



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 197

semana del 7 al 13 de abril de 2023

# LA SEMANA EN CIFRAS

## IP INFORMADAS

18

IP advertidas en múltiples campañas de phishing y de malware.



## URL ADVERTIDAS

19

URL asociadas a sitios fraudulentos y campañas de phishing y malware



## PARCHES COMPARTIDOS

206

Las mitigaciones son útiles en productos de Apple, Google (Android y Chrome), Microsoft, Sophos, Mozilla y SAP.



## HASH REPORTADOS

9

asociadas a múltiples campañas de phishing con archivos que contienen malware



# CONTENIDO

1.	Sitios fraudulentos .....	3
2.	Phishing .....	5
3.	Ataques de Fuerza Bruta .....	8
4.	Vulnerabilidades .....	9
5.	Malware.....	15
6.	Concientización.....	16
7.	Recomendaciones y buenas prácticas .....	18
8.	Muro de la Fama .....	19

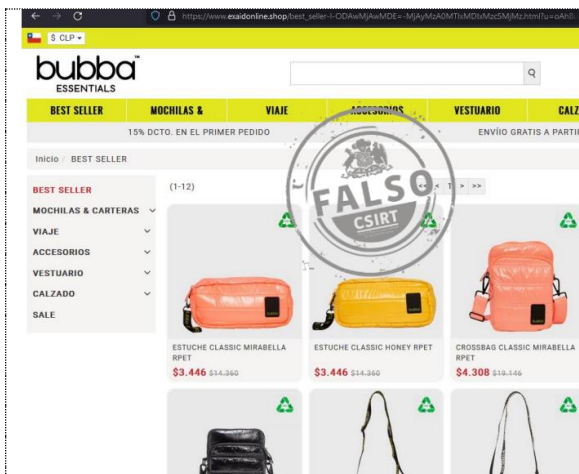
11111<

## 1. Sitios fraudulentos



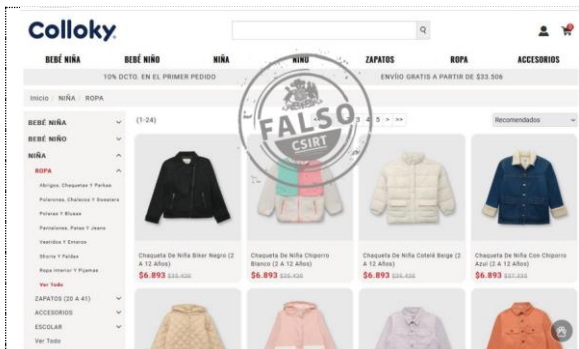
### CSIRT alerta de página fraudulenta que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01275-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de abril de 2023
Última revisión	11 de abril de 2023
<b>Indicadores de compromiso</b>	
URL sitio falso	<a href="https://www.saptofers[.]online/">https://www.saptofers[.]online/</a>
Dirección IP	[162.222.89.177]
Enlace para revisar loC:	<a href="https://www.csirt.gob.cl/alertas/8ffr23-01275-01">https://www.csirt.gob.cl/alertas/8ffr23-01275-01</a>



### CSIRT informa de nueva página fraudulenta que suplanta a Bubba Bags

Alerta de seguridad cibernética	8FFR23-01276-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2023
Última revisión	12 de abril de 2023
<b>Indicadores de compromiso</b>	
URL redirección	<a href="https://salebags.mailchimpsites[.]com/?gclid=CjwKCAjwitShBhA6EiwAq3RqAx_kTV3GfAXmW8rs2xeVhBV0keCWNlZiz59-q5Ks_k80k3a6VgtxRRoCNasQAvD_BwE">https://salebags.mailchimpsites[.]com/?gclid=CjwKCAjwitShBhA6EiwAq3RqAx_kTV3GfAXmW8rs2xeVhBV0keCWNlZiz59-q5Ks_k80k3a6VgtxRRoCNasQAvD_BwE</a>
URL sitio falso	<a href="https://www.exaidonline[.]shop/?u=oAhBi2q3bYU=">https://www.exaidonline[.]shop/?u=oAhBi2q3bYU=</a>
Dirección IP	[162.218.176.59]
Enlace para revisar loC:	<a href="https://www.csirt.gob.cl/alertas/8ffr23-01276-01">https://www.csirt.gob.cl/alertas/8ffr23-01276-01</a>

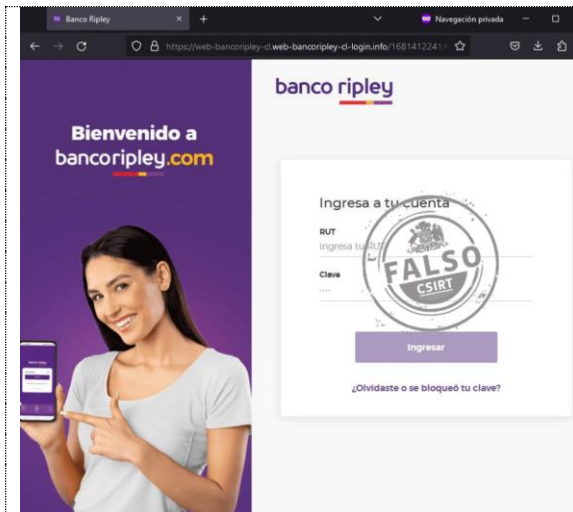


### CSIRT alerta de sitio fraudulento que suplanta a Colloky

Alerta de seguridad cibernética	8FFR23-01277-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2023
Última revisión	12 de abril de 2023
<b>Indicadores de compromiso</b>	
URL sitio falso	<a href="https://www.vetemcam[.]online">https://www.vetemcam[.]online</a>
Dirección IP	[167.160.3.13]
Enlace para revisar loC:	<a href="https://www.csirt.gob.cl/alertas/8ffr23-01277-01">https://www.csirt.gob.cl/alertas/8ffr23-01277-01</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 nueva página fraudulenta que suplanta a Banco Ripley

