



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 205
semana del 2 al 8 de junio de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

39

IP advertidas en múltiples campañas de phishing y de malware.



URL ADVERTIDAS

82

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

63

Las mitigaciones son útiles en productos de Google (Chrome y Android), Cisco, Microsoft y VMware.



HASH REPORTADOS

6

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



CONTENIDO

1.	Sitios fraudulentos	3
2.	Phishing	18
3.	Malware.....	20
4.	Vulnerabilidades	21
5.	Concientización.....	24
6.	Recomendaciones y buenas prácticas	25
7.	Muro de la Fama	26

11111<

1. Sitios fraudulentos



CSIRT alerta ante nuevo sitio fraudulento que suplanta a SQM

Alerta de seguridad cibernética	8FFR23-01354-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

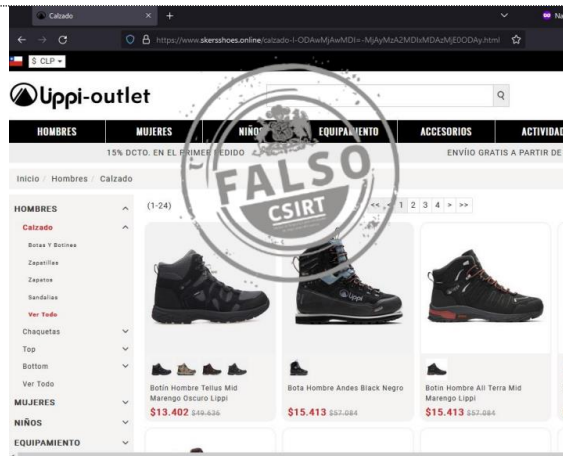
https://real-investoffer.com/es?campaign_id=sGMNdnt8&c=w7dtgil276mba54p2mrvj6cq&p1=mpanda_a&p4=sqm&theme=ccu&ksget=1&analytics_session_id=26e45d2b727512c77fe766be9efc982f6e4964b81685569609&token=6477c049696a73f73705ce73

Dirección IP

[172.67.173.59]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01354-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01355-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

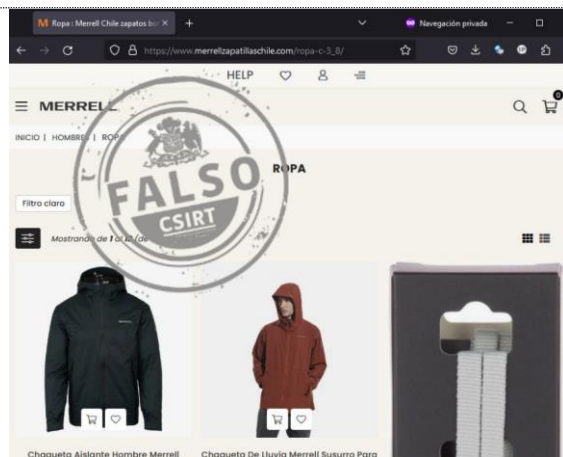
[https://www.skersshoes\[.\]online/](https://www.skersshoes[.]online/)

Dirección IP

[167.160.3.15]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01355-01>



CSIRT alerta de sitio fraudulento que suplanta a Merrell

Alerta de seguridad cibernética	8FFR23-01356-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

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

Dirección IP

[172.67.163.162]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01356-01>

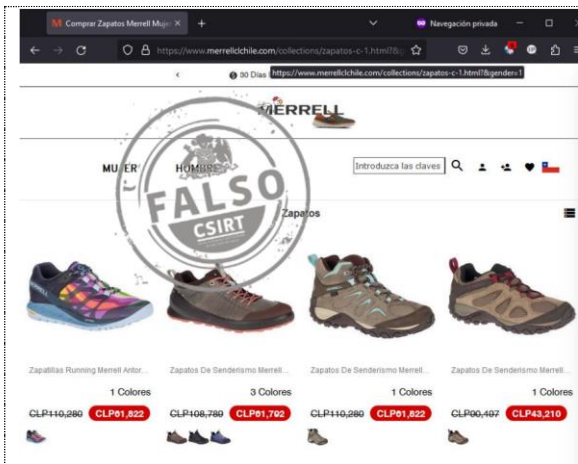
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 205

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

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



CSIRT alerta de sitio fraudulento que suplanta a Merrell

Alerta de seguridad cibernética	8FFR23-01357-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

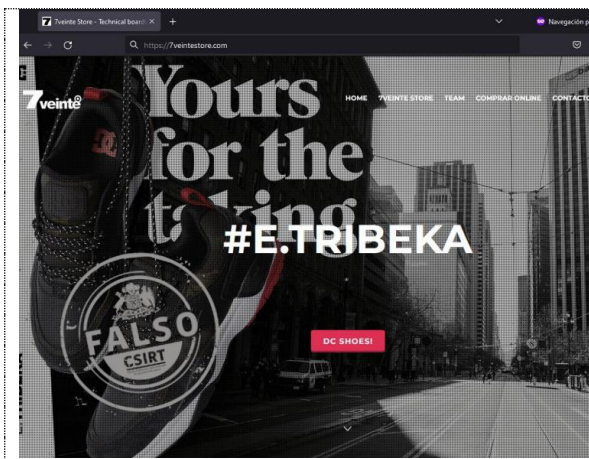
[https://www.merrellclchile\[.\]com](https://www.merrellclchile[.]com)

