



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 199

semana del 21 al 27 de abril de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

13

IP advertidas en múltiples campañas de phishing y de malware.



URL ADVERTIDAS

24

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

8

Las mitigaciones son útiles en productos de SolarWinds y VMware.



HASH REPORTADOS

4

asociadas a múltiples campañas de phishing con archivos que contienen malware



CONTENIDO

1.	Sitios fraudulentos	3
2.	Phishing	7
3.	Vulnerabilidades	10
4.	Malware.....	11
5.	Concientización.....	12
6.	Recomendaciones y buenas prácticas	16
7.	Muro de la Fama	17

11111<

1. Sitios fraudulentos



CSIRT alerta de página fraudulenta que suplanta a Colloky

Alerta de seguridad cibernética	8FFR23-01293-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2023
Última revisión	21 de abril de 2023

Indicadores de compromiso

URL sitio falso

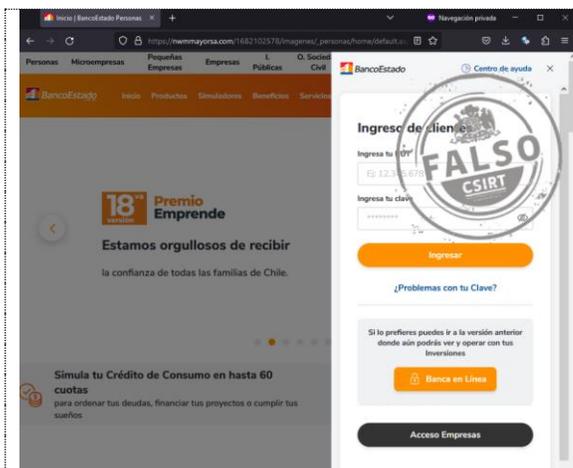
<https://clothingfactorys.weebly.com/>
<https://www.vetemcam.online/>

Dirección IP

[167.160.3.13]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01293-01>



CSIRT alerta de sitio fraudulento que suplanta a BancoEstado

Alerta de seguridad cibernética	8FFR23-01294-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023

Indicadores de compromiso

URL sitio falso

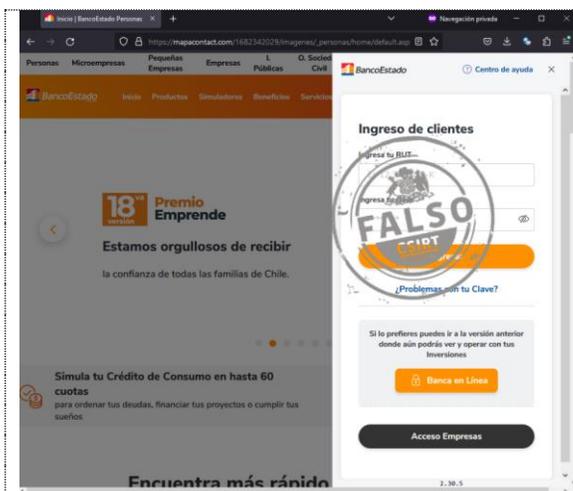
https://www.nwmmayorsa.com/1682102578/imagenes/_personas/home/default.asp

Dirección IP

[67.23.242.202]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01294-01>



CSIRT alerta de página fraudulenta que suplanta a BancoEstado

Alerta de seguridad cibernética	8FFR23-01295-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023

Indicadores de compromiso

URL sitio falso

[https://mapacontact\[.\]com/1682342029/imagenes/_personas/home/default.asp](https://mapacontact[.]com/1682342029/imagenes/_personas/home/default.asp)

