



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 202

semana del 12 al 18 de mayo de 2023

# LA SEMANA EN CIFRAS

## IP INFORMADAS

14

IP advertidas en múltiples campañas de phishing y de malware.



## URL ADVERTIDAS

28

URL asociadas a sitios fraudulentos y campañas de phishing y malware



## PARCHES COMPARTIDOS

16

Las mitigaciones son útiles en productos de Elementor (para Wordpress), Google (Chrome) y Cisco.



## HASH REPORTADOS

6

asociadas a múltiples campañas de phishing con archivos que contienen malware



# CONTENIDO

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

11111<



## 1. Sitios fraudulentos



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

Alerta de seguridad cibernética	8FFR23-01320-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023

#### Indicadores de compromiso

#### URL sitio falso

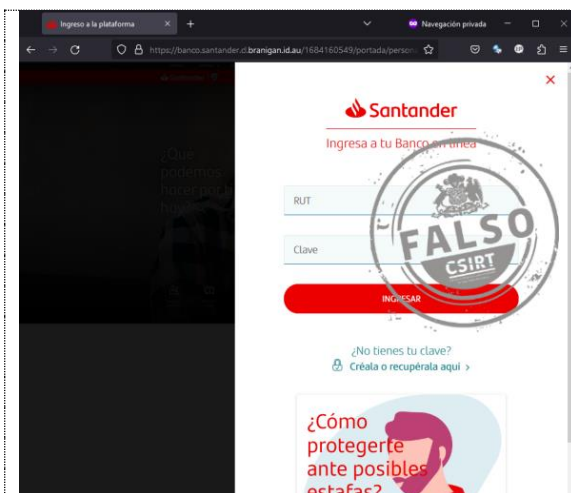
[https://t\[.\]co/HkG1dGu25c](https://t[.]co/HkG1dGu25c)  
[https://iruccs\[.\]cn/u4gb8cq6/fonasa-v3/?\\_t=1684157041148#1684157049446](https://iruccs[.]cn/u4gb8cq6/fonasa-v3/?_t=1684157041148#1684157049446)

#### Dirección IP

[104.21.23.119]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01320-01>



### CSIRT alerta de un nuevo sitio fraudulento que suplanta al Banco Santander

Alerta de seguridad cibernética	8FFR23-01321-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023

#### Indicadores de compromiso

#### URL sitio falso

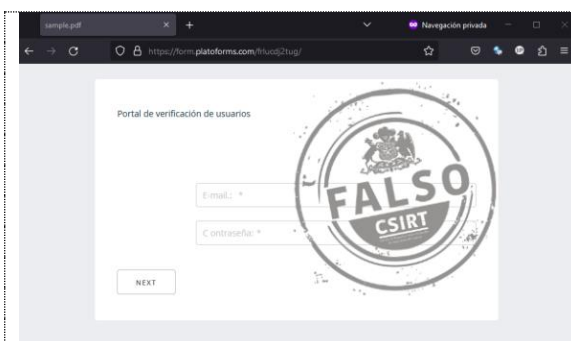
[https://banco.santander.cl/branigan\[.\]id.au/1684160549/portada/personas/home.asp](https://banco.santander.cl/branigan[.]id.au/1684160549/portada/personas/home.asp)

#### Dirección IP

[116.0.23.203]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01321-01>



### CSIRT alerta de sitio fraudulento que suplanta página de inicio de sesión de correo

Alerta de seguridad cibernética	8FFR23-01322-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2023
Última revisión	16 de mayo de 2023

#### Indicadores de compromiso

#### URL sitio falso

[https://form.platoforms\[.\]com/frlucdj2tug/](https://form.platoforms[.]com/frlucdj2tug/)

#### Dirección IP

[104.21.52.2]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01322-01>

### CSIRT alerta de página fraudulenta que suplanta a Cencosud Scotiabank

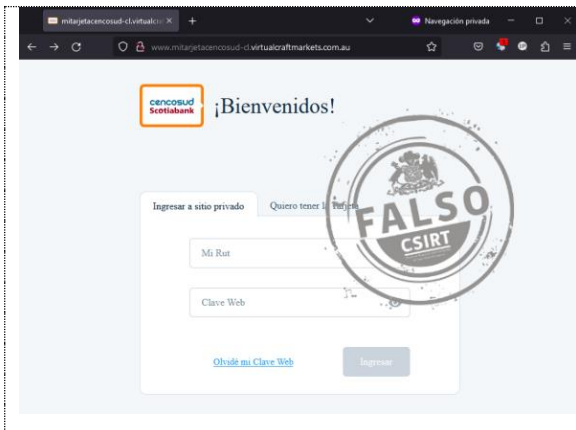
## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 202