Dirección IP

[5.157.59.40]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01357-01>



CSIRT alerta de un nuevo sitio fraudulento que suplanta a 7einte

Alerta de seguridad cibernética	8FFR23-01358-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

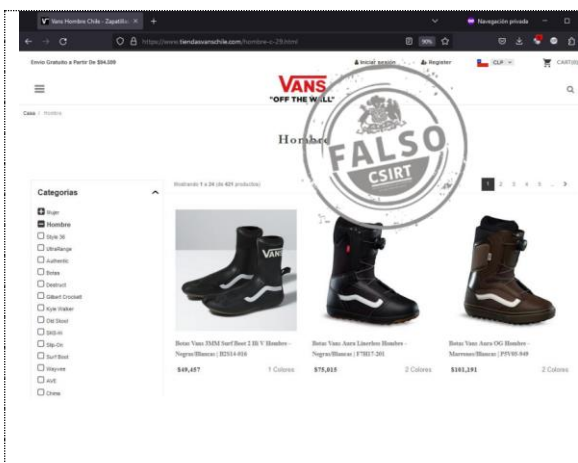
[https://7veintestore\[.\]com](https://7veintestore[.]com)

Dirección IP

[200.58.110.103]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01358-01>



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Vans

Alerta de seguridad cibernética	8FFR23-01359-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

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

Dirección IP

[196.242.16.220]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01359-01>

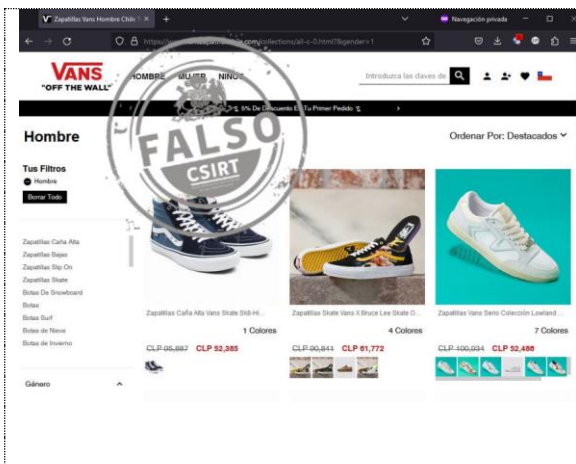
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 205

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

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Vans

Alerta de seguridad cibernética	8FFR23-01360-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

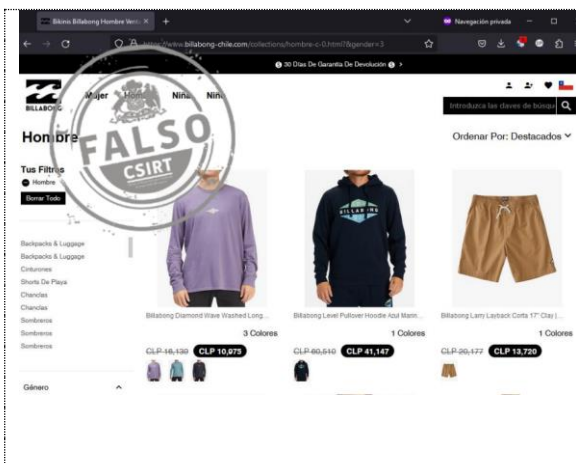
[https://www.vanszapattillaschile\[.\]com](https://www.vanszapattillaschile[.]com)

Dirección IP

[196.196.206.184]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01360-01>



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Billabong

Alerta de seguridad cibernética	8FFR23-01361-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

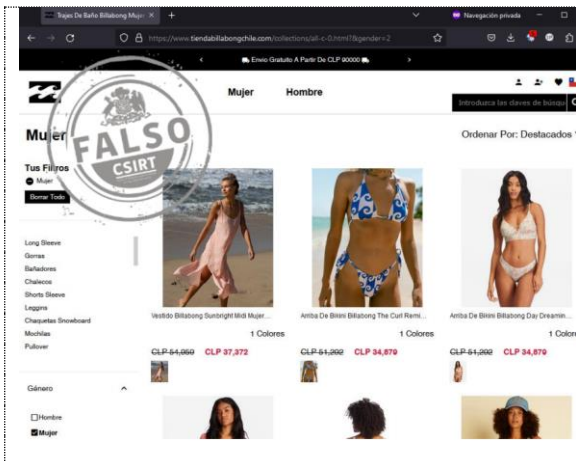
[https://www.billabong-chile\[.\]com/](https://www.billabong-chile[.]com/)

Dirección IP

[196.196.101.90]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01361-01>



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Billabong

Alerta de seguridad cibernética	8FFR23-01362-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