Dirección IP

[72.29.91.210]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01295-01>

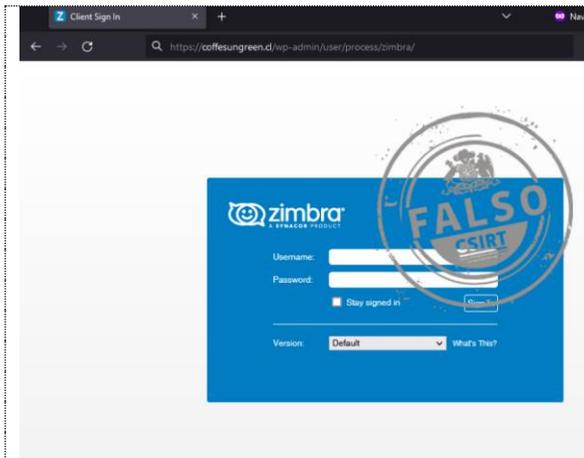
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

Boletín de Seguridad Cibernética N° 199

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

BOLETÍN 13BCS23-00208-01 | Semana del 21 al 27 de abril de 2023



CSIRT alerta de nueva página fraudulenta que suplanta a Zimbra

Alerta de seguridad cibernética	8FFR23-01296-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023

Indicadores de compromiso

URL sitio falso

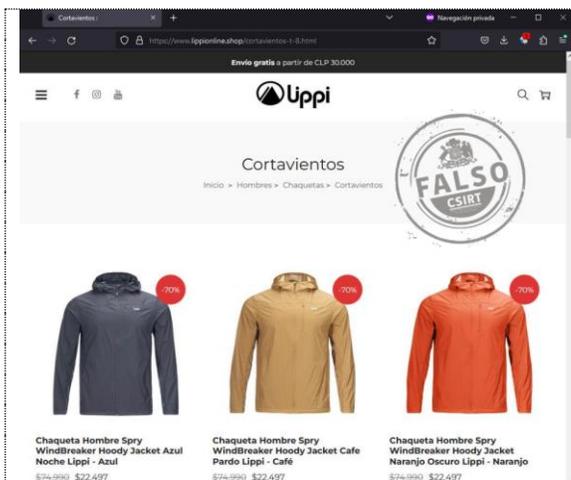
[https\[:\]//coffesungreen\[.\]cl/wp-admin/user/process/zimbra/](https[:]//coffesungreen[.]cl/wp-admin/user/process/zimbra/)

Dirección IP

[190.196.214.221]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01296-01>



CSIRT alerta ante nueva página fraudulenta que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01297-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023

Indicadores de compromiso

URL sitio falso

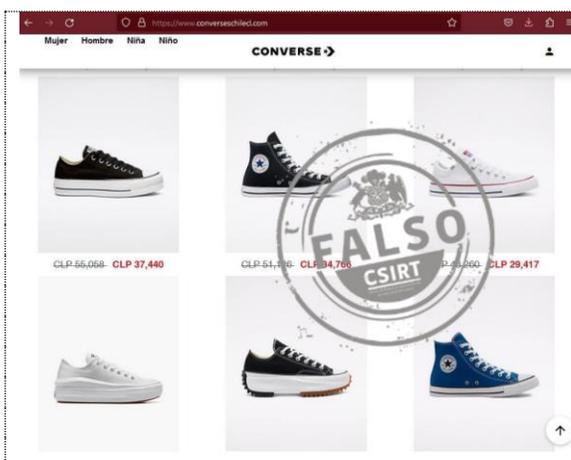
[https\[:\]//www.lippionline\[.\]shop/](https[:]//www.lippionline[.]shop/)

Dirección IP

[172.67.221.142]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01297-01>



CSIRT alerta de sitio fraudulento que suplanta a Converse

Alerta de seguridad cibernética	8FFR23-01298-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023

Indicadores de compromiso

URL sitio falso

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

Dirección IP

[196.247.29.14]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01298-01>

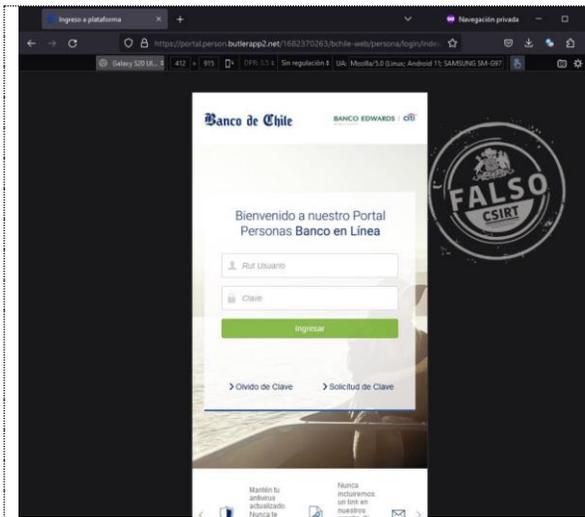
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