Alerta de seguridad cibernética	8FFR23-01278-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de abril de 2023
Última revisión	13 de abril de 2023

### Indicadores de compromiso

#### URL sitio falso

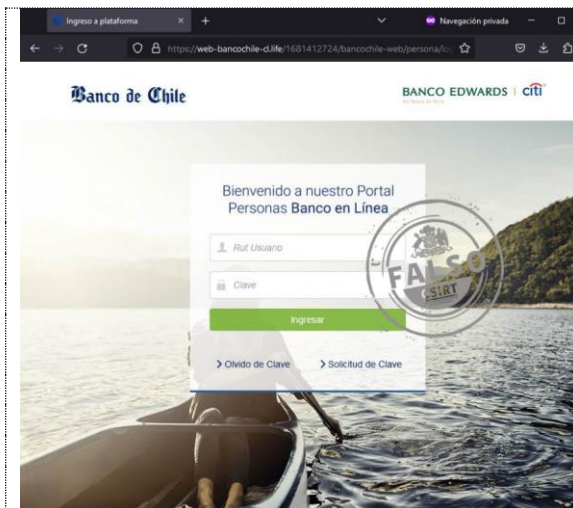
<https://web-bancoripley-cl.web-bancoripley-cl-login.info/1681412241/login/index.html>

#### Dirección IP

[172.67.133.184]

#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8ffr23-01278-01>



## CSIRT alerta de sitio fraudulento que suplanta al Banco de Chile

Alerta de seguridad cibernética	8FFR23-01279-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de abril de 2023
Última revisión	13 de abril de 2023

### Indicadores de compromiso

#### URL sitio falso

<https://web-bancochile-cl.life/1681412724/bancochile-web/persona/login/index.html/login>

#### Dirección IP

[104.21.46.118]

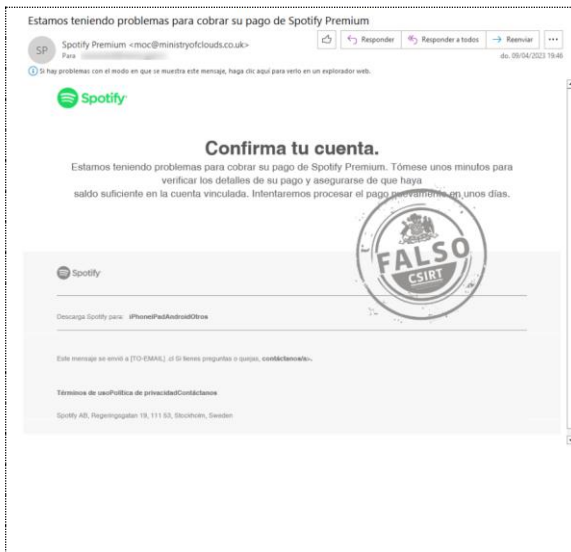
#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8ffr23-01279-01>

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

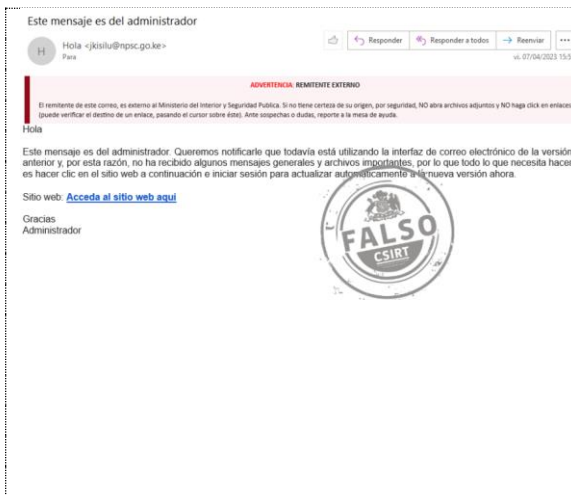
<https://www.csirt.gob.cl>  
Teléfonos: 1510 | + (562) 24863850 | Correo: [soc@interior.gob.cl](mailto:soc@interior.gob.cl)  
[@csirtgob](https://twitter.com/csirtgob)  
<https://www.linkedin.com/company/csirt-gob>