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

Dirección IP

[196.240.79.98]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01362-01>

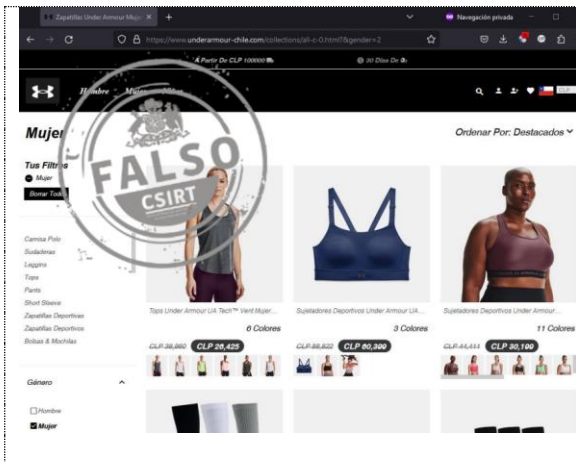
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 205

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

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Under Armour

Alerta de seguridad cibernética	8FFR23-01363-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

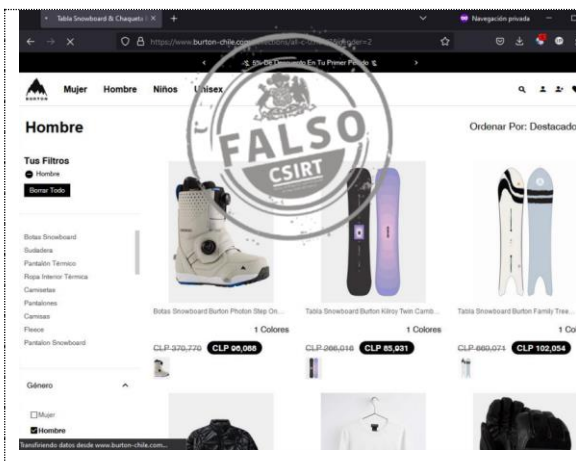
[https://www.underarmour-chile\[.\]com](https://www.underarmour-chile[.]com)

Dirección IP

[196.196.57.13]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01363-01>



CSIRT alerta de un sitio fraudulento que suplanta a Burton

Alerta de seguridad cibernética	8FFR23-01364-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

[https://www.burton-chile\[.\]com/](https://www.burton-chile[.]com/)

Dirección IP

[196.196.57.13]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01364-01>



CSIRT alerta de nueva página fraudulenta que suplanta a Under Armour

Alerta de seguridad cibernética	8FFR23-01365-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

Indicadores de compromiso

URL sitio falso

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

Dirección IP

[104.21.5.68]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01365-01>

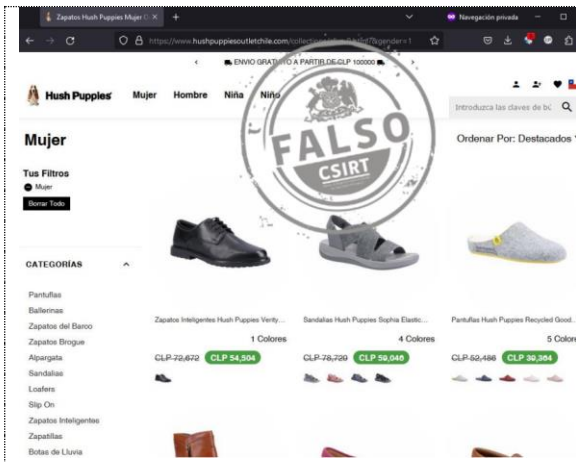
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 205

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

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



CSIRT alerta de nuevo sitio fraudulento que suplanta a Hush Puppies

Alerta de seguridad cibernética	8FFR23-01366-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2023
Última revisión	3 de junio de 2023

Indicadores de compromiso

URL sitio falso

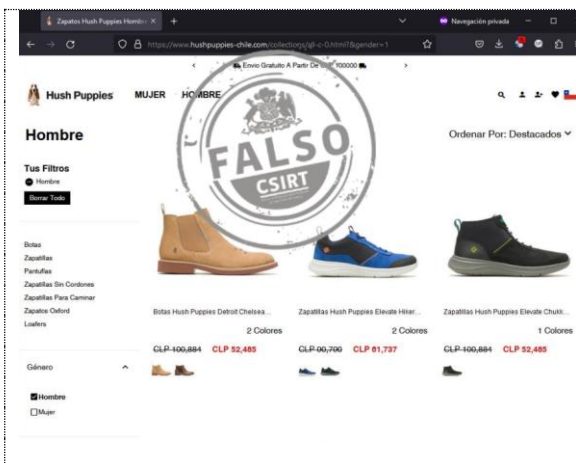
[https://www.hushpuppiesoutletchile\[.\]com/](https://www.hushpuppiesoutletchile[.]com/)

Dirección IP

[165.231.33.102]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01366-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Hush Puppies

Alerta de seguridad cibernética	8FFR23-01367-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2023
Última revisión	3 de junio de 2023