Boletín de Seguridad Cibernética N° 199

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

BOLETÍN 13BCS23-00208-01 | Semana del 21 al 27 de abril de 2023



CSIRT alerta de nueva página fraudulenta que suplanta al Banco de Chile

Alerta de seguridad cibernética	8FFR23-01299-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023

Indicadores de compromiso

URL sitio falso

[https://is\[.\]gd/AyudaBancoChile](https://is[.]gd/AyudaBancoChile)
[https://portal.person.butlerapp2\[.\]net/1682370263/bchile-web/persona/login/index.html/login](https://portal.person.butlerapp2[.]net/1682370263/bchile-web/persona/login/index.html/login)

Dirección IP

[68.66.216.52]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01299-01>



CSIRT alerta de sitio fraudulento que suplanta al Banco Ripley

Alerta de seguridad cibernética	8FFR23-01300-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023

Indicadores de compromiso

URL sitio falso

<https://web-bancoripley-cl.web-bancoripley-cl-login.info/1682428126/login/index.html>

Dirección IP

[172.64.80.1]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01300-01>



CSIRT alerta de sitio fraudulento que suplanta a Codelco

Alerta de seguridad cibernética	8FFR23-01301-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023

Indicadores de compromiso

URL sitio falso

[https://lps.lemonsharkonline\[.\]com/codc_es_lat_iso](https://lps.lemonsharkonline[.]com/codc_es_lat_iso)

Dirección IP

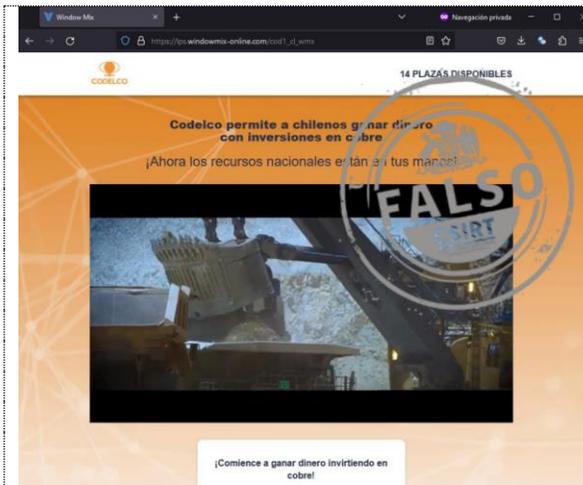
[104.21.53.39]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01301-01>

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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



CSIRT alerta ante sitio fraudulento que suplanta a Codelco

Alerta de seguridad cibernética	8FFR23-01302-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2023
Última revisión	26 de abril de 2023

Indicadores de compromiso

URL sitio falso

[https://ps.windowmix-online\[.\]com/cod1_cl_wmx](https://ps.windowmix-online[.]com/cod1_cl_wmx)

Dirección IP

[172.67.165.248]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01302-01>



CSIRT advierte ante nueva página fraudulenta que suplanta al Banco de Chile

Alerta de seguridad cibernética	8FFR23-01303-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2023
Última revisión	26 de abril de 2023

