



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 207

semana del 16 al 22 de junio de 2023

# LA SEMANA EN CIFRAS

## IP INFORMADAS

14

IP advertidas en múltiples campañas de phishing y de malware.



## URL ADVERTIDAS

23

URL asociadas a sitios fraudulentos y campañas de phishing y malware



## PARCHES COMPARTIDOS

8

Las mitigaciones son útiles en productos de VMware y Progress (MOVEit).



## HASH REPORTADOS

9

Hashes asociados a múltiples campañas de phishing con archivos que contienen malware



# CONTENIDO

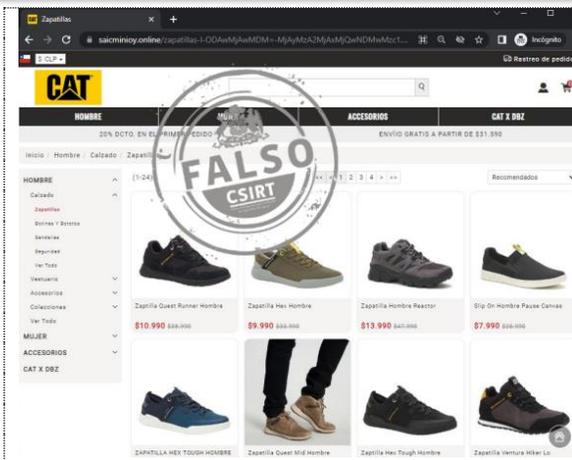
|    |  |    |
|----|--|----|
| 1. | Sitios fraudulentos .....                | 3  |
| 2. | Phishing .....                           | 7  |
| 3. | Malware.....                             | 9  |
| 4. | Vulnerabilidades .....                   | 10 |
| 5. | Concientización.....                     | 12 |
| 6. | Recomendaciones y buenas prácticas ..... | 15 |
| 7. | Muro de la Fama .....                    | 16 |

# Boletín de Seguridad Cibernética N° 207

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

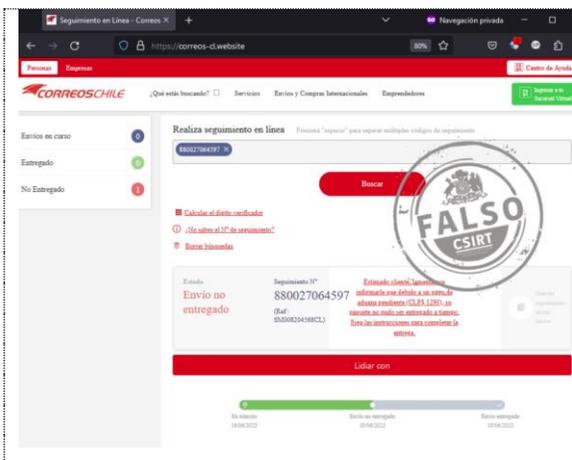
BOLETÍN 13BCS23-00216-01 | Semana del 16 al 22 de junio de 2023

## 1. Sitios fraudulentos



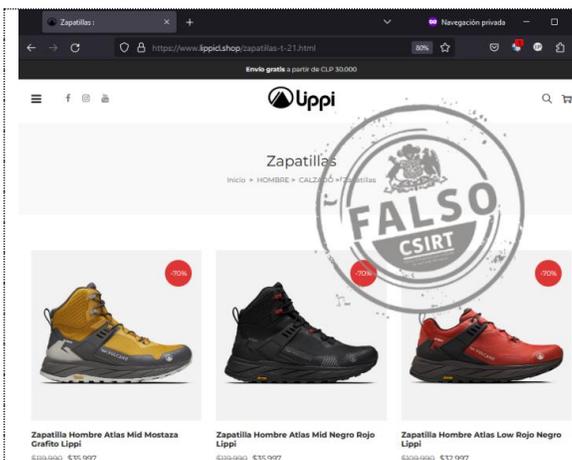
### CSIRT alerta de nueva página fraudulenta que suplanta a Caterpillar