## 2. Phishing



### CSIRT alerta de campaña de phishing que suplanta a Spotify

Alerta de seguridad cibernética	8FPH23-00780-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de abril de 2023
Última revisión	10 de abril de 2023
<b>URL sitio falso</b>	<a href="https://www.carlsencanvas.com/clpremiumes_brand_contextualspotify/cl_premiumfactura1/?viem=login&amp;appIdKey=fcd00c0656cc490&amp;country=">https://www.carlsencanvas.com/clpremiumes_brand_contextualspotify/cl_premiumfactura1/?viem=login&amp;appIdKey=fcd00c0656cc490&amp;country=</a>
<b>URL redirección</b>	<a href="https://letrazoom.com/yjwcsHR">https://letrazoom.com/yjwcsHR</a>
<b>Dirección IP</b>	[13.249.85.88]
<b>Enlace para revisar loC:</b>	<a href="https://www.csirt.gob.cl/alertas/8fph23-00780-01/">https://www.csirt.gob.cl/alertas/8fph23-00780-01/</a>

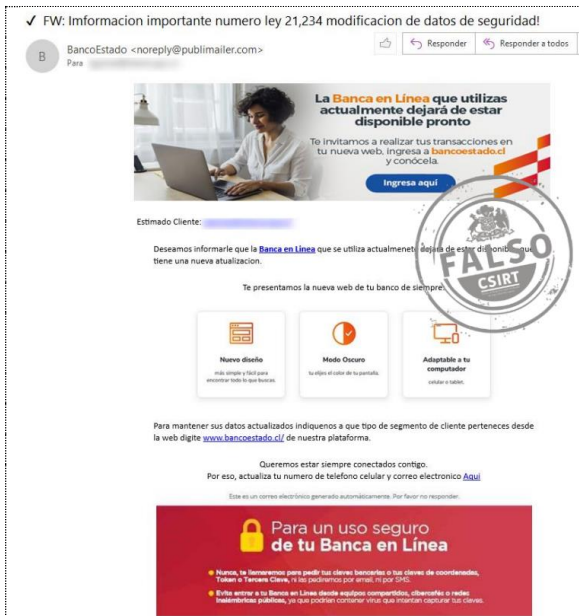


### CSIRT alerta de campaña de phishing que suplanta a Zimbra

Alerta de seguridad cibernética	8FPH23-00781-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de abril de 2023
Última revisión	10 de abril de 2023
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	<a href="https://firebasestorage.googleapis.com/v0/b/oiuuytrteertyu.appspot.com/o/index.html?alt=media&amp;token=87c0b2ef-b50a-467b-9bd6-021d581f8a3b">https://firebasestorage.googleapis.com/v0/b/oiuuytrteertyu.appspot.com/o/index.html?alt=media&amp;token=87c0b2ef-b50a-467b-9bd6-021d581f8a3b</a>
<b>Dirección IP</b>	[74.125.132.95]
<b>Enlace para revisar loC:</b>	<a href="https://www.csirt.gob.cl/alertas/8fph23-00781-01/">https://www.csirt.gob.cl/alertas/8fph23-00781-01/</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 advierte de nueva campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH23-00782-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de abril de 2023
Última revisión	10 de abril de 2023

### Indicadores de compromiso

#### URL sitio falso

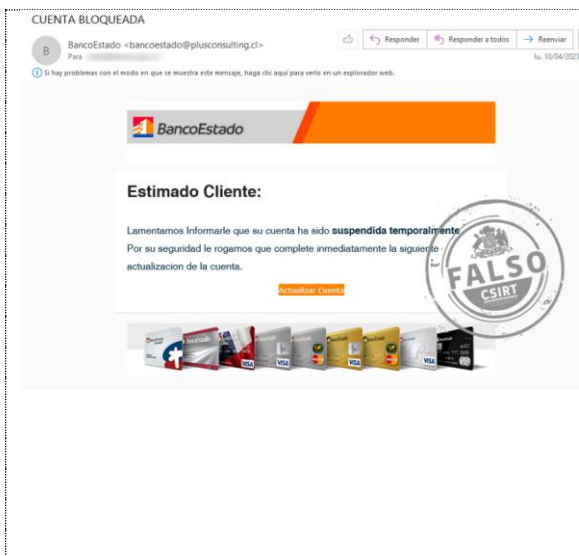
<https://firebasestorage.googleapis.com/v0/b/oiuuytrteertyu.appspot.com/o/index.html?alt=media&token=87c0b2ef-b50a-467b-9bd6-021d581f8a3b>

#### Dirección IP

[74.125.132.95]

#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00782-01/>



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

Alerta de seguridad cibernética	8FPH23-00783-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de abril de 2023
Última revisión	10 de abril de 2023

### Indicadores de compromiso

#### URL redirección

[https://clubmenthalist\[.\]com/promocion/cuenta-ooqn/](https://clubmenthalist[.]com/promocion/cuenta-ooqn/)

#### URL sitio falso



[https://nwmmayorsa\[.\]com/1681160466/imagenes/\\_personas/home/default.asp](https://nwmmayorsa[.]com/1681160466/imagenes/_personas/home/default.asp)


#### Dirección IP

[67.23.242.202]

#### Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00783-01/>

<p>Friday, April 7, 2023:Reminder Message</p> <p>Support Notification Noreply@delfinoriente.cl &lt;francis@allfreightl.com&gt; Para</p> <p>Mensaje enviado con importancia Alta.</p> <p>body</p> <p></p> <p>Hello,</p> <p>Password for your email account will be expiring today. To keep using same Password, verify request below</p> <p><a href="#">KEEP SAME PASSWORD</a></p> <p>SUPPORT NOTIFICATION</p> <p>©2023 MICROSOFT EXCHANGE</p> 	<p><b>CSIRT alerta de campaña de phishing que suplanta a Microsoft Outlook</b></p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00784-01</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>13 de abril de 2023</td> </tr> <tr> <td>Última revisión</td> <td>13 de abril de 2023</td> </tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b></p> <p><a href="https://m.exactag[.]com/cl.aspx?extProvApi=b2c&amp;extProvID=99&amp;extPu=ew-email&amp;extLi=promo_14-2023_de-DE_sixt&amp;url=https%3A%2F%2Fsimiaestudio.com/%2Fwp-admin%2Fcss%2F/qtckxc%2F%2F%2F%2FY2hnb256YWxlekBkZWxmaW5vcmlbnRlLmNs">https://m.exactag[.]com/cl.aspx?extProvApi=b2c&amp;extProvID=99&amp;extPu=ew-email&amp;extLi=promo_14-2023_de-DE_sixt&amp;url=https%3A%2F%2Fsimiaestudio.com/%2Fwp-admin%2Fcss%2F/qtckxc%2F%2F%2F%2FY2hnb256YWxlekBkZWxmaW5vcmlbnRlLmNs</a></p> <p><a href="https://simiaestudio[.]com//wp-admin/css//qtckxc///Y2hnb256YWxlekBkZWxmaW5vcmlbnRlLmNs?et_uk=c7849600a47042aab8be962e224c10f3">https://simiaestudio[.]com//wp-admin/css//qtckxc///Y2hnb256YWxlekBkZWxmaW5vcmlbnRlLmNs?et_uk=c7849600a47042aab8be962e224c10f3</a></p> <p><b>URL sitio falso</b></p> <p><a href="https://xiq5hxl3l6410c7eae98a6.ainnr.ru/ID-6436bbfce4245">https://xiq5hxl3l6410c7eae98a6.ainnr.ru/ID-6436bbfce4245</a></p> <p><b>Dirección IP</b></p> <p>[172.67.138.107]</p> <p><b>Enlace para revisar loC:</b></p> <p><a href="https://www.csirt.gob.cl/alertas/8fph23-00784-01/">https://www.csirt.gob.cl/alertas/8fph23-00784-01/</a></p>	Alerta de seguridad cibernética	8FPH23-00784-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	13 de abril de 2023	Última revisión	13 de abril de 2023
Alerta de seguridad cibernética	8FPH23-00784-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	13 de abril de 2023														
Última revisión	13 de abril de 2023														

<p>Fwd:ApA°rate! 0Y,tienes hasta 40% dcto en la tasa de tu AVANCE</p> <p>BancoRipley 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><b>CSIRT alerta de campaña de phishing que suplanta a Banco Ripley</b></p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00785-01</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>13 de abril de 2023</td> </tr> <tr> <td>Última revisión</td> <td>13 de abril de 2023</td> </tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b></p> <p><a href="https://bit[.]ly/3KWZi4k?l=www.bancoripley.cl">https://bit[.]ly/3KWZi4k?l=www.bancoripley.cl</a></p> <p><b>URL sitio falso</b></p> <p><a href="https://web.bancoripley.cl.berleymate.co[.]nz/1681404303/login">https://web.bancoripley.cl.berleymate.co[.]nz/1681404303/login</a></p> <p><b>Dirección IP</b></p> <p>[185.184.154.1]</p> <p><b>Enlace para revisar loC:</b></p> <p><a href="https://www.csirt.gob.cl/alertas/8fph23-00785-01/">https://www.csirt.gob.cl/alertas/8fph23-00785-01/</a></p>	Alerta de seguridad cibernética	8FPH23-00785-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	13 de abril de 2023	Última revisión	13 de abril de 2023
Alerta de seguridad cibernética	8FPH23-00785-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	13 de abril de 2023														
Última revisión	13 de abril de 2023														



## 3. Ataques de Fuerza Bruta

 <p>Ministerio del Interior y Seguridad Pública</p> <p><b>ALERTA DE Fuerza Bruta</b></p> <p><b>4IIA23-00066-01</b> <b>CSIRT alerta de ataques de fuerza bruta contra SMTP</b></p> <p>PARA REGISTRAR   562 2486 3850 UN INCIDENTE   <a href="http://www.csirt.gob.cl">www.csirt.gob.cl</a></p> <p><b>CSIRT</b> Equipo de Respuesta ante Incidentes de Seguridad Informática</p>	<b>CSIRT alerta de ataques de fuerza bruta contra SMTP</b>	
	Alerta de seguridad cibernética	4IIA22-00066-01
	Clase de alerta	Intentos de Intrusión
	Tipo de incidente	Intentos de acceso – Fuerza bruta
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	13 de abril de 2023
	Última revisión	13 de abril de 2023
	<b>Indicadores de compromiso</b>	
	<b>Direcciones IP</b>	
185.225.73.83		
141.98.10.60		
194.87.84.62		
176.111.173.56		
193.56.29.192		
212.87.204.201		
<b>Enlaces para revisar el informe:</b>		
<a href="https://www.csirt.gob.cl/alertas/4iia22-00066-01/">https://www.csirt.gob.cl/alertas/4iia22-00066-01/</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>

## 4. Vulnerabilidades



**INFORME DE Vulnerabilidad**

**9VSA23-00811-01**  
CSIRT comparte vulnerabilidades parchadas por Apple en iOS 16.4.1 y en iPadOS 16.4.1

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 parchadas por Apple en iOS 16.4.1 y en iPadOS 16.4.1

Alerta de seguridad cibernética	9VSA23-00811-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de abril de 2023
Última revisión	10 de abril de 2023

#### CVE

CVE-2023-28206  
CVE-2023-28205

#### Fabricantes

Apple

#### Productos afectados

iPhone 8 y posterior, iPad Pro (todos), iPad Air 3ra generación y posteriores, iPad 5ta generación y posteriores, iPad mini 5ta generación y posteriores.

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00811-01/>



**INFORME DE Vulnerabilidad**

**9VSA23-00812-01**  
CSIRT comparte vulnerabilidades parchadas en Google Chrome 112

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 parchadas en Google Chrome 112

Alerta de seguridad cibernética	9VSA23-00812-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de abril de 2023
Última revisión	10 de abril de 2023

#### CVE

CVE-2023-1810	CVE-2023-1815	CVE-2023-1820
CVE-2023-1811	CVE-2023-1816	CVE-2023-1821
CVE-2023-1812	CVE-2023-1817	CVE-2023-1822
CVE-2023-1813	CVE-2023-1818	CVE-2023-1823
CVE-2023-1814	CVE-2023-1819	

#### Fabricantes

Google

#### Productos afectados

Google Chrome.

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00812-01/>

## 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>



## CSIRT comparte vulnerabilidades parchadas en la actualización de seguridad de Android de abril 2023

Alerta de seguridad cibernética	9VSA23-00813-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de abril de 2023
Última revisión	10 de abril de 2023

### CVE

CVE-2021-0872	CVE-2022-33917	CVE-2023-20967
CVE-2021-0873	CVE-2022-36449	CVE-2023-21080
CVE-2021-0874	CVE-2022-38181	CVE-2023-21081
CVE-2021-0875	CVE-2022-40503	CVE-2023-21082
CVE-2021-0876	CVE-2022-40532	CVE-2023-21083
CVE-2021-0878	CVE-2022-41757	CVE-2023-21084
CVE-2021-0879	CVE-2022-42716	CVE-2023-21085
CVE-2021-0880	CVE-2022-4696	CVE-2023-21086
CVE-2021-0881	CVE-2022-47335	CVE-2023-21087
CVE-2021-0882	CVE-2022-47336	CVE-2023-21088
CVE-2021-0883	CVE-2022-47337	CVE-2023-21089
CVE-2021-0884	CVE-2022-47338	CVE-2023-21090
CVE-2021-0885	CVE-2023-20652	CVE-2023-21091
CVE-2022-20463	CVE-2023-20653	CVE-2023-21092
CVE-2022-20471	CVE-2023-20654	CVE-2023-21093
CVE-2022-32599	CVE-2023-20655	CVE-2023-21094
CVE-2022-33231	CVE-2023-20656	CVE-2023-21096
CVE-2022-33269	CVE-2023-20657	CVE-2023-21097
CVE-2022-33270	CVE-2023-20909	CVE-2023-21098
CVE-2022-33288	CVE-2023-20935	CVE-2023-21099
CVE-2022-33289	CVE-2023-20941	CVE-2023-21100
CVE-2022-33302	CVE-2023-20950	CVE-2023-21630

### Fabricantes

Google

### Productos afectados

Productos que usan el sistema Operativo Android.

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00813-01/>



**INFORME DE Vulnerabilidad**

**9VSA23-00814-01**  
CSIRT comparte vulnerabilidades parchadas en Update Tuesday de Microsoft Abril 2023

**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 las vulnerabilidades parchadas por Microsoft en su Update Tuesday de Abril

Alerta de seguridad cibernética	9VSA23-00814-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de abril de 2023
Última revisión	11 de abril de 2023

### CVE

CVE-2023-21729	CVE-2023-28254	CVE-2023-28229
CVE-2023-28304	CVE-2023-28275	CVE-2023-28227
CVE-2023-23375	CVE-2023-28276	CVE-2023-28224
CVE-2023-28300	CVE-2023-28252	CVE-2023-28226
CVE-2023-28292	CVE-2023-28274	CVE-2023-28225
CVE-2023-28291	CVE-2023-28277	CVE-2023-28223
CVE-2023-28313	CVE-2023-28250	CVE-2023-28222
CVE-2023-28312	CVE-2023-28273	CVE-2023-28221
CVE-2023-28287	CVE-2023-28249	CVE-2023-28220
CVE-2023-24893	CVE-2023-28272	CVE-2023-28219
CVE-2023-28314	CVE-2023-28271	CVE-2023-28218
CVE-2023-28299	CVE-2023-28247	CVE-2023-28217
CVE-2023-28296	CVE-2023-28248	CVE-2023-28216
CVE-2023-28263	CVE-2023-28269	CVE-2023-24931
CVE-2023-28262	CVE-2023-28270	CVE-2023-24929
CVE-2023-28260	CVE-2023-28246	CVE-2023-24887
CVE-2023-28311	CVE-2023-28268	CVE-2023-24928
CVE-2023-28309	CVE-2023-28244	CVE-2023-24886
CVE-2023-28308	CVE-2023-28266	CVE-2023-24927
CVE-2023-28307	CVE-2023-28267	CVE-2023-24885
CVE-2023-28306	CVE-2023-28243	CVE-2023-24926
CVE-2023-28305	CVE-2023-28241	CVE-2023-24884
CVE-2023-28295	CVE-2023-28240	CVE-2023-24925
CVE-2023-28302	CVE-2023-28236	CVE-2023-24883
CVE-2023-28298	CVE-2023-28238	CVE-2023-24924
CVE-2023-28297	CVE-2023-28237	CVE-2023-24914
CVE-2023-28293	CVE-2023-28232	CVE-2023-24912
CVE-2023-28288	CVE-2023-28235	CVE-2023-24860
CVE-2023-28285	CVE-2023-28231	CVE-2023-23384
CVE-2023-28256	CVE-2023-28234	CVE-2023-21769
CVE-2023-28278	CVE-2023-28233	CVE-2023-21727
CVE-2023-28255	CVE-2023-28228	CVE-2023-21554
CVE-2023-28253		