Indicadores de compromiso

URL sitio falso

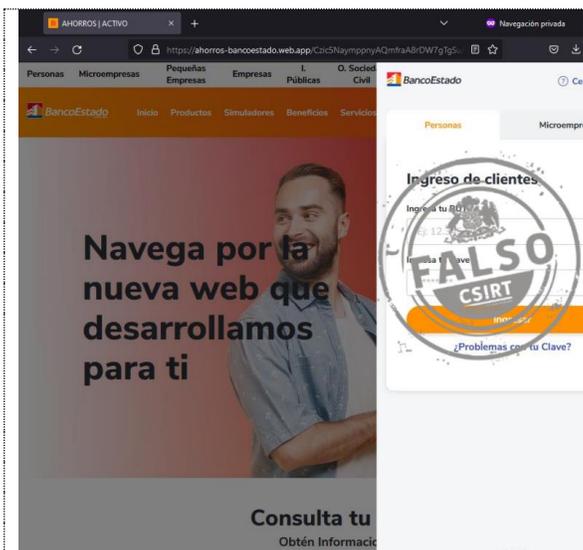
[https://p0rtalpersons-bnncochile.cl-sow\[.\]top/1682458068/bchile-web/persona/login/index.html/login](https://p0rtalpersons-bnncochile.cl-sow[.]top/1682458068/bchile-web/persona/login/index.html/login)

Dirección IP

[104.21.57.217]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01303-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado

Alerta de seguridad cibernética	8FFR23-01304-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2023
Última revisión	26 de abril de 2023

Indicadores de compromiso

URL sitio falso

[https://bit\[.\]ly/40wP5AM](https://bit[.]ly/40wP5AM)

[https://ahorros-bancoestado.web\[.\]app/btCXLHfcDNukkZqUaL9TrbtdBY9xqA/itm?source=true&f_rd_r=hjdfdl67bjk](https://ahorros-bancoestado.web[.]app/btCXLHfcDNukkZqUaL9TrbtdBY9xqA/itm?source=true&f_rd_r=hjdfdl67bjk)

Dirección IP

[199.36.158.100]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01304-01>

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

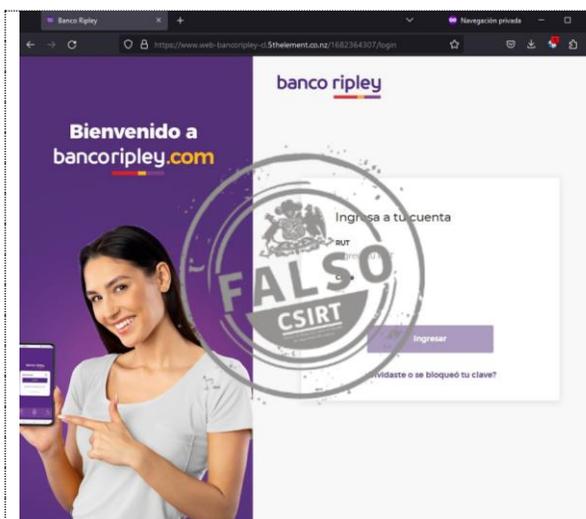
<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

2. Phishing



CSIRT alerta ante campaña de smishing que suplanta a CorreosChile

Alerta de seguridad cibernética	8FPH23-00797-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023
URL redirección	http://cuqd[.]me/Zs1ucE
URL sitio falso	https://informu[.]live/correos_cl/ https://fndngsmnspcltdy.com/user
Dirección IP	[93.95.227.126]
Enlace para revisar loC:	https://www.csirt.gob.cl/alertas/8fph23-00797-01/