Indicadores de compromiso

URL sitio falso

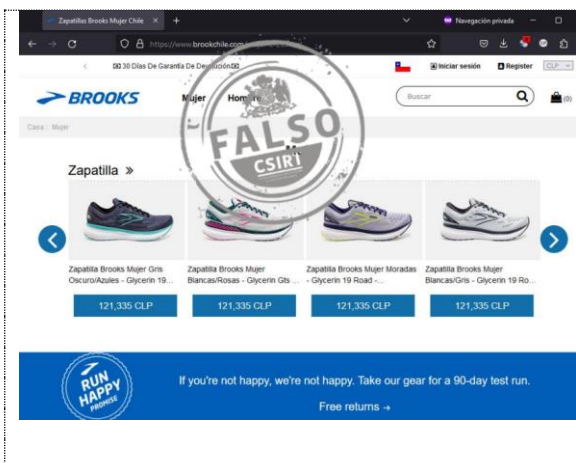
[https://www.hushpuppies-chile\[.\]com/](https://www.hushpuppies-chile[.]com/)

Dirección IP

[196.196.98.14]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01367-01>



CSIRT alerta de un sitio fraudulento que suplanta a Brooks

Alerta de seguridad cibernética	8FFR23-01368-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2023
Última revisión	3 de junio de 2023

Indicadores de compromiso

URL sitio falso

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

Dirección IP

[196.247.61.19]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01368-01>

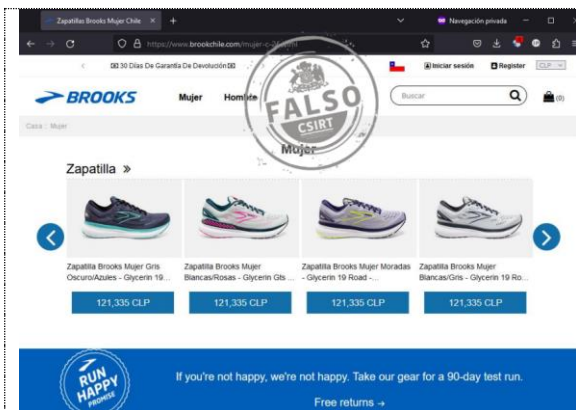
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 205

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

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



CSIRT alerta de un sitio fraudulento que suplanta a Brooks

Alerta de seguridad cibernética	8FFR23-01369-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2023
Última revisión	3 de junio de 2023

Indicadores de compromiso

URL sitio falso

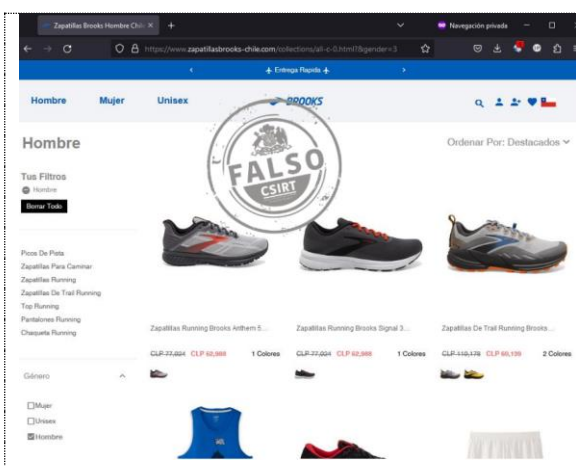
[https://www.chilebrooks\[.\]com/](https://www.chilebrooks[.]com/)

Dirección IP

[104.21.42.54]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01369-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Brooks

Alerta de seguridad cibernética	8FFR23-01370-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2023
Última revisión	3 de junio de 2023

Indicadores de compromiso

URL sitio falso

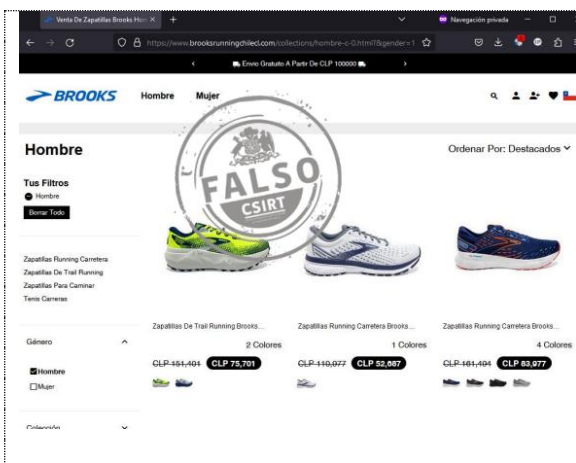
[https://www.zapatillasbrooks-chile\[.\]com/](https://www.zapatillasbrooks-chile[.]com/)

Dirección IP

[196.196.210.145]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01370-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Brooks

Alerta de seguridad cibernética	8FFR23-01371-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2023
Última revisión	3 de junio de 2023