|  |   |
|--|---|
| Alerta de seguridad cibernética        | 8FFR23-01409-01   |
| Clase de alerta                        | Fraude  |
| Tipo de incidente                      | Falsificación de Registros o Identidad  |
| Nivel de riesgo                        | Alto  |
| TLP                                    | Blanco  |
| Fecha de lanzamiento original          | 19 de junio de 2023   |
| Última revisión                        | 19 de junio de 2023   |
| <b>Indicadores de compromiso</b>       |   |
| <b>URL sitio falso</b>                 | <a href="https://www.saicminioy[.]online/">https://www.saicminioy[.]online/</a>                                 |
| <b>Dirección IP</b>                    | [199.21.150.21]   |
| <b>Enlace para revisar el informe:</b> | <a href="https://www.csirt.gob.cl/alertas/8ffr23-01409-01">https://www.csirt.gob.cl/alertas/8ffr23-01409-01</a> |



### CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile

|  |   |
|--|---|
| Alerta de seguridad cibernética        | 8FFR23-01410-01   |
| Clase de alerta                        | Fraude  |
| Tipo de incidente                      | Falsificación de Registros o Identidad  |
| Nivel de riesgo                        | Alto  |
| TLP                                    | Blanco  |
| Fecha de lanzamiento original          | 19 de junio de 2023   |
| Última revisión                        | 19 de junio de 2023   |
| <b>Indicadores de compromiso</b>       |   |
| <b>URL sitio falso</b>                 | <a href="https://correos-cl[.]website/">https://correos-cl[.]website/</a>                                       |
| <b>Dirección IP</b>                    | [38.60.196.88]  |
| <b>Enlace para revisar el informe:</b> | <a href="https://www.csirt.gob.cl/alertas/8ffr23-01410-01">https://www.csirt.gob.cl/alertas/8ffr23-01410-01</a> |



### CSIRT alerta de nueva página fraudulenta que suplanta a Lippi

|  |   |
|--|---|
| Alerta de seguridad cibernética        | 8FFR23-01411-01   |
| Clase de alerta                        | Fraude  |
| Tipo de incidente                      | Falsificación de Registros o Identidad  |
| Nivel de riesgo                        | Alto  |
| TLP                                    | Blanco  |
| Fecha de lanzamiento original          | 19 de junio de 2023   |
| Última revisión                        | 19 de junio de 2023   |
| <b>Indicadores de compromiso</b>       |   |
| <b>URL sitio falso</b>                 | <a href="https://www.lippicl[.]shop">https://www.lippicl[.]shop</a>   |
| <b>Dirección IP</b>                    | [172.67.179.240]  |
| <b>Enlace para revisar el informe:</b> | <a href="https://www.csirt.gob.cl/alertas/8ffr23-01411-01">https://www.csirt.gob.cl/alertas/8ffr23-01411-01</a> |

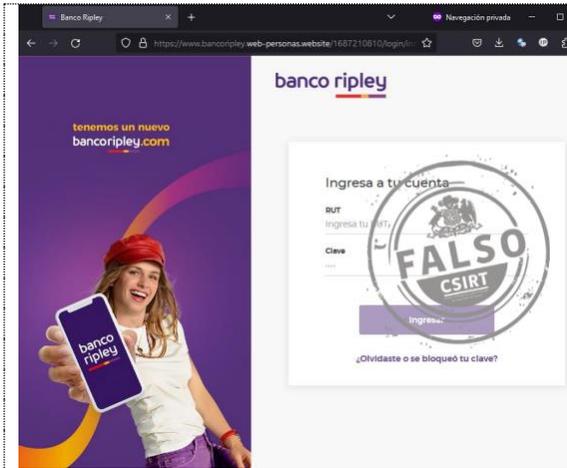
## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

# Boletín de Seguridad Cibernética N° 207

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

BOLETÍN 13BCS23-00216-01 | Semana del 16 al 22 de junio de 2023



## CSIRT alerta ante nueva página fraudulenta que suplanta a Banco Ripley

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR23-01412-01                        |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 19 de junio de 2023                    |
| Última revisión                 | 19 de junio de 2023                    |