CSIRT alerta campaña de phishing que suplanta a Banco Ripley

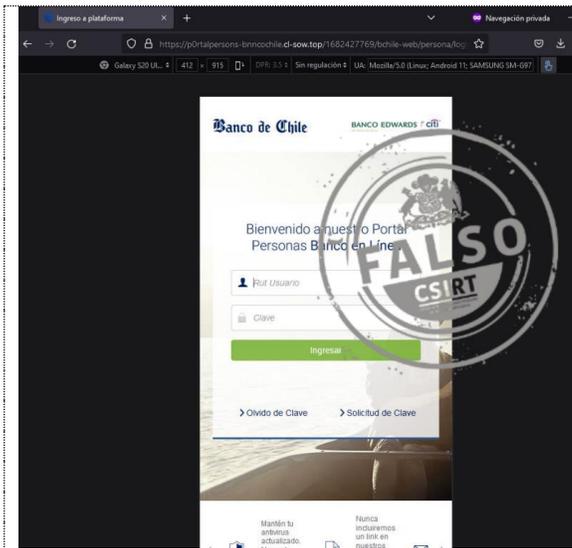
Alerta de seguridad cibernética	8FPH23-00798-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2023
Última revisión	24 de abril de 2023
Indicadores de compromiso	
URL sitio falso	https://www.web-bancoripley-cl.5thelement[.]co.nz/1682364307/login
URL redirección:	https://bit[.]ly/40tvcd7?l=www.bancoripley.cl
Dirección IP sitio falso	[185.184.154.1]
Enlace para revisar loC:	https://www.csirt.gob.cl/alertas/8fph23-00798-01/

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

Boletín de Seguridad Cibernética N° 199

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

BOLETÍN 13BCS23-00208-01 | Semana del 21 al 27 de abril de 2023



CSIRT alerta ante nueva campaña de phishing que suplanta al Banco de Chile

Alerta de seguridad cibernética	8FPH23-00799-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023

Indicadores de compromiso

URL sitio falso

[https\[:\]//p0rtalpersons-bnncochile.cl-sow\[.\]top/1682427635/bchile-web/persona/login/index.html/login](https[:]//p0rtalpersons-bnncochile.cl-sow[.]top/1682427635/bchile-web/persona/login/index.html/login)

URL redirección:

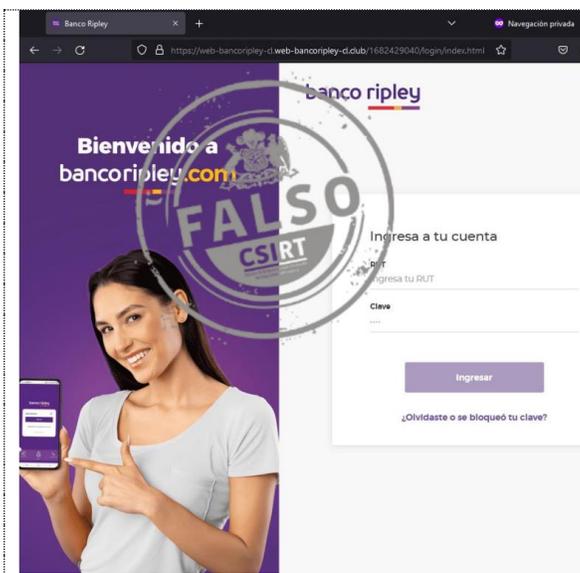
[https\[:\]//bit\[.\]ly/3N6INUQ](https[:]//bit[.]ly/3N6INUQ)

Dirección IP sitio falso

[104.21.57.217]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00799-01/>



CSIRT alerta ante nueva campaña de phishing que suplanta al Banco Ripley

Alerta de seguridad cibernética	8FPH23-00800-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023

Indicadores de compromiso

URL redirección:

[https\[:\]//bit\[.\]ly/40B3Hyg?l=www.bancoripley.cl](https[:]//bit[.]ly/40B3Hyg?l=www.bancoripley.cl)

[https\[:\]//sam-tech\[.\]jp/bancoripley/cuenta-wplw/](https[:]//sam-tech[.]jp/bancoripley/cuenta-wplw/)

URL sitio falso:

[https\[:\]//web-bancoripley-cl.web-bancoripley-cl\[.\]club/1682429040/login/index.html](https[:]//web-bancoripley-cl.web-bancoripley-cl[.]club/1682429040/login/index.html)