Indicadores de compromiso

URL sitio falso

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

Dirección IP

[196.247.55.122]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01371-01>

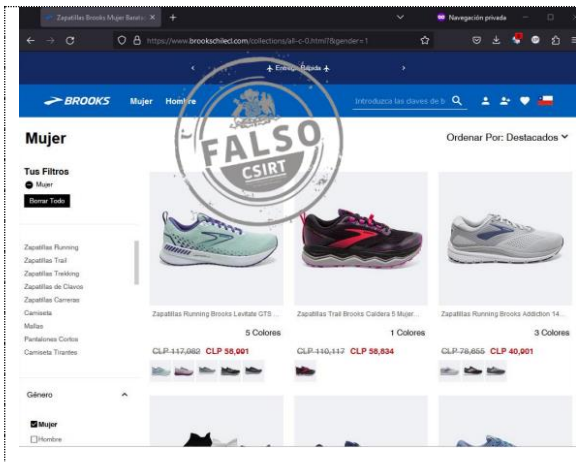
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 205

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

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



CSIRT alerta de nuevo sitio fraudulento que suplanta a Brooks

Alerta de seguridad cibernética	8FFR23-01372-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL sitio falso

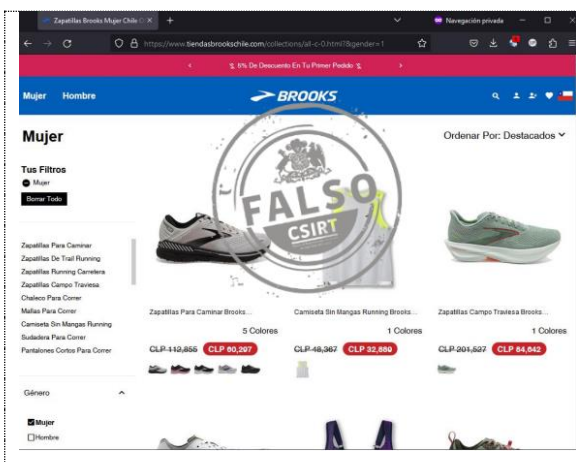
[https://www.brookschilecl\[.\]com/](https://www.brookschilecl[.]com/)

Dirección IP

[196.196.223.167]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01372-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Brooks

Alerta de seguridad cibernética	8FFR23-01373-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL sitio falso

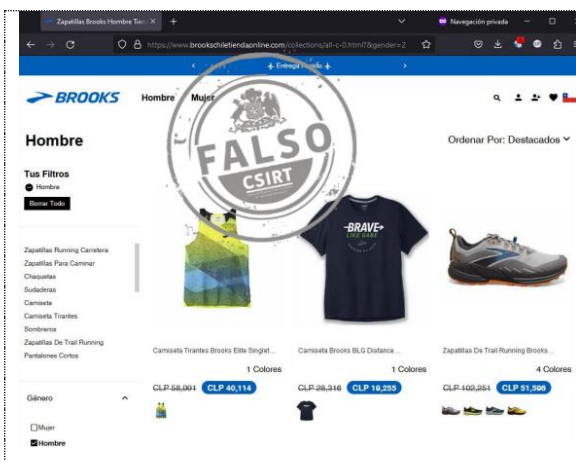
[https://www.tiendasbrookschile\[.\]com/](https://www.tiendasbrookschile[.]com/)

Dirección IP

[196.196.38.172]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01373-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Brooks

Alerta de seguridad cibernética	8FFR23-01374-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL sitio falso

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

Dirección IP

[91.108.179.144]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01374-01>

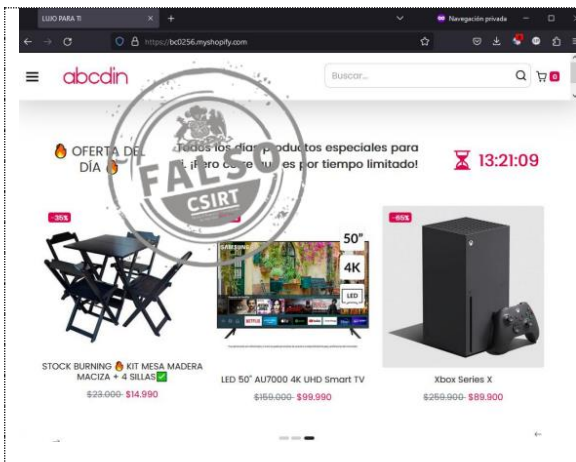
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 205

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

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



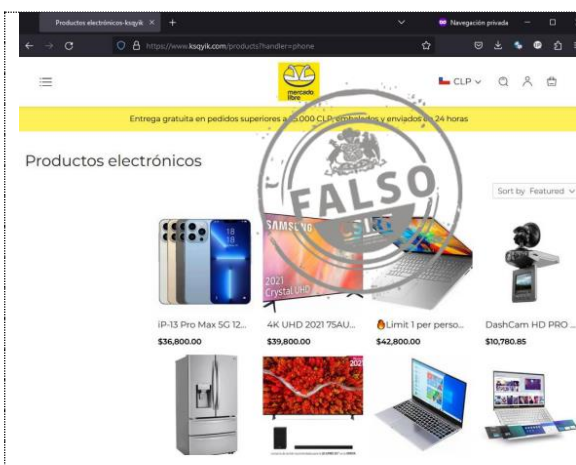
CSIRT alerta de sitio fraudulento que suplanta a ABCDin