### Indicadores de compromiso

#### URL sitio falso

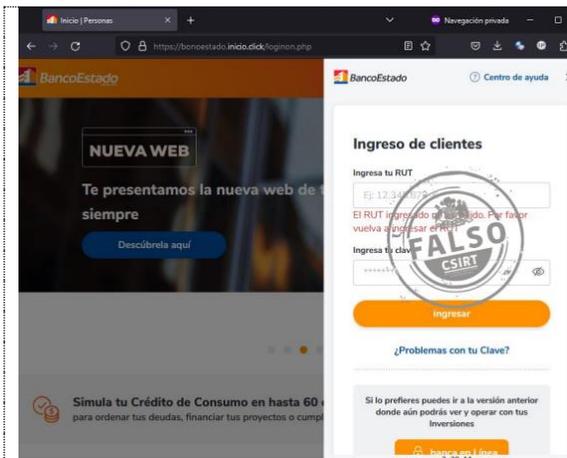
[https://www.bancoripley.web-personas\[.\]website/1687210810/login/index.html](https://www.bancoripley.web-personas[.]website/1687210810/login/index.html)

#### Dirección IP

[192.64.117.217]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01412-01>



## CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR23-01413-01                        |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 20 de junio de 2023                    |
| Última revisión                 | 20 de junio de 2023                    |

### Indicadores de compromiso

#### URL sitio falso

[https://bonoestado.inicio\[.\]click/loginon.php](https://bonoestado.inicio[.]click/loginon.php)

#### Dirección IP

[104.21.78.226]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01413-01>



## CSIRT alerta ante nuevo sitio fraudulento que suplanta a Wild Foods

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR23-01414-01                        |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 20 de junio de 2023                    |
| Última revisión                 | 20 de junio de 2023                    |

### Indicadores de compromiso

#### URL sitio falso

[https://sites.google\[.\]com/view/wildsoul-foods/wildsoul-foods](https://sites.google[.]com/view/wildsoul-foods/wildsoul-foods)

#### Dirección IP

[74.125.126.139]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8FFR23-01414-01>

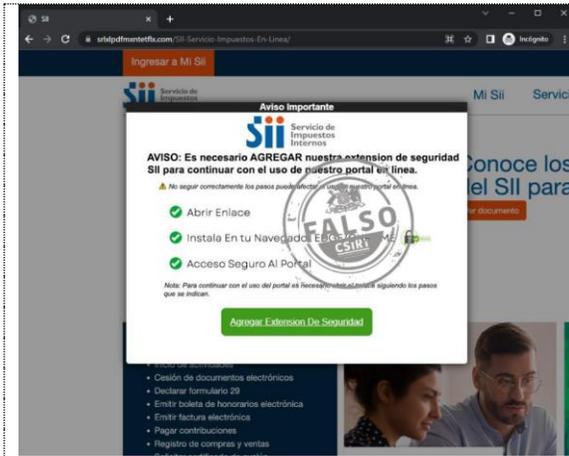
## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

# Boletín de Seguridad Cibernética N° 207

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

BOLETÍN 13BCS23-00216-01 | Semana del 16 al 22 de junio de 2023



## CSIRT alerta de nueva página fraudulenta que suplanta al Servicio de Impuestos Internos

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR23-01415-01                        |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 22 de junio de 2023                    |
| Última revisión                 | 22 de junio de 2023                    |

### Indicadores de compromiso

#### URL sitio falso

[https://srlx|pdfmxtetflx\[.\]com/SII-Servicio-Impuestos-En-Linea/](https://srlx|pdfmxtetflx[.]com/SII-Servicio-Impuestos-En-Linea/)

#### Dirección IP

[172.67.214.30]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8FFR23-01415-01>



## CSIRT alerta de nuevo sitio fraudulento que suplanta al SII

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR23-01416-01                        |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 22 de junio de 2023                    |
| Última revisión                 | 22 de junio de 2023                    |

### Indicadores de compromiso

#### URL sitio falso

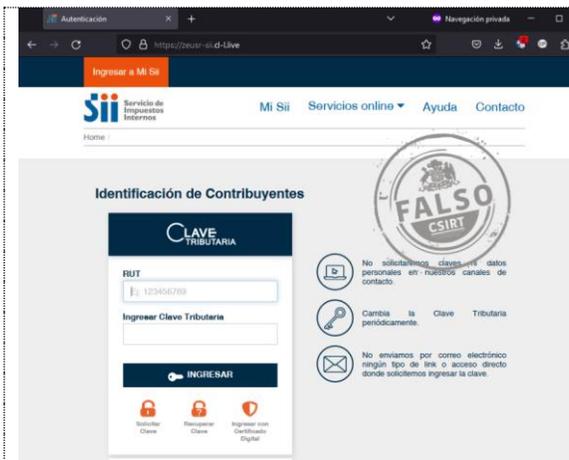
[http://170.39.230\[.\]80/inicio.html](http://170.39.230[.]80/inicio.html)

#### Dirección IP

[170.39.230.80]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8FFR23-01416-01>



## CSIRT alerta ante nuevo sitio falso que suplanta al Servicio de Impuestos Internos

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR23-01417-01                        |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 22 de junio de 2023                    |
| Última revisión                 | 22 de junio de 2023                    |

### Indicadores de compromiso

#### URL sitio falso

[https://zeusr-sii-cl-\[.\]live/](https://zeusr-sii-cl-[.]live/)

#### Dirección IP

[172.67.223.228]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8FFR23-01417-01>

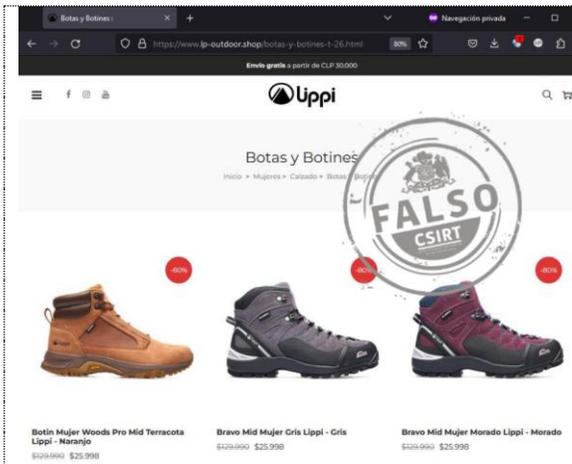
## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

# Boletín de Seguridad Cibernética N° 207

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

BOLETÍN 13BCS23-00216-01 | Semana del 16 al 22 de junio de 2023



## CSIRT alerta de nuevo sitio fraudulento que suplanta a Lippi

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR23-01418-01                        |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 22 de junio de 2023                    |
| Última revisión                 | 22 de junio de 2023                    |

### Indicadores de compromiso

#### URL sitio falso

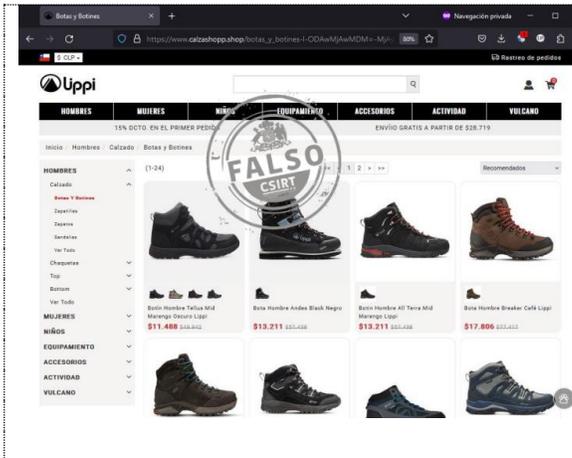
[https://www.lp-outdoor\[.\]shop/](https://www.lp-outdoor[.]shop/)

#### Dirección IP

[104.21.2.127]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8FFR23-01418-01>



## CSIRT alerta de nueva página fraudulenta que suplanta a Lippi

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR23-01419-01                        |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 22 de junio de 2023                    |
| Última revisión                 | 22 de junio de 2023                    |

