



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 216

semana del 18 al 24 de agosto de 2023

# LA SEMANA EN CIFRAS

## IP INFORMADAS

4

IP advertidas en múltiples campañas de phishing y de fraude.



## URL ADVERTIDAS

5

URL asociadas a sitios fraudulentos y campañas de phishing y malware



## PARCHES COMPARTIDOS

5

Las mitigaciones son útiles en productos de Juniper y WinRAR.

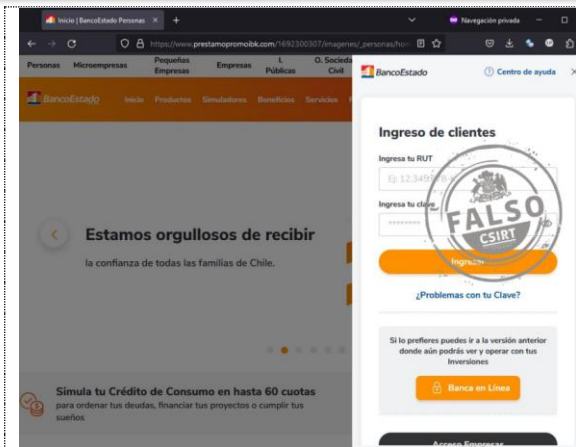


# CONTENIDO

1.	Sitios fraudulentos .....	3
2.	Phishing .....	4
3.	Vulnerabilidades .....	5
4.	Concientización .....	6
5.	Recomendaciones y buenas prácticas .....	8
6.	Muro de la Fama .....	9

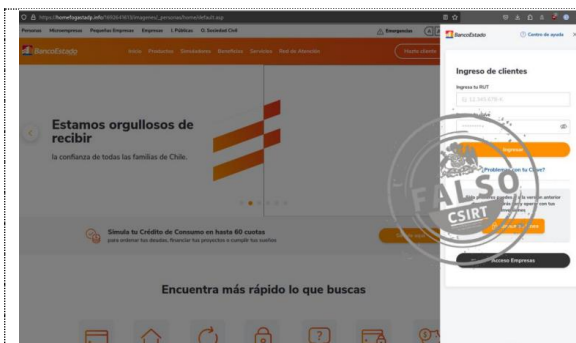


## 1. Sitios fraudulentos



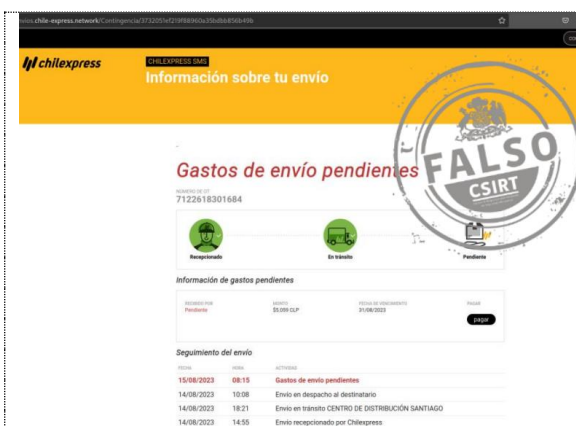
### CSIRT alerta de sitio fraudulento que suplanta a BancoEstado

Alerta de seguridad cibernética	8FFR23-01498-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 agosto, 2023
Última revisión	21 agosto, 2023
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	<a href="https://www.prestamopromoibk[.]com/1692300307/imagenes/_personas/home/default.asp">https://www.prestamopromoibk[.]com/1692300307/imagenes/_personas/home/default.asp</a>
<b>IP del sitio falso</b>	[64.37.50.122]
<b>Enlace para revisar el informe:</b>	<a href="https://www.csirt.gob.cl/alertas/8ffr23-01498-01/">https://www.csirt.gob.cl/alertas/8ffr23-01498-01/</a>



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

Alerta de seguridad cibernética	8FFR23-01499-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 agosto, 2023
Última revisión	21 agosto, 2023
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	<a href="https://homefogastadp.info/1692641613/imagenes/_personas/home/default.asp">https://homefogastadp.info/1692641613/imagenes/_personas/home/default.asp</a>
<b>Dirección IP</b>	[107.190.131.66]
<b>Enlace para revisar el informe:</b>	<a href="https://www.csirt.gob.cl/alertas/8ffr23-01499-01/">https://www.csirt.gob.cl/alertas/8ffr23-01499-01/</a>