Alerta de seguridad cibernética	8FFR23-01375-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023
Indicadores de compromiso	
URL sitio falso	https://bc0256.myshopify[.]com/
Dirección IP	[23.227.38.74]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01375-01



CSIRT alerta de sitio fraudulento que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01376-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023
Indicadores de compromiso	
URL sitio falso	https://www.lp-outdoor[.]shop
Dirección IP	[172.67.152.204]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01376-01

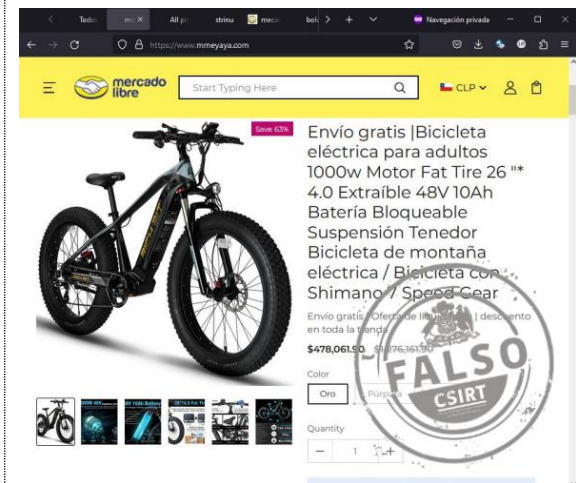
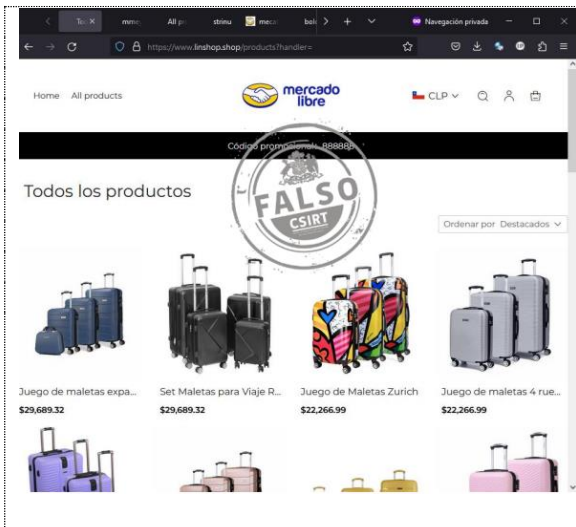


CSIRT alerta de sitio fraudulento que suplanta a Mercado Libre

Alerta de seguridad cibernética	8FFR23-01377-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023
Indicadores de compromiso	
URL sitio falso	https://www.ksqyik[.]com
Dirección IP	[75.2.103.32]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01377-01

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.instagram.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>



CSIRT alerta ante varios sitios fraudulentos que suplantan a Mercado Libre

Alerta de seguridad cibernética	8FFR23-01378-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL sitio falso

[https://www.linshop\[.\]shop](https://www.linshop[.]shop)
[https://www.mmeyaya\[.\]com/](https://www.mmeyaya[.]com/)
[https://www.autorza\[.\]com/](https://www.autorza[.]com/)
[https://www.strinu\[.\]com/](https://www.strinu[.]com/)
[https://www.mecator\[.\]shop/](https://www.mecator[.]shop/)
[https://www.bold-bright\[.\]com/](https://www.bold-bright[.]com/)
[https://www.mouumo\[.\]com/](https://www.mouumo[.]com/)
[https://www.mosheis\[.\]com/](https://www.mosheis[.]com/)
[https://www.flodors\[.\]com/](https://www.flodors[.]com/)
[https://www.momymi\[.\]com/](https://www.momymi[.]com/)
[https://www.dskkj\[.\]com/](https://www.dskkj[.]com/)
[https://www.cyber-zap\[.\]com/](https://www.cyber-zap[.]com/)
[https://www.qvukxp\[.\]com/](https://www.qvukxp[.]com/)
[https://www.moexie\[.\]com/](https://www.moexie[.]com/)
[https://www.wise-rose\[.\]com/](https://www.wise-rose[.]com/)
[https://www.vbhsag\[.\]com/](https://www.vbhsag[.]com/)
[https://www.buravw\[.\]com/](https://www.buravw[.]com/)
[https://www.wise-glaze\[.\]com/](https://www.wise-glaze[.]com/)
[https://www.rocket-tide\[.\]com/](https://www.rocket-tide[.]com/)
[https://www.mocimci\[.\]com/](https://www.mocimci[.]com/)
[https://www.emyjuk\[.\]com/](https://www.emyjuk[.]com/)
[https://www.hottyou\[.\]com/](https://www.hottyou[.]com/)
[https://www.bbjsqj\[.\]com/](https://www.bbjsqj[.]com/)
[https://www.uoueuo\[.\]com/](https://www.uoueuo[.]com/)

Dirección IP

[75.2.103.32]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01378-01>



CSIRT alerta de sitio fraudulento que suplanta a Falabella

Alerta de seguridad cibernética	8FFR23-01379-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL sitio falso