### Indicadores de compromiso

#### URL sitio falso

[https://www.calzashopp\[.\]shop/](https://www.calzashopp[.]shop/)

#### Dirección IP

[199.21.150.9]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8FFR23-01419-01>

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

# Boletín de Seguridad Cibernética N° 207

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

BOLETÍN 13BCS23-00216-01 | Semana del 16 al 22 de junio de 2023

## 2. Phishing



### CSIRT alerta de una nueva página fraudulenta que suplanta a BancoEstado

|                                 |   |
|---------------------------------|---|
| Alerta de seguridad cibernética | 8FPH23-00836-01   |
| Clase de alerta                 | Fraude  |
| Tipo de incidente               | Phishing  |
| Nivel de riesgo                 | Alto  |
| TLP                             | Blanco  |
| Fecha de lanzamiento original   | 20 de junio de 2023   |
| Última revisión                 | 20 de junio de 2023   |
| <b>URL redirección</b>          | <a href="https://trylocal[.]com/wp-content/activacion/cuenta-kyhu/">https://trylocal[.]com/wp-content/activacion/cuenta-kyhu/</a>                                     |
| <b>URL sitio falso</b>          | <a href="https://homefogastadp[.]info/1686775823/imagenes/_personas/home/default.asp">https://homefogastadp[.]info/1686775823/imagenes/_personas/home/default.asp</a> |
| <b>Dirección IP</b>             | [107.190.131.66]  |
| <b>Enlace para revisar loC:</b> | <a href="https://www.csirt.gob.cl/alertas/8FPH23-00836-01/">https://www.csirt.gob.cl/alertas/8FPH23-00836-01/</a>   |



### CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado

|                                  |   |
|----------------------------------|---|
| Alerta de seguridad cibernética  | 8FPH23-00837-01   |
| Clase de alerta                  | Fraude  |
| Tipo de incidente                | Phishing  |
| Nivel de riesgo                  | Alto  |
| TLP                              | Blanco  |
| Fecha de lanzamiento original    | 20 de junio de 2023   |
| Última revisión                  | 20 de junio de 2023   |
| <b>Indicadores de compromiso</b> |   |
| <b>URL redirección</b>           | <a href="https://reachercontact[.]com/activacion/cuenta-zksc/">https://reachercontact[.]com/activacion/cuenta-zksc/</a>   |
| <b>URL sitio falso</b>           | <a href="https://comunistable[.]com/1687268783/imagenes/_personas/home/default.asp">https://comunistable[.]com/1687268783/imagenes/_personas/home/default.asp</a> |
| <b>Dirección IP sitio falso</b>  | [98.142.101.90]   |
| <b>Enlace para revisar loC:</b>  | <a href="https://www.csirt.gob.cl/alertas/8FPH23-00837-01/">https://www.csirt.gob.cl/alertas/8FPH23-00837-01/</a>   |

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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



## CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado

|                                  |   |
|----------------------------------|---|
| Alerta de seguridad cibernética  | 8FPH23-00838-01   |
| Clase de alerta                  | Fraude  |
| Tipo de incidente                | Phishing  |
| Nivel de riesgo                  | Alto  |
| TLP                              | Blanco  |
| Fecha de lanzamiento original    | 22 de junio de 2023   |
| Última revisión                  | 22 de junio de 2023   |
| <b>Indicadores de compromiso</b> |   |
| <b>URL redirección</b>           | <a href="https://www.hopgia[.jvn]/upload/news/activacion/cuenta-kzy">https://www.hopgia[.jvn]/upload/news/activacion/cuenta-kzy</a>                                       |
| <b>URL sitio falso</b>           | <a href="https://homefogastadp[.jinfo]/1687449138/imagenes/_personas/home/default.a sp">https://homefogastadp[.jinfo]/1687449138/imagenes/_personas/home/default.a sp</a> |
| <b>Dirección IP sitio falso</b>  | [107.190.131.66]  |
| <b>Enlace para revisar loC:</b>  | <a href="https://www.csirt.gob.cl/alertas/8FPH23-00838-01/">https://www.csirt.gob.cl/alertas/8FPH23-00838-01/</a>   |

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

## 3. Malware

Convocatoria Aviso de citación electrónica - (119935)

INTIMO <avisosjudicial@...>  
Para [Redacted] lu 19/06/2023 13:39

**Advertencia de Citación**

Buenos días Sr(a),

De conformidad con el art. 405, § 1 del Código de Procedimiento Civil se hace presente al INTIMO a su Señoría comparezca como testigo, en la audiencia que se celebrará a miércoles, 19 de junio de 2023.

Documento adjunto referente al trámite:  
[Citación Adjunta n° 50824559789200](#)



Resolución de Archivo Provisional: Accion Legal en curso - (150007)

DI Documentación Importante <avisosjudicial@...>  
Para [Redacted] lu 19/06/2023 13:40

**Notificación automática emitida por el sistema de poder judicial.**

Sigla la continuación con una copia del caso judicial en PDF.  
\*Descargue copia en PDF en el siguiente enlace:  
[Orden Investigativa Junio 2023/04 - Nº 931084011-29689](#)

[Orden Petición de Ejecución 2023/04 - Ref. - 7356-HI-2023](#)

Con el escrito electrónico del 19 de junio del año en curso y su archivo adjunto, téngase por cumplida la notificación dispuesta (a propósito de fecha: 18.06.2023), pidiéndose a resolver la presentación de fecha 19 de junio del corriente año 2023.  
Regístrase, notifíquese de oficio y por medios electrónicos (conf. art. 1 artículo 3 -1-1, resol. Presidencia) y complácese con el archivo ordenado.  
Suscripto y registrado por el Actuario Firmante, en la fecha indicada en la constancia de la firma digital (Lc. 3.971/20 y modif.).

### CSIRT alerta de nueva campaña de phishing con malware, que suplanta al Poder Judicial

|                                 |                     |
|---------------------------------|---------------------|
| Alerta de seguridad cibernética | 2CMV23-00419-01     |
| Clase de alerta                 | Fraude              |
| Tipo de incidente               | Malware             |
| Nivel de riesgo                 | Alto                |
| TLP                             | Blanco              |
| Fecha de lanzamiento original   | 20 de junio de 2023 |
| Última revisión                 | 20 de junio de 2023 |

#### Indicadores de compromiso

##### URL-Dominio

[https://jccrivelliabogadospubicidad.brazilsouth.cloudapp\[.\]azure.com/http://20.206.121\[.\]188/](https://jccrivelliabogadospubicidad.brazilsouth.cloudapp[.]azure.com/http://20.206.121[.]188/)  
[https://www.dropbox\[.\]com/s/dl/wdw1uk4rc4iihly/](https://www.dropbox[.]com/s/dl/wdw1uk4rc4iihly/)  
[https://www.dropbox\[.\]com/s/dl/0thjroopb2nae4x/](https://www.dropbox[.]com/s/dl/0thjroopb2nae4x/)  
[https://www.dropbox\[.\]com/s/dl/zl93ykl0jlz7dcr/](https://www.dropbox[.]com/s/dl/zl93ykl0jlz7dcr/)  
[http://ip-api\[.\]com/json](http://ip-api[.]com/json)

##### SHA256

58cfa0e09bc0acc1bc993045633ea70e3cd3797ff55d86045168fee3db2562e149123043ba4257cb61d00a931ea273f724a9cda06ec8eb107ddeab4d664ac8830604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15865f12dd2959457978155d2eb83833ea00d0afc06f3aa820866f6a55476ad3e484d73fd51c09a001c449100862d48062eee947bc2d632264f820cdf3393789ef0604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15816266195405aa5c6d9564f0db7fc58dca1c064558f7c96c47f7cbfc3bf68d7d5ccb8f4becf4f5c5440d62ebb9c21abf84d5c564eb72ec9d12f27fc8243079980604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15

##### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv23-00418-01/>

## 4. Vulnerabilidades



Ministerio del Interior y Seguridad Pública

### INFORME DE Vulnerabilidad

**9VSA23-00850-01**  
CSIRT comparte información de vulnerabilidades parchadas por MOVEit

PARA REGISTRAR | 1510  
UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)