Dirección IP sitio falso

[104.21.17.239]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00800-01/>

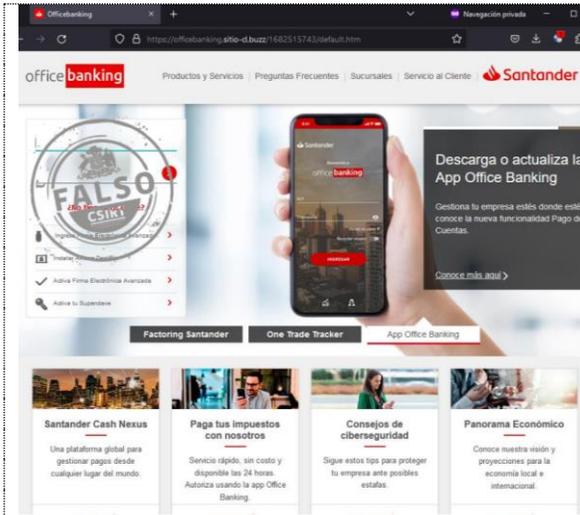
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

Boletín de Seguridad Cibernética N° 199

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

BOLETÍN 13BCS23-00208-01 | Semana del 21 al 27 de abril de 2023



CSIRT alerta de una nueva campaña de phishing que suplanta a Banco Santander

Alerta de seguridad cibernética	8FPH23-00801-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2023
Última revisión	26 de abril de 2023
Indicadores de compromiso	
URL sitio redirección	
https://bit.ly/3HgiyYp?l=www.officebanking.cl http://wordpress.zuliatec.com/ve/activacion/cuenta-ufbq/	
URL sitio falso	
https://officebanking.sitio-cl.buzz/1682515743/default.htm	
Dirección IP	
[172.67.212.81]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00801-01/	

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

3. Vulnerabilidades



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00821-01
CSIRT comparte vulnerabilidades parchadas por VMware para uno de sus productos

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

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte vulnerabilidades críticas para VMware Aria Operations for Logs

Alerta de seguridad cibernética	9VSA23-00821-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2023
Última revisión	21 de abril de 2023
CVE	
	CVE-2023-20864
	CVE-2023-20865
Fabricantes	
	VMware
Productos afectados	
	VMware Aria Operations for Logs
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00821-01/



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00822-01
CSIRT comparte vulnerabilidades parchadas por SolarWinds para uno de sus productos

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

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de vulnerabilidades parchadas en SolarWinds Platforms

Alerta de seguridad cibernética	9VSA23-00822-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2023
Última revisión	25 de abril de 2023
CVE	
	CVE-2022-36963
	CVE-2022-47505
	CVE-2022-47509
	CVE-2023-23838
	CVE-2023-23837
Fabricantes	
	Solarwinds
Productos afectados	
	SolarWinds Platform, versiones anteriores a la 2023.2, que resuelve ambas vulnerabilidades.
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00825-01/

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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



CSIRT comparte vulnerabilidad crítica parchada por VMware	
Alerta de seguridad cibernética	9VSA23-00823-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de abril de 2023
Última revisión	27 de abril de 2023
CVE	
CVE-2023-20869	
Fabricantes	
VMware	
Productos afectados	
VMware Workstation y Fusion. Versiones corregidas: Workstation 17.0.2 y Fusion 13.0.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00823-01/	

4. Malware



CSIRT alerta de nueva campaña de phishing con malware, que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV23-00411-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2023
Última revisión	21 de abril de 2023
Indicadores de compromiso	
URL-Dominio	bazuca20233.hopto[.]org
SHA256	f1b1e0e27582995da9cf2c954a41b18a3d4397b9e24cfc981f50ab0e20461e2de87c8713fac002b0b0a0f9b02c4e3ebcccf65282a22f5ab5912a9da00f35c2afe2b187f223d323379ff82e2f561ec3b559e6422166800def2d192d5cd8cb56c09d0790e550694350b94ca6b077c54f983c135fab8990df5a75462804150912
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00411-01/	

5. Concientización

Advertencia email de phishing

Esta semana alertamos a la comunidad, a través de nuestros Instagram y Twitter de CSIRT Conciencia, de un correo malicioso que simulaba provenir de un supuesto hacker chino, y que extorsionaba a sus receptores amenazando que si no era pagado publicaría fotos privadas de ellos. Pueden verlo aquí: <https://twitter.com/CSIRTConciencia/status/1650608697058492416?s=20>.



CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

Ciberdiccionario Volumen 34

En la presente edición del Ciberdiccionario decidimos incluir dos situaciones, el grooming y la sextorsión, que, de sufrirlas, pueden ser denunciados a la Policía de Investigaciones (PDI) y el Ministerio Público. Además, revisamos el single sign-on y los ataques BEC. Como siempre, está disponible también en el siguiente link: csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-34/.

 <h3>Ciber diccionario</h3> <h4>Sextorsión</h4> <p>Chantaje realizado generalmente a través de internet, en el cual se exige a la víctima un pago, material pornográfico u otras acciones, a cambio de no revelar material íntimo que dice tener de ésta. Es clave tener mucho cuidado si se decide compartir este tipo material, de uno mismo o de otras personas, ya que puede ser usado por delincuentes. La sextorsión también puede ser parte del grooming.</p> 	 <h3>Ciber diccionario</h3> <h4>Grooming</h4> <p>Proceso a través del cual un adulto va ganando la confianza de un menor de edad, con el objetivo de conseguir material pornográfico o contacto sexual con éste. Para lograrlo, muchas veces estos adultos se hacen pasar por otros niños en sitios de juegos o redes sociales. Para combatirlo es clave mantener una relación de confianza y comunicación con nuestros hijos.</p> 
 <h3>Ciber diccionario</h3> <h4>Single sign-on (SSO)</h4> <p>Servicio que permite a un usuario acceder a varias aplicaciones haciendo login una sola vez. Entrega comodidad, pero también tiene implicancias para la seguridad. SSO puede ser usado en empresas, como también por personas naturales. Si accedemos, por ejemplo, a otras aplicaciones con nuestras credenciales de Google o Facebook, estamos utilizando formas de SSO.</p> 	 <h3>Ciber diccionario</h3> <h4>BEC (Business Email Compromise)</h4> <p>En castellano llamado Compromiso del Email Corporativo, es un ataque en el que los criminales contactan a mandos medios de una empresa haciéndose pasar por un jefe e instruyendo pagos a alguna cuenta bancaria o la entrega de datos sensibles, supuestamente a un cliente o proveedor, en general con urgencia. Creyendo que se trata de una orden de su superior, el empleado aprueba la transacción de dinero o datos.</p> 

Ciberconsejos para cuidar tu ClaveÚnica

La ClaveÚnica es la forma que tienes para acceder a los servicios del Estado de forma online y realizar diversos trámites, por eso nunca debes entregar tus datos de ClaveÚnica a ninguna institución ni persona, ya que podrías ser víctima de un mal uso o de algún fraude. ¡Sólo tú eres el dueño de esa información!

El CSIRT de Gobierno junto con Gobierno Digital lanzamos una campaña con las siguientes recomendaciones: csirt.gob.cl/recomendaciones/ciberconsejos-para-cuidar-tu-claveunica/



The infographic is divided into three sections. The top-left section, titled '¿Qué es la ClaveÚnica?', explains that it is the way to access state services online. The top-right section, titled '¿Para qué se usa?', lists 1,795 public services and provides five examples: applying for benefits, reporting crimes, getting certificates, accessing social registry, and accessing tax information. The bottom section, titled 'Recomendaciones', lists four security tips: do not share the key, do not give it to anyone, use it only on personal devices, and verify access on the official portal.

¿Qué es la ClaveÚnica?

Es la forma que tienes para acceder a los servicios del Estado de forma online y realizar diversos trámites.

¿Para qué se usa?

En la actualidad, puedes hacer más de 1.795 trámites en el sector público, como por ejemplo:

- Postular a beneficios y subsidios.
- Efectuar denuncias en la Comisaría Virtual.
- Obtener certificados y efectuar trámites en el Registro Civil.
- Acceder a tu ficha del Registro Social de Hogares.
- Acceder a tu información tributaria.