[https://cl.moceryce\[.\]com](https://cl.moceryce[.]com)

Dirección IP

[104.17.232.29]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01379-01>

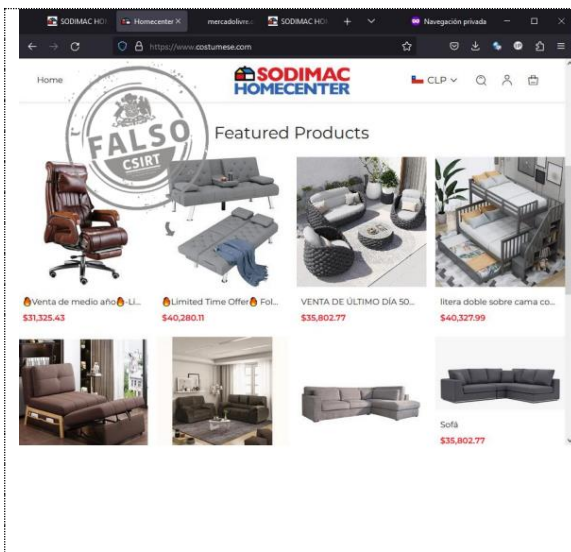
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 205

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

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



CSIRT alerta de un sitio fraudulento que suplanta a Sodimac

Alerta de seguridad cibernética	8FFR23-01380-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL sitio falso

[https://www.fincheeap\[.\]com/](https://www.fincheeap[.]com/)
[https://www.costumese\[.\]com/](https://www.costumese[.]com/)
[https://www.speedy-fawn\[.\]com/](https://www.speedy-fawn[.]com/)
[https://www.mordeniy\[.\]com/](https://www.mordeniy[.]com/)

Dirección IP

[75.2.103.32]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01380-01>



CSIRT alerta de sitio fraudulento que suplanta a Linio

Alerta de seguridad cibernética	8FFR23-01381-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL sitio falso

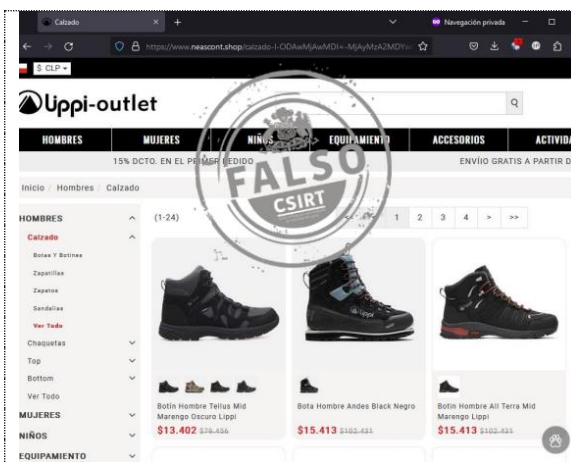
[https://www.horrototol\[.\]com](https://www.horrototol[.]com)

Dirección IP

[75.2.103.32]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01381-01>



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01382-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL sitio falso

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

Dirección IP

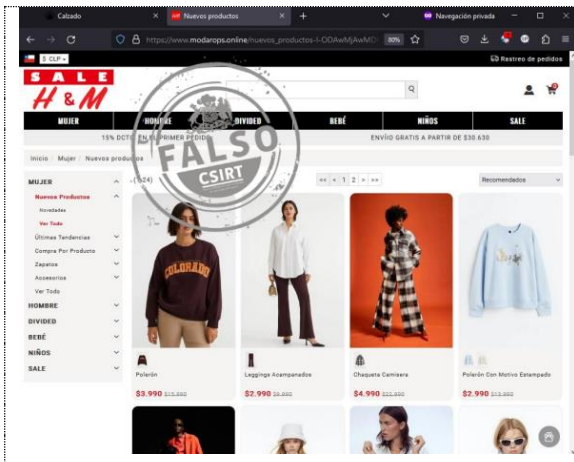
[91.92.112.236]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01382-01>

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 de nuevo sitio fraudulento que suplanta a H&M

Alerta de seguridad cibernética	8FFR23-01383-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL sitio falso

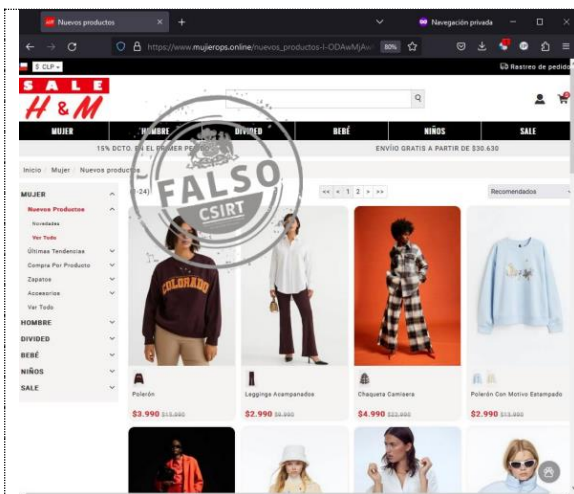
[https://www.modarops\[.\]online/](https://www.modarops[.]online/)