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

**CSIRT comparte información de vulnerabilidades críticas en MOVEit, al menos una ya se encuentra siendo explotada**

|                                 |                              |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00850-01              |
| Clase de alerta                 | Vulnerabilidad               |
| Tipo de incidente               | Sistema y/o Software Abierto |
| Nivel de riesgo                 | Alto                         |
| TLP                             | Blanco                       |
| Fecha de lanzamiento original   | 16 de junio de 2023          |
| Última revisión                 | 16 de junio de 2023          |

#### CVE

CVE-2023-34362  
CVE-2023-35036

#### Fabricantes

Progress

#### Productos afectados

MOVEit Transfer 2023.0.0  
MOVEit Transfer 2022.1.x  
MOVEit Transfer 2022.0.x  
MOVEit Transfer 2021.1.x  
MOVEit Transfer 2021.0.x

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00850-01/>



Ministerio del Interior y Seguridad Pública

### INFORME DE Vulnerabilidad

**9VSA23-00851-01**  
CSIRT comparte información de nueva vulnerabilidad en MOVEit Transfer

PARA REGISTRAR | 1510  
UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)

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

**CSIRT comparte información de nueva vulnerabilidad en MOVEit Transfer**

|                                 |                              |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00851-01              |
| Clase de alerta                 | Vulnerabilidad               |
| Tipo de incidente               | Sistema y/o Software Abierto |
| Nivel de riesgo                 | Alto                         |
| TLP                             | Blanco                       |
| Fecha de lanzamiento original   | 20 de junio de 2023          |
| Última revisión                 | 20 de junio de 2023          |

#### CVE

CVE-2023-35708

#### Fabricante

MOVEit Transfer 2023.0.x (15.0.x)  
MOVEit Transfer 2022.1.x (14.1.x)  
MOVEit Transfer 2022.0.x (14.0.x)  
MOVEit Transfer 2021.1.x (13.1.x)  
MOVEit Transfer 2021.0.x (13.0.x)  
MOVEit Transfer 2020.1.x (12.1)  
MOVEit Transfer 2020.0.x (12.0) o anterior  
MOVEit Cloud

#### Productos afectados

Progress

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00851-01/>

### CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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



## CSIRT comparte información de nuevas vulnerabilidades en vCenter Server de VMware

|                                 |                              |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00852-01              |
| Clase de alerta                 | Vulnerabilidad               |
| Tipo de incidente               | Sistema y/o Software Abierto |
| Nivel de riesgo                 | Alto                         |
| TLP                             | Blanco                       |
| Fecha de lanzamiento original   | 22 de junio de 2023          |
| Última revisión                 | 22 de junio de 2023          |

### CVE

CVE-2023-20892  
CVE-2023-20893  
CVE-2023-20894  
CVE-2023-20895  
CVE-2023-20896

### Fabricantes

VMware

### Productos afectados

VCenter Server 7.0, 8.0.  
Cloud Foundation (vCenter Server) 5.x, 4.x

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00852-01/>

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

## 5. Concientización

### Ciberconsejos para evitar realizar falsas inversiones | CMF y CSIRT

En conjunto con la Comisión para el Mercado Financiero, en el CSIRT preparamos estos consejos para que no caigas en falsas inversiones, estafas que se promocionan con peligrosa facilidad en las redes sociales. Evita estafas y aumenta la seguridad de tus amigos y familiares compartiendo nuestros Ciberconsejos: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-cmf-y-csirt/>



### CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

## Exitosa cuarta versión de la simulación de ciberataque para funcionarios públicos, presentada por el CSIRT y Microsoft.

Más de 130 funcionarios públicos de todas las regiones del país participaron de la primera instancia telemática de las simulaciones de ciberataque que cada mes entrega el CSIRT de la mano de Microsoft, sesiones que comenzaron en marzo.

Como en las presentaciones anteriores, los funcionarios participantes pudieron presenciar un video que simula las distintas situaciones a las que se enfrentan las diferentes funciones dentro de una organización que sufre un ciberataque, y las decisiones que deben ir tomando, enfatizando la importancia que tiene el rol que debe tener la ciberseguridad en una empresa o entidad pública, y la necesidad de crear planes de contingencia y recuperación conocidos a todo nivel de la organización.



### SIMULACIÓN DE CIBERATAQUE | VERSIÓN TELEMÁTICA

El CSIRT de Gobierno le invita a participar de una simulación de ciberataque en tiempo real, realizada por Microsoft, que pone a sus participantes en el lugar de una organización que enfrenta un incidente de ciberseguridad que amenaza su continuidad operacional.

**La actividad será TELEMÁTICA**, y se realizará el jueves 22 de junio, de 9:30 a 11:30 horas.

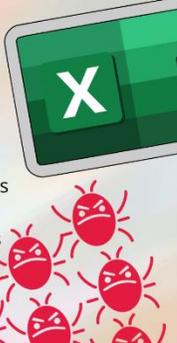
**Para inscribirse solo necesita responder al formulario que se incluye en el mensaje anexo, o escribir a [comunicaciones@interior.gob.cl](mailto:comunicaciones@interior.gob.cl) con su nombre, institución y región en la que se desempeña.**

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

## Ciberdiccionario Volumen 39

Nuevas definiciones se suman al Ciberdiccionario del CSIRT esta semana, la primera del invierno. Añadimos los significados, en el contexto de la ciberseguridad, de entropía, virus de macros, STEM y CIO. Esperamos que les resulten útiles. Todos los volúmenes del ciberdiccionario, junto al resto de nuestras recomendaciones están contenidas siempre en: <http://csirt.gob.cl/recomendaciones>.

|  |   |
|--|---|
|  <h3>Ciber diccionario</h3> <p><b>Virus de macros</b></p> <p>Tipo de malware que se propaga utilizando macros, las secuencias de comandos automatizadas utilizados en procesadores de texto y hojas de cálculo, como los populares Word y Excel. Así, este tipo de virus utiliza la capacidad de ejecución de las macros para infectar los archivos y sistemas de un equipo. Por eso solo debemos ejecutar archivos de fuentes conocidas y analizados por antivirus.</p>  |  <h3>Ciber diccionario</h3> <p><b>CIO</b></p> <p>CIO viene de la sigla en inglés de "chief information officer" o director de tecnologías de la información (TI). Es el cargo ejecutivo responsable de la gestión y dirección de las personas, procesos y activos relativos a las TI en la organización. Dada la creciente importancia de las tecnologías en los negocios, el CIO debe participar de las decisiones estratégicas de la organización y trabajar de cerca a la gerencia general.</p>  |
|  <h3>Ciber diccionario</h3> <p><b>STEM</b></p> <p>Sigla en inglés utilizada para referirse a las disciplinas académicas correspondientes a Ciencias, Tecnologías, Ingeniería y Matemáticas (<i>Science, Technology, Engineering y Mathematics</i>). La enseñanza de tecnología y ciberseguridad a escolares y universitarios se enmarca muchas veces en el contexto del desarrollo de habilidades STEM.</p>    |  <h3>Ciber diccionario</h3> <p><b>Entropía</b></p> <p>Una de las acepciones de entropía en la informática tiene relación con la generación de claves criptográficas. Una clave criptográfica con alta entropía (aleatoriedad) es más difícil de adivinar o descifrar, por lo tanto, en el contexto de un ransomware, se refiere a la utilización de algoritmos de cifrado fuertes y claves aleatorias de difícil descifrado.</p>    |

## 6. Recomendaciones y buenas prácticas

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

### CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

## 7. Muro de la Fama

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

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

- Juan Pablo Berríos
- Luis Miguel Bravo Ramírez
- David Soto
- Enrique Moraga
- Andrés Rodríguez
- Pamela Lillo Fabres
- Andrea de los Ángeles Salas Piraino
- Sergio Sanguinetti
- Manuel Alfredo Carvajal Castillo
- Rodrigo Andrés Silva Maldonado
- Rafael

### CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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