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

BOLETÍN 13BCS23-00211-01 | Semana del 12 al 18 de mayo de 2023



Alerta de seguridad cibernética	8FFR23-01323-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2023
Última revisión	16 de mayo de 2023

#### Indicadores de compromiso9

#### URL sitio falso

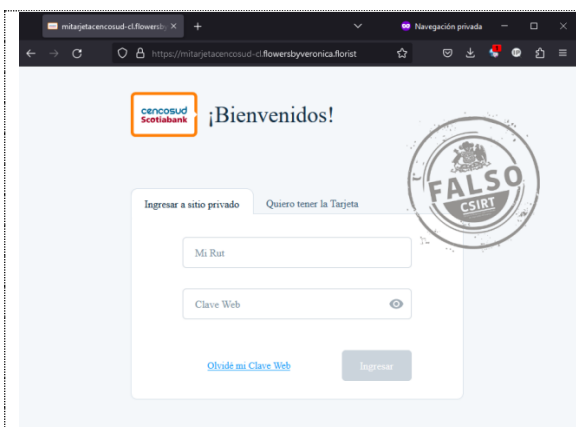
[http://www.mitarjetacencosud-cl.virtualcraftmarkets\[.\]com.au/](http://www.mitarjetacencosud-cl.virtualcraftmarkets[.]com.au/)

#### Dirección IP

[103.20.202.161]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01323-01>



#### CSIRT alerta de sitio fraudulento que suplanta a Cencosud Scotiabank

Alerta de seguridad cibernética	8FFR23-01324-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2023
Última revisión	16 de mayo de 2023

#### Indicadores de compromiso9

#### URL sitio falso

[http://wordpress.zuliatec\[.\]com.ve/cuentas/cuenta-test/](http://wordpress.zuliatec[.]com.ve/cuentas/cuenta-test/)

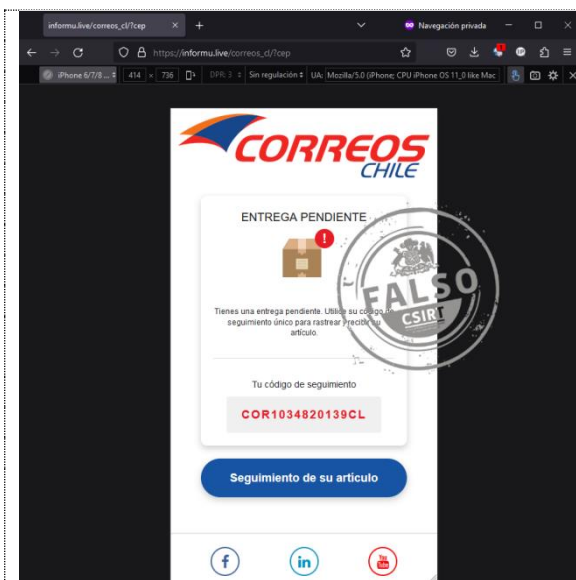
[https://mitarjetacencosud-cl.flowersbyveronica\[.\]florist/](https://mitarjetacencosud-cl.flowersbyveronica[.]florist/)

#### Dirección IP

[185.184.154.1]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01324-01>



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

Alerta de seguridad cibernética	8FFR23-01325-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de mayo de 2023
Última revisión	17 de mayo de 2023

#### Indicadores de compromiso9

#### URL sitio falso

[http://pspa\[.\]me/ZE2cl4](http://pspa[.]me/ZE2cl4)

[https://informu.live/correos\\_cl/?cep](https://informu.live/correos_cl/?cep)

#### Dirección IP

[93.95.227.126]

#### Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01325-01>

#### CSIRT alerta de sitio fraudulento que suplanta a Banco Ripley

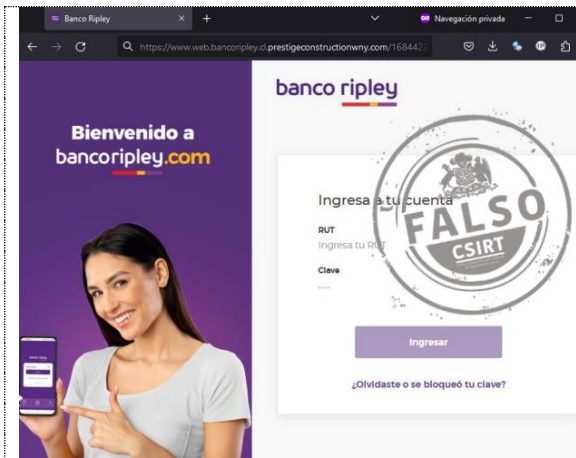
## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

# Boletín de Seguridad Cibernética N° 202

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

BOLETÍN 13BCS23-00211-01 | Semana del 12 al 18 de mayo de 2023



Alerta de seguridad cibernética	8FFR23-01326-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de mayo de 2023
Última revisión	18 de mayo de 2023
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	<a href="https://www.web.bancoripley.cl/prestigeconstructionwny.com/1684422767/login">https://www.web.bancoripley.cl/prestigeconstructionwny.com/1684422767/login</a>
<b>Dirección IP</b>	[192.185.21.172]
<b>Enlace para revisar el informe:</b>	<a href="https://www.csirt.gob.cl/alertas/8ffr23-01326-01">https://www.csirt.gob.cl/alertas/8ffr23-01326-01</a>

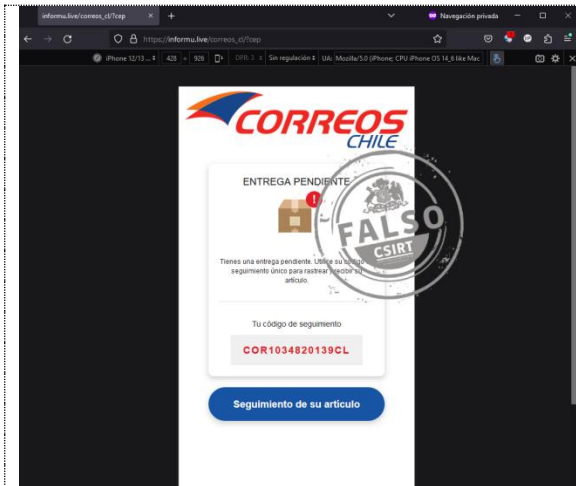


<b>CSIRT alerta ante sitio fraudulento que suplanta a Coca-Cola</b>	
Alerta de seguridad cibernética	8FFR23-01327-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de mayo de 2023
Última revisión	18 de mayo de 2023
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	<a href="https://www.daily-markets.co/lp-cola-es/">https://www.daily-markets.co/lp-cola-es/</a>
<b>Dirección IP</b>	[172.67.176.187]
<b>Enlace para revisar el informe:</b>	<a href="https://www.csirt.gob.cl/alertas/8ffr23-01327-01">https://www.csirt.gob.cl/alertas/8ffr23-01327-01</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>

## 2. Phishing



### CSIRT alerta de nueva campaña de phishing, que suplanta a CorreosChile

Alerta de seguridad cibernética	8FPH23-00808-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de mayo de 2023
Última revisión	12 de mayo de 2023

#### URL redirección

[http://eaaa\[.\]me/ZEE3Hy](http://eaaa[.]me/ZEE3Hy)

#### URL sitio falso

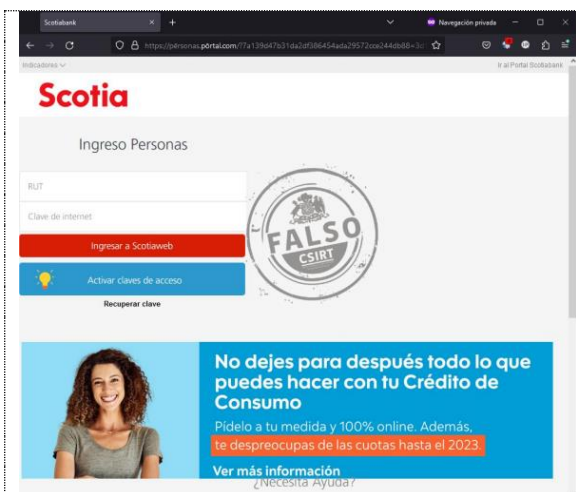
[https://informu.live/correos\\_cl/?cep](https://informu.live/correos_cl/?cep)

#### Dirección IP

[93.95.227.126]

#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00808-01/>



### CSIRT alerta de nueva campaña de phishing, que suplanta al banco Scotia

Alerta de seguridad cibernética	8FPH23-00809-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de mayo de 2023
Última revisión	12 de mayo de 2023

#### Indicadores de compromiso

#### URL sitio falso

[https://qrco\[.\]de/46199a88e8921dedd2c68b8252f6afcf8fc56902?trackid=OBMSXPTVMK](https://qrco[.]de/46199a88e8921dedd2c68b8252f6afcf8fc56902?trackid=OBMSXPTVMK)

[https://qrco\[.\]de/46199a88e8921dedd2c68b8252f6afcf8fc56902?trackid=ISESLXOVHB](https://qrco[.]de/46199a88e8921dedd2c68b8252f6afcf8fc56902?trackid=ISESLXOVHB)

#### URL redirección:

[https://p̄ersonas.p̄ortal\[.\]com/?7a139d47b31da2df386454ada29572cce244db88=3d1dd3a2e1ab9329b4ffc31f3d98ab92&p=login&country=CL&lang=es](https://p̄ersonas.p̄ortal[.]com/?7a139d47b31da2df386454ada29572cce244db88=3d1dd3a2e1ab9329b4ffc31f3d98ab92&p=login&country=CL&lang=es)

#### Dirección IP sitio falso

[3.0.200.196]

#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00809-01/>

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

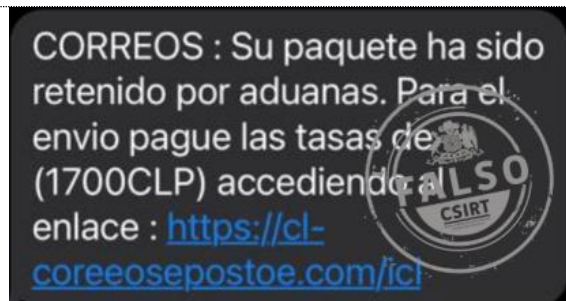
<https://www.csirt.gob.cl>  
Teléfonos: 1510 | + (562) 24863850 | Correo: [soc@interior.gob.cl](mailto:soc@interior.gob.cl)  
[@csirtgob](https://twitter.com/csirtgob)  
<https://www.linkedin.com/company/csirt-gob>



# Boletín de Seguridad Cibernética N° 202

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

BOLETÍN 13BCS23-00211-01 | Semana del 12 al 18 de mayo de 2023



## CSIRT alerta de nueva campaña de phishing que suplanta a CorreosChile

Alerta de seguridad cibernética	8FPH23-00810-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023

### Indicadores de compromiso

#### URL redirección

<https://cl-coreeosepostoe.com/ici>

#### URL sitio falso

<https://cl-coreeosepostoe.com/ici/parcel/>

#### Dirección IP sitio falso

[3.0.200.196]

#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00810-01/>



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

Alerta de seguridad cibernética	8FPH23-00811-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023

### Indicadores de compromiso

#### URL redirección

<https://hopgia.vn/module/activacion/cuenta-kzho/>

#### URL sitio falso

[https://homepatitostadof.bio/1684159549/imagenes/\\_personas/home/default.asp](https://homepatitostadof.bio/1684159549/imagenes/_personas/home/default.asp)

#### Dirección IP sitio falso

[172.67.202.214]

#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00811-01/>



## CSIRT alerta de campaña de phishing por SMS que suplanta a CorreosChile

Alerta de seguridad cibernética	8FPH23-00812-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2023
Última revisión	16 de mayo de 2023

### Indicadores de compromiso

#### URL redirección

<http://jxfs.me/ZEWYVN>

#### URL sitio falso

[https://informu.live/correos\\_cl?cep=](https://informu.live/correos_cl?cep=)

#### Dirección IP sitio falso

[93.95.227.126]

#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00812-01/>

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

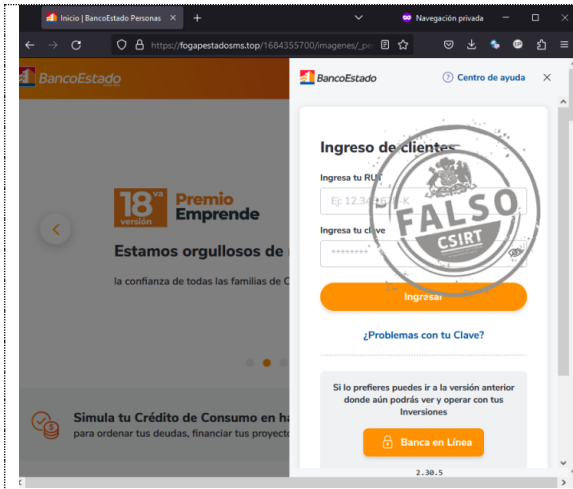
<https://www.csirt.gob.cl>  
Teléfonos: 1510 | + (562) 24863850 | Correo: [soc@interior.gob.cl](mailto:soc@interior.gob.cl)  
[@csirtgob](https://twitter.com/csirtgob)  
<https://www.linkedin.com/company/csirt-gob>



# Boletín de Seguridad Cibernética N° 202

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

BOLETÍN 13BCS23-00211-01 | Semana del 12 al 18 de mayo de 2023



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

Alerta de seguridad cibernética	8FPH23-00813-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de mayo de 2023
Última revisión	18 de mayo de 2023

### Indicadores de compromiso

#### URL redirección

[https\[:\]//hopgia\[.\]vn/module/activacion/cuenta-kzho/](https[:]//hopgia[.]vn/module/activacion/cuenta-kzho/)

#### URL sitio falso

[https\[:\]//fogapestadosms\[.\]top/1684355700/imagenes/\\_personas/home/default.asp](https[:]//fogapestadosms[.]top/1684355700/imagenes/_personas/home/default.asp)

#### Dirección IP sitio falso

[172.67.140.95]



#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00813-01/>

## 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>

## 3. Malware

<p>ACTA JUDICIAL UNIDAD JURIDICA</p> <p>HL Hipolito Lagos &lt;hlagosos@gmail.com&gt; Para CCO</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>Primera instancia, número de ingreso ( 132000020 )</p> <p>Casillero Judicial No: 07 Juzgado 02 Casillero Judicial Electrónico No: 01 En el siguiente Documento le dejó la información anexada</p> <p>CLAVE DEL FORMULARIO: 092 Consulta el proceso judicial:</p> <p><a href="#">CONSULTAR Demanda</a></p> 	<p><b>CSIRT alerta de nueva campaña de phishing con malware, difundido via una falsa acta judicial y una supuesta retención de factura</b></p>															
<p>RETENCIÓN 001-002-00006770 FACTURA ELECTRÓNICA POR PAGAR</p> <p>HL Hipolito Lagos &lt;hlagosos@gmail.com&gt; Para CCO</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>Fecha: 16 Mayo, 2023</p> <p>FACTURA ELECTRONICA PENDIENTE DE PAGO</p> <p>Valor: <b>\$ 100.00</b></p> <p>Consulta el comprobante detallado en línea.</p> <p><a href="#">VER DOCUMENTO DE FACTURA</a></p> <p>CLAVE DEL DOCUMENTO : 095</p> 	<table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>2CMV23-00413-01</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>17 de mayo de 2023</td> </tr> <tr> <td>Última revisión</td> <td>17 de mayo de 2023</td> </tr> </table>	Alerta de seguridad cibernética	2CMV23-00413-01	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	17 de mayo de 2023	Última revisión	17 de mayo de 2023	
Alerta de seguridad cibernética	2CMV23-00413-01															
Clase de alerta	Fraude															
Tipo de incidente	Malware															
Nivel de riesgo	Alto															
TLP	Blanco															
Fecha de lanzamiento original	17 de mayo de 2023															
Última revisión	17 de mayo de 2023															
	<p><b>Indicadores de compromiso</b></p>															
	<p><b>URL-Dominio</b></p>															
	<p><a href="https://acortar[.]link/NCMHbI">https://acortar[.]link/NCMHbI</a>  <a href="https://acortar[.]link/zlbaw7">https://acortar[.]link/zlbaw7</a>  <a href="https://lessecuador[.]con-ip.com:2434">lessecuador[.]con-ip.com:2434</a>  <a href="https://178.237.33[.]50">178.237.33[.]50</a>  <a href="https://186.169.64[.]87">186.169.64[.]87</a></p>															
	<p><b>SHA256</b></p>															
	<p>40e7707233efd5935367b041f8dbfdd5237b3efbdde7dec15ce38f1152bd6a16  e803b7421aa3bd70991445974558ef0955cc84e260222e5cac8b28a4ebb7e6b0  9a50e8852c21875b333fa210d814be7f0acc096afab6d06cc438d1ace3f42993  e803b7421aa3bd70991445974558ef0955cc84e260222e5cac8b28a4ebb7e6b0  5e908c1a0f74bc26d9f2dd21bcfb4b3ff077b39d4296763eb251889435790f78ae3  dba8130c56c7373e63b7f1b2cb0d89baa536f418173cf59a4db928d02db6e</p>															
	<p><b>Enlaces para revisar el informe:</b></p>															
	<p><a href="https://www.csirt.gob.cl/alertas/2cmv23-00413-01/">https://www.csirt.gob.cl/alertas/2cmv23-00413-01/</a></p>															

## 4. Vulnerabilidades



**INFORME DE Vulnerabilidad**

**9VSA23-00832-01**  
CSIRT informa de vulnerabilidad crítica en plugin Essential Addons for Elementor de Wordpress

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

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

CSIRT comparte información de una vulnerabilidad crítica que afecta al plugin **Essential Addons for Elementor, de WordPress**

Alerta de seguridad cibernética	9VSA23-00832-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de mayo de 2023
Última revisión	15 de mayo de 2023

**CVE**

CVE-2023-32243

**Fabricantes**

Elementor

**Productos afectados**

Plugin Essential Addons for Elementor de WordPress posteriores a la 5.4.0 y anteriores a la versión 5.7.2, que parcha la vulnerabilidad.

**Enlaces para revisar el informe:**

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00832-01/>



**INFORME DE Vulnerabilidad**

**9VSA23-00833-01**  
CSIRT comparte vulnerabilidades parchadas en actualización a Google Chrome 113

PARA REGISTRAR | 15 10  
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 parchadas en actualización a **Google Chrome 113**

Alerta de seguridad cibernética	9VSA23-00833-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de mayo de 2023
Última revisión	17 de mayo de 2023

**CVE**

CVE-2023-2721	CVE-2023-2723	CVE-2023-2725
CVE-2023-2722	CVE-2023-2724	CVE-2023-2726

**Fabricantes**

Google

**Productos afectados**

Google Chrome

**Enlaces para revisar el informe:**

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00833-01/>





**Informe de Vulnerabilidad**

9VSA23-00834-01  
CSIRT comparte vulnerabilidades informadas por Cisco para varios de sus switches

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

## CSIRT comparte vulnerabilidades informadas por Cisco para varios de sus switches

Alerta de seguridad cibernética	9VSA23-00834-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	18 de mayo de 2023
Última revisión	18 de mayo de 2023

### CVE

CVE-2023-20159	CVE-2023-20189	CVE-2023-20157
CVE-2023-20160	CVE-2023-20024	CVE-2023-20158
CVE-2023-20161	CVE-2023-20156	CVE-2023-20162

### Fabricantes

Cisco

### Productos afectados

250 Series Smart Switches, 350 Series Managed Switches, 350X Series Stackable Managed Switches, and 550X Series Stackable Managed Switches (fixed in firmware version 2.5.9.16).  
Business 250 Series Smart Switches and Business 350 Series Managed Switches (fixed in firmware version 3.3.0.16).  
Small Business 200 Series Smart Switches, Small Business 300 Series Managed Switches, Small Business 500 Series Stackable Managed Switches (no patch available).

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00834-01/>

## 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

### Ciberdiccionario Volumen 37

Con la intención de seguir sumando conceptos a nuestro Ciberdiccionario, esta semana les traemos definiciones de bot, VLAN, VoIP y lo que son las llaves pública y privada en el concepto de la criptografía. Todos los volúmenes del ciberdiccionario, junto al resto de nuestras recomendaciones están en: <http://csirt.gob.cl/recomendaciones>.

 <h3>Ciber diccionario</h3> <p><b>Llave pública y llave privada</b></p> <p>Un mecanismo usado para encriptar información, conocido como criptografía asimétrica o de llave pública, consta de una llave (o clave) pública, utilizada para convertir un texto plano (legible por humanos) en un texto cifrado (o "ciphertext"), y una correspondiente llave privada única que puede descifrar el ciphertext generado por esta llave pública, usada para permitir leer el texto plano original.</p> 	 <h3>Ciber diccionario</h3> <p><b>Bot</b></p> <p>Abreviatura de robot, programa de software o script (secuencia de comandos) que realiza tareas automatizadas, repetidas y predefinidas. Pueden imitar el comportamiento humano, y reemplazarlos en algunas labores. En ciberseguridad, se llaman bots al malware (programas maliciosos) que toma el control remoto de un equipo. Algunos tipos de bots: spiders, crawlers y web bots.</p> 
 <h3>Ciber diccionario</h3> <p><b>VLAN</b></p> <p>En inglés, sigla de Red virtual de área local, refiere a una red virtual o lógica creada sobre una o varias redes físicas de área local (o LAN). Esto permite lograr una mayor seguridad de las comunicaciones entre los equipos que pertenecen a una misma VLAN, al controlar las interacciones que son permitidas. Son claves para las organizaciones que manejan sistemas de redes complejos.</p> 	 <h3>Ciber diccionario</h3> <p><b>VoIP</b></p> <p>Sigla en inglés de "voz sobre el protocolo de internet", es la tecnología que permite la comunicación de voz por esta red, incluyendo llamadas telefónicas. Al trabajar sobre internet, esta tecnología está expuesta a riesgos de ciberseguridad, como el call tampering (inyección de paquetes de ruido por parte de hackers), entorpeciendo la comunicación. El VoIP, además, como toda comunicación por voz, puede ser usado para el phishing (llamado, en este caso, vishing).</p> 

#### 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>





## El CSIRT de Gobierno alerta ante resurgimiento de Remcos, malware difundido a través de archivos de Word

Como CSIRT de Gobierno hemos visto con mayor frecuencia, entre las campañas de phishing que detectamos, el uso del troyano Remcos, un peligroso virus informático que permite a un ciberdelincuente tomar total control del teléfono o computador de la víctima. También vemos que las campañas apuntan principalmente a empresas e instituciones públicas de nuestro país.

En vista de esta situación, y para ampliar el conocimiento de la ciudadanía respecto de las amenazas que enfrentamos en el ciberespacio, compartimos algunas de las características que hacen peligroso a Remcos, y algunas formas en que podemos evitar ser sus víctimas. Están disponibles en el siguiente enlace: <https://www.csirt.gob.cl/noticias/10cnd23-00100-01/>.



## 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>



## Ciberconsejos en el Día Mundial de Internet

El 17 de mayo se celebró el Día Mundial de las Telecomunicaciones y de la Sociedad de la Información, con el objetivo de promover el uso de Internet, dar a conocer la importancia que tienen las TIC en el mundo y disminuir la brecha digital. Para navegar seguros y evitar ser víctima de una estafa o robo de información, entregamos algunos ciberconsejos generales sobre el uso más seguro de internet: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-en-el-dia-mundial-de-internet/>.



**CIBERCONSEJOS**  
**Día Internacional de Internet**

**1. Usa contraseñas robustas y diferentes**

- Una clave segura dificulta que los delincuentes tengan acceso a tus redes sociales, correo, cuentas bancarias, etc.
- Para crear una contraseña robusta: combina letras, números y símbolos.
- En caso de robo, tener claves diferentes ayuda a que los delincuentes no puedan ingresar a todas tus cuentas creadas.

**2. Cuida tus dispositivos (celular, computadores, etc.)**

- Instala un programa de antivirus (software).
- Mantén actualizado el software, sistema operativo, navegadores y aplicaciones de tus dispositivos, así te aseguras de parchar las vulnerabilidades que puedan tener los productos.
- Utiliza doble factor de autenticación (2FA) siempre que sea posible.

**3. Protege tus dispositivos IoT**  
(televisores, parlantes, cámaras de seguridad, etc. que sean inteligentes)


- Implementa medidas de seguridad para evitar el robo de datos personales, perder el control del equipo u otras amenazas.
- Utiliza contraseñas para cada dispositivo que lo permita.
- Oculta el nombre de la red inalámbrica a la que se conectan los dispositivos.
- Configura tu dispositivo en modo privado.

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

## 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.

- Diego Ignacio Concha de la Fuente.
- Sugy Nam.
- Juan Eduardo Báez.
- Marly Robles.
- Rigoberto Cancino.
- Marcelo Esteban Rodríguez Kong.

### 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>