### Fabricante

Microsoft

### Productos afectados

.NET 6.0  
.NET 7.0  
Azure Machine Learning  
Azure Service Connector  
Microsoft 365 Apps for Enterprise for 32-bit Systems  
Microsoft 365 Apps for Enterprise for 64-bit Systems  
Microsoft Dynamics 365 (on-premises) version 9.0  
Microsoft Dynamics 365 (on-premises) version 9.1  
Microsoft Malware Protection Engine

## 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>

Microsoft ODBC Driver 17 for SQL Server  
Microsoft ODBC Driver 18 for SQL Server  
Microsoft Office 2019 for 32-bit editions  
Microsoft Office 2019 for 64-bit editions  
Microsoft Office 2019 for Mac  
Microsoft Office LTSC 2021 for 32-bit editions  
Microsoft Office LTSC 2021 for 64-bit editions  
Microsoft Office LTSC for Mac 2021  
Microsoft OLE DB Driver 18 for SQL Server  
Microsoft OLE DB Driver 19 for SQL Server  
Microsoft Publisher 2013 Service Pack 1 (32-bit editions)  
Microsoft Publisher 2013 Service Pack 1 (64-bit editions)  
Microsoft Publisher 2013 Service Pack 1 RT  
Microsoft Publisher 2016 (32-bit edition)  
Microsoft Publisher 2016 (64-bit edition)  
Microsoft SharePoint Enterprise Server 2013 Service Pack 1  
Microsoft SharePoint Enterprise Server 2016  
Microsoft SharePoint Foundation 2013 Service Pack 1  
Microsoft SharePoint Server 2019  
Microsoft SharePoint Server Subscription Edition  
Microsoft SQL Server 2008 for 32-bit Systems Service Pack 4 (QFE)  
Microsoft SQL Server 2008 for x64-Based Systems Service Pack 4 (QFE)  
Microsoft SQL Server 2008 R2 for 32-Bit Systems Service Pack 3 (QFE)  
Microsoft SQL Server 2008 R2 for x64-Based Systems Service Pack 3 (QFE)  
Microsoft SQL Server 2012 for 32-bit Systems Service Pack 4 (QFE)  
Microsoft SQL Server 2012 for x64-based Systems Service Pack 4 (QFE)  
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4)  
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)  
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4)  
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)  
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)  
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure  
Connectivity Pack  
Microsoft SQL Server 2017 for x64-based Systems (CU 31)  
Microsoft SQL Server 2017 for x64-based Systems (GDR)  
Microsoft SQL Server 2019 for x64-based Systems (CU 18)  
Microsoft SQL Server 2019 for x64-based Systems (GDR)  
Microsoft SQL Server 2022 for x64-based Systems (GDR)  
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 – 15.8)  
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)  
Microsoft Visual Studio 2022 version 17.0  
Microsoft Visual Studio 2022 version 17.2  
Microsoft Visual Studio 2022 version 17.4  
Microsoft Visual Studio 2022 version 17.5  
Raw Image Extension  
Remote Desktop client for Windows Desktop  
Send Customer Voice survey from Dynamics 365  
Visual Studio Code  
Windows 10 for 32-bit Systems  
Windows 10 for x64-based Systems  
Windows 10 Version 1607 for 32-bit Systems  
Windows 10 Version 1607 for x64-based Systems  
Windows 10 Version 1809 for 32-bit Systems  
Windows 10 Version 1809 for ARM64-based Systems  
Windows 10 Version 1809 for x64-based Systems

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

Windows 10 Version 20H2 for 32-bit Systems  
 Windows 10 Version 20H2 for ARM64-based Systems  
 Windows 10 Version 20H2 for x64-based Systems  
 Windows 10 Version 21H2 for 32-bit Systems  
 Windows 10 Version 21H2 for ARM64-based Systems  
 Windows 10 Version 21H2 for x64-based Systems  
 Windows 10 Version 22H2 for 32-bit Systems  
 Windows 10 Version 22H2 for ARM64-based Systems  
 Windows 10 Version 22H2 for x64-based Systems  
 Windows 11 version 21H2 for ARM64-based Systems  
 Windows 11 version 21H2 for x64-based Systems  
 Windows 11 Version 22H2 for ARM64-based Systems  
 Windows 11 Version 22H2 for x64-based Systems  
 Windows Server 2008 for 32-bit Systems Service Pack 2  
 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)  
 Windows Server 2008 for x64-based Systems Service Pack 2  
 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)  
 Windows Server 2008 R2 for x64-based Systems Service Pack 1  
 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)  
 Windows Server 2012  
 Windows Server 2012 (Server Core installation)  
 Windows Server 2012 R2  
 Windows Server 2012 R2 (Server Core installation)  
 Windows Server 2016  
 Windows Server 2016 (Server Core installation)  
 Windows Server 2019  
 Windows Server 2019 (Server Core installation)  
 Windows Server 2022  
 Windows Server 2022 (Server Core installation)

**Enlaces para revisar el informe:**

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00814-01/>



Ministerio del Interior y Seguridad Pública

**INFORME DE Vulnerabilidad**

**9VSA23-00815-01**  
 CSIRT comparte vulnerabilidades parchadas en Sophos Web Appliance 4.3.10.4

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 vulnerabilidades parchadas en Sophos Web Alliance versión 4.3.10.4**

Alerta de seguridad cibernética	9VSA23-00815-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2023
Última revisión	12 de abril de 2023

**CVE**

CVE-2023-1671  
 CVE-2022-4934  
 CVE-2020-36692

**Fabricante**

Sophos

**Productos afectados**

Sophos Web Alliance, versiones anteriores a la 4.3.10.4.

**Enlaces para revisar el informe:**

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00815-01/>

**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://www.linkedin.com/company/csirt-gob>



**INFORME DE Vulnerabilidad**

**9VSA23-00816-01**  
CSIRT comparte vulnerabilidades parchadas en Mozilla Firefox 112, Firefox ESR 102.10

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 vulnerabilidades parchadas en Mozilla Firefox 112, Firefox ESR 102.10

Alerta de seguridad cibernética	9VSA23-00816-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2023
Última revisión	12 de abril de 2023

### CVE

CVE-2023-29531	CVE-2023-29538	CVE-2023-29545
CVE-2023-29532	CVE-2023-29539	CVE-2023-29546
CVE-2023-29533	CVE-2023-29540	CVE-2023-29547
CVE-2023-29534	CVE-2023-29541	CVE-2023-29548
CVE-2023-29535	CVE-2023-29542	CVE-2023-29549
CVE-2023-29536	CVE-2023-29543	CVE-2023-29550
CVE-2023-29537	CVE-2023-29544	CVE-2023-29551

### Fabricante

Mozilla

### Productos afectados

Versiones anteriores a Firefox 112, Firefox for Android 112 y Focus for Android 112, y Firefox ESR anterior a Firefox ESR 102.10.

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00816-01/>



**INFORME DE Vulnerabilidad**

**9VSA23-00817-01**  
CSIRT comparte vulnerabilidades parchadas en SAP Diagnostics Agent y BusinessObjects

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 vulnerabilidades parchadas en productos SAP

Alerta de seguridad cibernética	9VSA23-00817-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2023
Última revisión	12 de abril de 2023

### CVE

CVE-2023-27267
CVE-2023-28765
CVE-2023-29186

### Fabricante

SAP

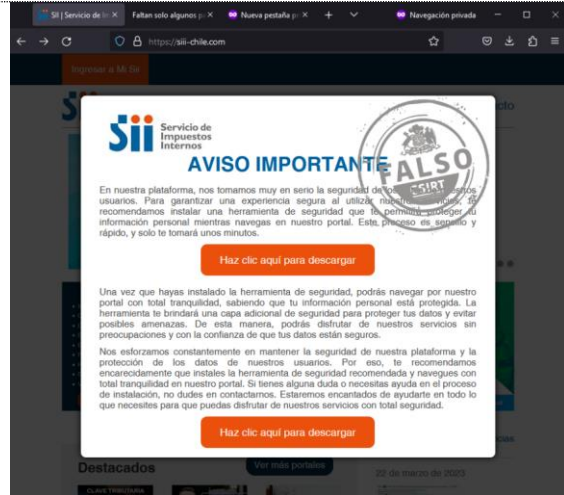
### Productos afectados

SAP Diagnostics Agent y SAP BusinessObjects Business Intelligence Platform

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00817-01/>


## 5. Malware



### CSIRT alerta de una nueva campaña de phishing con malware, que suplanta al SII

Alerta de seguridad cibernética	2CMV23-00408-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de abril de 2023
Última revisión	13 de abril de 2023
<b>Indicadores de compromiso</b>	
<b>URL-Dominio</b>	
<a href="https://siii-chile.com/">https://siii-chile.com/</a> <a href="https://www.grafoce.com/scripts/index.php?id=2">https://www.grafoce.com/scripts/index.php?id=2</a> <a href="file:\\139.162.73.58@80\YtmpEoBw\Herramienta_de_Seguridad_SII.jse">file:\\139.162.73.58@80\YtmpEoBw\Herramienta_de_Seguridad_SII.jse</a> <a href="https://www.grafoce.com/wp-content/execution.php?tag=russian">https://www.grafoce.com/wp-content/execution.php?tag=russian</a>	
<b>SHA256</b>	
e1d2e20285cf909e7075665104948b6ca5c47b356cde4babe06ef91637e743b3 209e96742311be142f2ad42f63250aab879a4518978e4d7d74c6859730595ec039 5b6bf1b3a8155aaaca12672272c976a29854d12bdeac948e8d6d0059e81cd2	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/2cmv23-00408-01/">https://www.csirt.gob.cl/alertas/2cmv23-00408-01/</a> <a href="https://www.csirt.gob.cl/media/2023/04/2CMV23-00408-01.pdf">https://www.csirt.gob.cl/media/2023/04/2CMV23-00408-01.pdf</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://www.linkedin.com/company/csirt-gob>



## 6. Concientización

### Ciberconsejos para no caer en el smishing

Como smishing se conoce a una forma de estafa virtual, que tal como el phishing, busca convencernos de entregar nuestros datos personales o hacer clic en enlaces maliciosos, para descargar programas perjudiciales o permitir a delincuentes tomar control de nuestras cuentas en redes sociales o bancarias. Es importante que estemos al tanto de este tipo de estafa para así evitar caer en ella. Por eso los publicamos esta semana en nuestra web de Recomendaciones: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-no-caer-en-el-smishing/>



The infographic is a 2x2 grid of dark blue panels with white and red text. Each panel features the CSIRT logo at the top right. The top-left panel has the title 'CIBERCONSEJOS PARA EVITAR EL SMISHING' and a white arrow pointing left towards the top-right panel. The top-right panel is titled 'EL SMISHING ES' and defines it as a type of scam using SMS or WhatsApp. The bottom-left panel is titled 'CARACTERÍSTICAS DEL SMISHING' and lists five points. The bottom-right panel is titled 'RECOMENDACIONES' and lists three key advice points. A red circle and line connect the bottom-left and bottom-right panels.

**CIBERCONSEJOS PARA EVITAR EL SMISHING**

**EL SMISHING ES**

Un tipo de estafa, como el phishing, pero a través de SMS o WhatsApp en la que los delincuentes se hacen pasar por personas o entidades legítimas, con el objetivo de robar dinero u obtener información confidencial de las personas.

**CARACTERÍSTICAS DEL SMISHING**


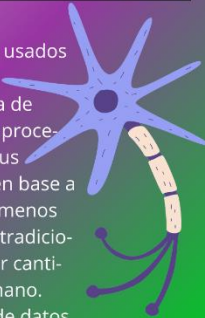






- 1 Generalmente, son mensajes no solicitados.
- 2 Se solicita información financiera, un código de verificación u otro dato personal.
- 3 Los mensajes son alarmantes y presionan para actuar.
- 4 Son mensajes con ofertas o regalos demasiado buenos para ser ciertos.
- 5 Incluyen enlaces o números de teléfono sospechosos.

**RECOMENDACIONES**





- DESCONFÍA de los SMS que provienen de fuentes desconocidas.
- NO hagas clic en enlaces sospechosos.
- REVISÁ el contenido, que no sea alarmante o tenga faltas de ortografía.
- NUNCA entregues información confidencial.
- SI DUDAS, habla directamente con la empresa o entidad aludida.

## Ciberdiccionario Volumen 32

Redes neuronales, minería de datos, tabletop exercise y brecha de datos son los nuevos términos que sumamos a nuestro Ciberdiccionario en su edición 32, disponible también en el siguiente enlace: <https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-32/>.

 <h3>Ciberdiccionario</h3> <h4>Redes neuronales</h4> <p>Modelos de <i>machine learning</i> usados para analizar procesos complejos, inspirados en la forma de funcionar del cerebro. Así, el procesamiento está distribuido y sus partes ganan conocimiento en base a mecanismos de aprendizaje menos restrictivos que los métodos tradicionales, que definen una mayor cantidad de parámetros de antemano. Son utilizados en la minería de datos.</p> 	 <h3>Ciberdiccionario</h3> <h4>Brecha de datos</h4> <p>Salida no autorizada de información sensible desde una organización, también conocida como exfiltración o fuga de datos. Acciones necesarias para que exista una brecha de datos, como el ingreso no autorizado a un sistema, y su interceptación, están penadas en Chile por la Ley sobre Delitos Informáticos, aprobada en 2022.</p> 
 <h3>Ciberdiccionario</h3> <h4>Tabletop exercise</h4> <p>Ejercicio en el cual los distintos roles que componen el equipo de ciberseguridad de una organización discuten y deciden en conjunto cursos de acción para enfrentar un incidente hipotético que se les presenta. La actividad se realiza en un ambiente más relajado e informal que en una simulación de ciberataque propiamente tal.</p> 	 <h3>Ciberdiccionario</h3> <h4>Minería de datos</h4> <p>En inglés <i>data mining</i>, se define como el análisis de enormes cantidades de datos (denominados también <i>big data</i>) para crear nueva información valiosa, incluyendo patrones de relación entre los datos. Es algo que resultaba mucho más difícil, o incluso imposible de realizar antes de la existencia de la necesaria capacidad de almacenamiento y procesamiento de datos.</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>

## 7. 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>


## 8. 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.

- Rodrigo Alex López Pineda
- César Alberto Camacho Sánchez
- Gabriel Matias Yuseff Campusano
- Christopher Pérez
- Miguel Saldias Cossio
- Patricio Rosas Barriga
- María José Farfán Márquez
- Claudia Fernández Carvajal
- María Gabriela Fernández
- Agustín Covarrubias Izquierdo

### 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>