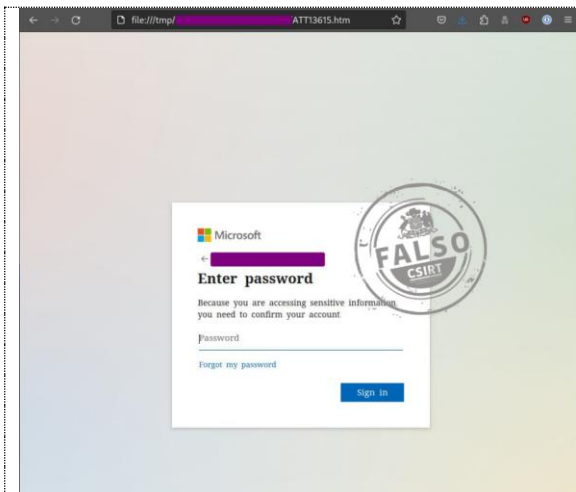
### CSIRT alerta de nueva página fraudulenta que suplanta a Chilexpress

Alerta de seguridad cibernética	8FFR23-01500-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 agosto, 2023
Última revisión	22 agosto, 2023
<b>Indicadores de compromiso</b>	
<b>URL redirección</b>	<a href="https://r.chile-express[.]network/r/KSj4kms">https://r.chile-express[.]network/r/KSj4kms</a>
<b>URL sitio falso</b>	<a href="https://sercarnet[.]cl/chilexpress">https://sercarnet[.]cl/chilexpress</a>
<b>Dirección IP</b>	[179.43.142.224]
<b>Enlace para revisar el informe:</b>	<a href="https://www.csirt.gob.cl/alertas/8ffr23-01500-01/">https://www.csirt.gob.cl/alertas/8ffr23-01500-01/</a>

## CONTACTO Y REDES SOCIALES CSIRT

<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>

## 2. Phishing



### CSIRT alerta de nueva campaña de phishing en falsa liquidación





Alerta de seguridad cibernética	8FPH23-00878-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
<b>URL redirección</b>	N/A
<b>URL sitio falso</b>	<a href="https://voipdataentuoercall.store/kokanaye/data.php">https://voipdataentuoercall.store/kokanaye/data.php</a>
<b>Dirección IP</b>	[192.64.119.209]
<b>Enlace para revisar loC:</b>	<a href="https://www.csirt.gob.cl/alertas/8fph23-00878-01/">https://www.csirt.gob.cl/alertas/8fph23-00878-01/</a>



### CSIRT alerta de nueva campaña de phishing con falsa renovación de cuenta de correo

Alerta de seguridad cibernética	8FPH23-00879-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 agosto, 2023
Última revisión	14 agosto, 2023
<b>Indicadores de compromiso</b>	
<b>URL redirección</b>	N/A
<b>URL sitio falso</b>	<a href="https://mesadeayuda.brizy[.]site/">https://mesadeayuda.brizy[.]site/</a>
<b>Dirección IP sitio falso</b>	N/A
<b>Enlace para revisar loC:</b>	<a href="https://www.csirt.gob.cl/alertas/8fph23-00879-01/">https://www.csirt.gob.cl/alertas/8fph23-00879-01/</a>

### CONTACTO Y REDES SOCIALES CSIRT

-  <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. Vulnerabilidades



Ministerio del Interior y Seguridad Pública

### INFORME DE Vulnerabilidad

**9VSA23-00884-01**  
CSIRT comparte vulnerabilidad que afecta a WinRAR, parchada en su última versión

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



### CSIRT comparte información de vulnerabilidad en WinRAR, ya parchada

Alerta de seguridad cibernética	9VSA23-00884-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 agosto, 2023
Última revisión	21 agosto, 2023

#### CVE

CVE-2023-40477

#### Fabricante

WinRAR

#### Productos afectados

WinRAR

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00884-01/>



Ministerio del Interior y Seguridad Pública

### INFORME DE Vulnerabilidad

**9VSA23-00885-01**  
CSIRT comparte información de vulnerabilidades parchadas en Junos OS

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



### CSIRT comparte información de vulnerabilidades parchadas en Juniper OS

Alerta de seguridad cibernética	9VSA23-00885-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 agosto, 2023
Última revisión	21 agosto, 2023