Recomendaciones

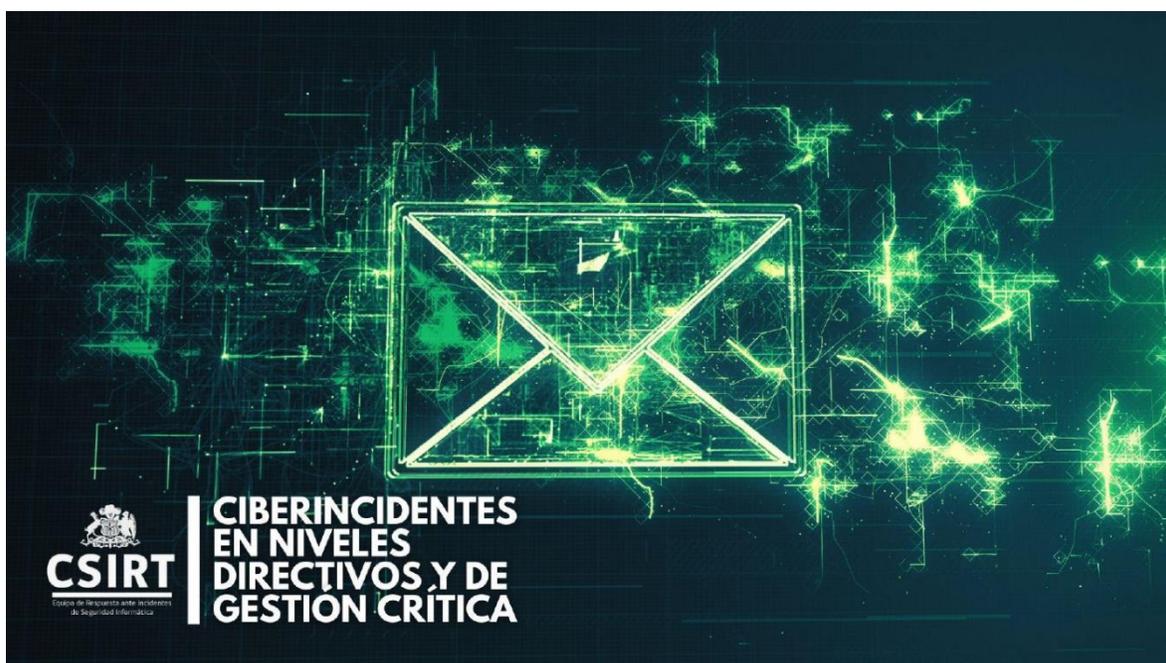
- ✓ No compartas tu ClaveÚnica con otras personas o empresas, incluso si se trata de amigos.
- ✓ Nadie te llamará para pedir tu ClaveÚnica.
- ✓ Trata de utilizar tu ClaveÚnica sólo en tus dispositivos móviles y computadoras personales.
- ✓ Accede a tu perfil en el portal de ClaveÚnica en <https://claveunica.gob.cl/>, aquí puedes verificar tus accesos a las diversas plataformas integradas.

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

BEC | Ciberincidentes en niveles directivos y de gestión crítica

Una forma en la que los ciberdelincuentes buscan causar el mayor daño a empresas y otras instituciones es enfocándose en engañar a personas en los niveles directivos y de gestión crítica de las organizaciones. Estos ataques, entre los que se encuentran el BEC, o compromiso de correo empresarial, y el Fraude del CEO.

En el siguiente enlace les explicamos las características de los principales ataques contra los niveles directivos y de gestión crítica, y cómo darnos cuenta de que podemos estar en presencia de alguno de ellos, para evitar ser una víctima: <https://www.csirt.gob.cl/recomendaciones/bec-2023/>.



CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

6. Recomendaciones y buenas prácticas

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

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: 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.

- Andres Santana Mansilla
- Cristian Navarrete
- Claudio Soto
- Wladimir Hernandez
- Juan Carlos Molina
- Tamara Llana
- Isabel Alejandra González
- Julio López Rodríguez
- Raúl Yañez Belmar
- Jorge Alejandro Ramos
- Oscar Rodrigo Ulloa
- Ximena Pérez

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO