> <p>Nota de credito.zip 370 KB</p> <p>PREC230-11188.zip 370 KB</p> <p>Buen día,</p> <p>Junto con saludarles, adjunto solicitud para realizar una nota de crédito, esto es para el cliente de Danisco el cual hizo devolución del producto. Esta factura corresponde al mes de septiembre la cual no será refacturada ya que el cliente se le entregó otra alternativa más costosa, que se encuentra pendiente de ser aceptada (adjunto cotización).</p> <p>El documento se encuentra en el plazo para ser anulado hasta noviembre en donde se cumple el plazo de los tres meses, para generar la nota sin perder impuesto.</p> <p>Quedo atento a sus comentarios,</p> <p>Saludos Cordiales,</p>  | <p>CSIRT alerta de nueva campaña de phishing con malware Agent Tesla</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>2CMV23-00432-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Malware</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>6 noviembre, 2023</td> </tr> <tr> <td>Última revisión</td> <td>6 noviembre, 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL-Dominio</p> <p>https://discord[.]com/api/webhooks/1169917901906653224/YjkyFWX_CawSIPQ02zeV3XExHGtDteoh-fLuvdqfL772Pb_cJUtnVv4DqDRhm0ks1</p> <p>SHA256</p> <p>6a457eb922af750f662dbbcc59386c742538066c222a298c04175d4a5e802fd 4d7b65d0e759355d6b6295db58ad985efdd04f01e80e1c34bfc8c39787735a44 b0941553bf71a3d7dbc296f544d5b00832e6207cfdaaa6cdec2bf6a8a3dc39a8 4d7b65d0e759355d6b6295db58ad985efdd04f01e80e1c34bfc8c39787735a44</p> <p>Enlaces para revisar el informe:</p> <p>https://www.csirt.gob.cl/alertas/2cmv23-00432-01/</p> | Alerta de seguridad cibernética | 2CMV23-00432-01 | Clase de alerta | Fraude | Tipo de incidente | Malware | Nivel de riesgo | Alto | TLP | Blanco | Fecha de lanzamiento original | 6 noviembre, 2023 | Última revisión | 6 noviembre, 2023 |
| Alerta de seguridad cibernética | 2CMV23-00432-01 | | | | | | | | | | | | | | |
| Clase de alerta | Fraude | | | | | | | | | | | | | | |
| Tipo de incidente | Malware | | | | | | | | | | | | | | |
| Nivel de riesgo | Alto | | | | | | | | | | | | | | |
| TLP | Blanco | | | | | | | | | | | | | | |
| Fecha de lanzamiento original | 6 noviembre, 2023 | | | | | | | | | | | | | | |
| Última revisión | 6 noviembre, 2023 | | | | | | | | | | | | | | |

Boletín de Seguridad Cibernética N° 227

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

BOLETÍN 13BCS23-00236-01 | Semana del 3 al 9 de noviembre de 2023

Solicitud de Cotización Urgente: 202310_30432UCH/CL

JL Jorge Loyola
Para [Redacted]
Mensaje enviado con importancia Alta
Solicitud de Cotización Urgente (202310_30432UCH-CL).pdf.rar
Archivo.rar

ADVERTENCIA: REMITENTE EXTERNO

El remitente de este correo, es externo al Ministerio del Interior y Seguridad Pública. Si no tiene certeza de su origen, por seguridad, NO abra archivos adjuntos y NO puede verificar el destino de un enlace, pasando el cursor sobre éste. Ante sospechas o dudas, reporte a la mesa de ayuda.

Hola,

¡Espero que esté bien!
Tenemos un requisito **MUY URGENTE** para los artículos adjuntos, así que verifique y déjeme saber su mejor oferta junto con el estado del de producción.

Por favor, se necesita su rápida respuesta.
Gracias.

Atentamente,



CSIRT alerta de una nueva campaña de phishing con malware, que suplanta a la Universidad de Chile

| | |
|---------------------------------|-------------------|
| Alerta de seguridad cibernética | 2CMV23-00433-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 7 noviembre, 2023 |
| Última revisión | 7 noviembre, 2023 |

Indicadores de compromiso

URL-Dominio
[https://drive.google\[.\]com/uc?export=download&id=1R4xBOHz985Aknw3ujsQ6NpAXJ3vbaqp7](https://drive.google[.]com/uc?export=download&id=1R4xBOHz985Aknw3ujsQ6NpAXJ3vbaqp7)
[https://doc-00-c4-docs.googleusercontent\[.\]com/docs/securesc/ha0r0937guc7l7deffksulhg5h7mbp1/thoc2tionc5fg4pm29mmucd39cal2chm/1699284900000/15460567426367328879/*1R4xBOHz985Aknw3ujsQ6NpAXJ3vbaqp7?e=download&uuiid=d16c2812-aea1-4b95-bd02-485c17e0d88a](https://doc-00-c4-docs.googleusercontent[.]com/docs/securesc/ha0r0937guc7l7deffksulhg5h7mbp1/thoc2tionc5fg4pm29mmucd39cal2chm/1699284900000/15460567426367328879/*1R4xBOHz985Aknw3ujsQ6NpAXJ3vbaqp7?e=download&uuiid=d16c2812-aea1-4b95-bd02-485c17e0d88a)
[https://drive.google\[.\]com/uc?export=download&id=1R2oKSmimiwjQppJp7FLYWk5PfZXuKfGc](https://drive.google[.]com/uc?export=download&id=1R2oKSmimiwjQppJp7FLYWk5PfZXuKfGc)
[http://146.190.157\[.\]174/NcBb73GzFMtT6SI](http://146.190.157[.]174/NcBb73GzFMtT6SI)

SHA256
8e52dd0278b75ba5b0411951d8397e5ce7813dff9ccffcb3e2d21eab71604a1c8f3bc71f3d8339af58bdfc7054bbb8436a1a52b41d86ac33c735f627bcbace3

Enlaces para revisar el informe:
<https://www.csirt.gob.cl/alertas/2cmv23-00433-01/>

Re: CV Forner, Eugenia // Postulación para puesto de trabajo

ME María Eugenia Forner <[Redacted]>
Para [Redacted]
mi. 08/11/2023 11:08

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

2023-11-CV Forner Eugenia.cvp
567 KB

Buenos días,

Soy Eugenia Forner, me dirijo a quien corresponda con el fin de transmitirle mi interés para ser tomada en cuenta para un puesto laboral en su empresa. Si bien cuento con amplia experiencia en diferentes sectores, principalmente en administración y finanzas en los últimos años desempeñándome como implementadora de sistemas de gestión contable, quisiera postularme en esta oportunidad para el área comercial. En el año 2020 en plena pandemia me desempeñé en la empresa Matuschka como responsable comercial del canal mayorista, desarrollando una cartera de más de 150 clientes y manejando la logística de envíos al interior.

En este momento me encuentro con amplia disponibilidad horaria y con ganas de continuar desarrollándome en el área comercial como vendedora o cajera, o puesto afín. No tengo problemas de comenzar cubriendo francos o como personal temporario.

Desde ya muchas gracias y quedo a la espera de una posible entrevista.

Saludos cordiales,



CSIRT alerta de nueva campaña de phishing con malware, contenido en falsa postulación laboral

| | |
|---------------------------------|-------------------|
| Alerta de seguridad cibernética | 2CMV23-00434-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 8 noviembre, 2023 |
| Última revisión | 8 noviembre, 2023 |

Indicadores de compromiso

URL-Dominio
[https://discord\[.\]com/api/webhooks/1171723200741257216/Gcyp_pKpHXDEZGtrdsBTGVDcc2OYUckNC6AxbqtT3aDfY8F2m1FbeqjnbOgcclHOZqy](https://discord[.]com/api/webhooks/1171723200741257216/Gcyp_pKpHXDEZGtrdsBTGVDcc2OYUckNC6AxbqtT3aDfY8F2m1FbeqjnbOgcclHOZqy)

SHA256
0e9ee8e1f09d84f6d77878591c6f15a818b38e636022becab44f5630d5cf6af5df3035bf5b05466757706b2b5ef5028b7ada1227ae0d1b73314c71a6026f1239

Enlaces para revisar el informe:
<https://www.csirt.gob.cl/alertas/2cmv23-00434-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

4. Vulnerabilidades



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00932-01
CSIRT comparte nueva vulnerabilidad crítica en Apache ActiveMQ

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



CSIRT informa de vulnerabilidad crítica en Apache ActiveMQ

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00932-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 6 noviembre, 2023 |
| Última revisión | 6 noviembre, 2023 |

CVE

CVE-2023-46604

Fabricante

Apache Software Foundation

Productos afectados

Apache Active MQ and Legacy OpenWire Module versiones:
5.18.x versiones anteriores a la 5.18.3
5.17.x versiones anteriores a la 5.17.6
5.16.x versiones anteriores a la 5.16.7
Todas las versiones anteriores a la 5.15.16

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00932-01/>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00933-01
CSIRT comparte información de nuevas vulnerabilidades críticas en QNAP QTS

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



CSIRT comparte información de vulnerabilidades críticas en QNAP QTS

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00933-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 7 noviembre, 2023 |
| Última revisión | 7 noviembre, 2023 |

CVE

CVE-2023-23368

CVE-2023-23369

Fabricante

QNAP

Productos afectados

QTS 5.0.x y 4.5.x, QuTS hero h5.0.x y h4.5.x, y QuTScloud
QTS 5.1.x, 4.3.6, 4.3.4, 4.3.3, y 4.2.x, Multimedia Console 2.1.x y 1.4.x, y Media Streaming add-on 500.1.x y 500.0.x

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00933-01/>

CONTACTO Y REDES SOCIALES CSIRT

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



CSIRT informa de vulnerabilidades, dos de ellas críticas, que afectan a Veeam ONE IT

| | |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00934-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 7 noviembre, 2023 |
| Última revisión | 7 noviembre, 2023 |

CVE

CVE-2023-38547
CVE-2023-38548
CVE-2023-38549
CVE-2023-41723

Fabricante

Veeam

Productos afectados

Todas las versiones de Veeam ONE anteriores a las siguientes, que han sido actualizadas para parchar estas vulnerabilidades:

Veeam ONE 12 P20230314 (12.0.1.2591)

Veeam ONE 11a (11.0.1.1880)

Veeam ONE 11 (11.0.0.1379)

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00934-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

5. Noticias y concientización

Chile obtuvo primer y segundo lugar en la final del OEA Cyberwomen Challenge en Colombia



A fines de septiembre del año 2022 se llevó a cabo de forma online en nuestro país la 5ta edición del OEA Cyberwomen Challenge. El evento fue organizado por la OEA y el CSIRT de Gobierno y congregó a mujeres de distintas regiones de nuestro país, quienes formaron equipos para enfrentarse a diversos retos de ciberseguridad.

Las ganadoras de esa ocasión, Gabriela Mayro, Melissa Silva, Paola de la Vega, Lizette González y Marta Castillo, tuvieron la oportunidad de participar en la final regional del OEA Cyberwomen Challenge que se realizó el 1 de noviembre de este año en Colombia, y competir contra 11 equipos más provenientes de Argentina, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, México, Panamá, Paraguay, República Dominicana y Uruguay.

La nota completa: <https://www.csirt.gob.cl/noticias/chile-obtuvo-primer-y-segundo-lugar-en-la-final-del-oea-cyberwomen-challenge/>

CONTACTO Y REDES SOCIALES CSIRT

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

Ciberconsejos | ¿Qué hacer si te roban la cuenta de Whatsapp?

El robo de cuentas de WhatsApp se está convirtiendo en una de las formas más utilizada por los ciberdelincuentes para suplantar la identidad de la víctima y robar dinero. ¿Qué hacer si te roban tu cuenta y cómo prevenir?

La campaña completa, para descargar y compartir sus infografías con sus trabajadores, amigos y familiares, aquí: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-robo-cuenta-whatsapp/>



¿QUÉ HACER SI TE ROBAN LA CUENTA DE WHATSAPP?

1 Ingresa nuevamente tu número en la app

2 Al ingresar tu número, te pedirá un código de verificación. Ingrévalo para recuperar tu cuenta.

Una vez que secuestran, tu whatsapp aparece este mensaje.

Tu número de teléfono ya no está registrado con WhatsApp en este teléfono. Esto puede ser porque lo registraste en otro teléfono.

Si no lo hiciste, verifica tu número de teléfono para volver a iniciar sesión en tu cuenta.

VERIFICAR OK

Te damos la bienvenida a WhatsApp

Ingresar tu número de teléfono

Verificación de tu número

CONTACTO Y REDES SOCIALES CSIRT

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

6. Recomendaciones y buenas prácticas

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

CONTACTO Y REDES SOCIALES CSIRT

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.

- Ender Salas
- Emilio De La Maza
- Hellis Leiva
- Julio López
- Juan Correa Poblete
- Martín Alonso Muñoz Maulen
- Pablo Andres Bustos Gonzalez
- Juan Carlos Molina
- Jose Camelio
- Diego Concha de la Fuente
- Florencia Rojas González
- Exequiel Moisés Medina Parra
- Pablo Ignacio Pizarro Cortínez
- Clemente Zamudio
- Paula Andrea Sepúlveda Cruz
- Jorge Federico Ernesto von Bischoffshausen Ávalos
- Constanza Valentina Arroyo Carreño
- Loredana Arata Reyes

CONTACTO Y REDES SOCIALES CSIRT