#### CVE

CVE-2023-36844

CVE-2023-36845

CVE-2023-36846

CVE-2023-36847

#### Fabricante

Juniper

#### Productos afectados

Junos OS

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00885-01/>

## CONTACTO Y REDES SOCIALES CSIRT

<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>

## 4. Concientización

### Lleno total en la tercera conferencia 8.8 Gobierno, que en esta ocasión tuvo como sede la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile

Desarrollada en conjunto por el CSIRT del Ministerio del Interior y 8.8, la tercera edición de la conferencia 8.8 Gobierno fue nuevamente un éxito, logrando reunir unos 200 asistentes entre funcionarios públicos y estudiantes de Ingeniería Civil en Computación de la Universidad de Chile.

Quienes formaron parte del evento pudieron presenciar las exposiciones de Daniel Álvarez, coordinador nacional de Ciberseguridad; el senador Kenneth Pugh; Sabina Torres, asesora del CSIRT, César Cerrudo, famoso hacker argentino y, en una presentación especialmente valorada por los estudiantes presentes, “Aprender Ju(hack)gando”, de Caetano Borges, estudiante de Ingeniería Civil en Computación de la Universidad Católica y Renato Garretón, content developer en OffSec, quienes mostraron cómo las competencias de ciberseguridad ayudan a descubrir bugs y vulnerabilidades.

Agradecemos finalmente la bienvenida entregada por el decano de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, profesor Francisco Martínez, y la disposición de la facultad y del Departamento de Ciencias de la Comunicación (DCC) de la Universidad de Chile, quienes acogieron este evento y nos apoyaron de forma invaluable para lograr su exitosa ejecución.



El coordinador Nacional de Ciberseguridad, Daniel Álvarez, realizando su exposición.

### CONTACTO Y REDES SOCIALES CSIRT

<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>



## Ciberconsejos | El candado verde NO significa seguridad

El candado en la barra de direcciones, o la mención https (en lugar de solo http) solían ser un buen indicio para determinar si una página era auténtica o maliciosa. Pero ya no. En los Ciberconsejos de esta semana explicamos qué pasó y recordamos la importancia de estar siempre alertos y suspicaces, debiendo fijarnos en la dirección de las páginas web que visitamos, para cerciorarnos de estar en los sitios en que realmente creemos estar.

Aquí, también en PDF: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-candado/>.



**CIBERCONSEJOS**  
**CUIDADO CON EL CANDADO VERDE: NO SIGNIFICA QUE UN SITIO SEA SEGURO**

**Candado verde NO significa seguridad**

Antiguamente, que apareciera un candado o https en la barra de direcciones indicaban que el sitio probablemente era seguro. Esto, porque contar con ellos requiere de la compra de un certificado digital.

Pero el costo de estos certificados cayó, siendo hoy conveniente para los ciberdelincuentes usarlos en sus sitios falsos para darles credibilidad.

**HTTPS://**

**Candado verde NO significa seguridad**

Por esto, el llamado es no confiar de manera automática en los sitios con candado o https.

Debemos mantenernos siempre alerta en internet, fijándonos bien en que las direcciones que se muestran sean la de los sitios oficiales.

También es útil estar al tanto de las últimas alertas de sitios fraudulentos que publicamos en [csirt.gob.cl/alertas](https://www.csirt.gob.cl/alertas)

### CONTACTO Y REDES SOCIALES CSIRT

<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. 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

 <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>

## 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.

- Hernaldo Andrés Salazar Mendoza.
- Pablo Pizarro Cortínez.
- Betzabé Fabiola Galaz Nader.
- Diego Ignacio Concha de la Fuente.
- Rocío Becerra Álvarez.
- Novita.
- Miguel Morales Saravia.
- Alexander Vianney.
- Thiare Lizama.
- Enrique Moraga.
- Luis Egaña Valle.
- Gonzalo Andrés Araya Navarrete.
- Wladimir Alexis Medina González.
- Paula Galdames Bazaes.
- Bruno.
- Constanza Ignacia Saint Jean Careaga.
- Francisco Flefil.
- Ignacio.
- René Valdés.

### CONTACTO Y REDES SOCIALES CSIRT