Dirección IP

[91.92.112.236]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01383-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a H&M

Alerta de seguridad cibernética	8FFR23-01384-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de junio de 2023
Última revisión	6 de junio de 2023

Indicadores de compromiso

URL sitio falso

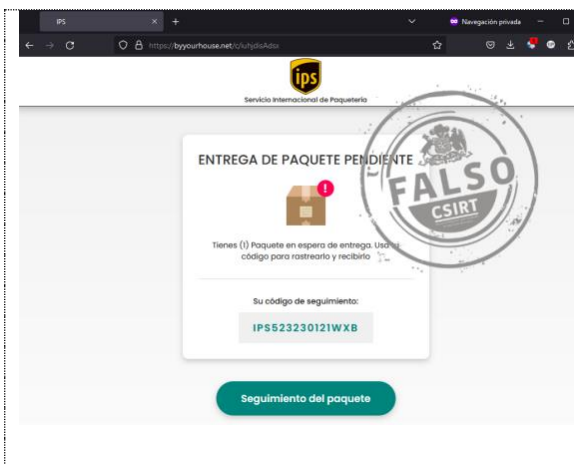
[https://www.mujierops\[.\]online/](https://www.mujierops[.]online/)

Dirección IP

[5.255.62.8]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01384-01>



CSIRT alerta ante página fraudulenta que suplanta a UPS

Alerta de seguridad cibernética	8FFR23-01385-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de junio de 2023
Última revisión	7 de junio de 2023

Indicadores de compromiso

URL sitio falso

[https://byyourhouse\[.\]net/c/iuhjdisAdsx](https://byyourhouse[.]net/c/iuhjdisAdsx)

Dirección IP

[104.21.92.165]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01385-01>

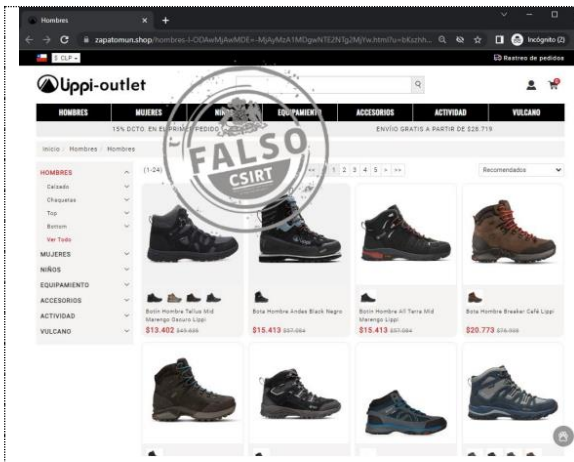
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

- <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° 205

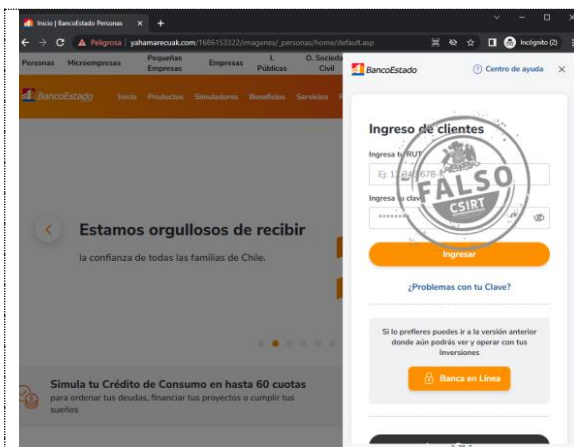
Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



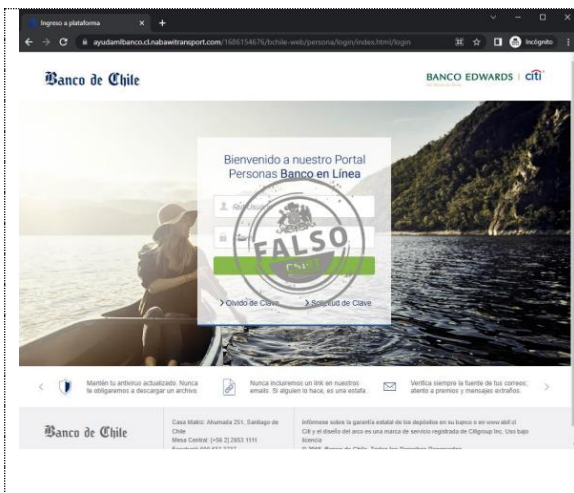
CSIRT alerta de sitio fraudulento que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01386-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de junio de 2023
Última revisión	7 de junio de 2023
Indicadores de compromiso	
URL sitio falso	https://www.zapatomun[.]shop/
Dirección IP	[199.21.150.12]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01386-01



CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado

Alerta de seguridad cibernética	8FFR23-01387-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de junio de 2023
Última revisión	7 de junio de 2023
Indicadores de compromiso	
URL sitio falso	http://yahamarecuak[.]com/1686153322/imagenes/_personas/home/default.asp
Dirección IP	[98.142.101.90]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01387-01

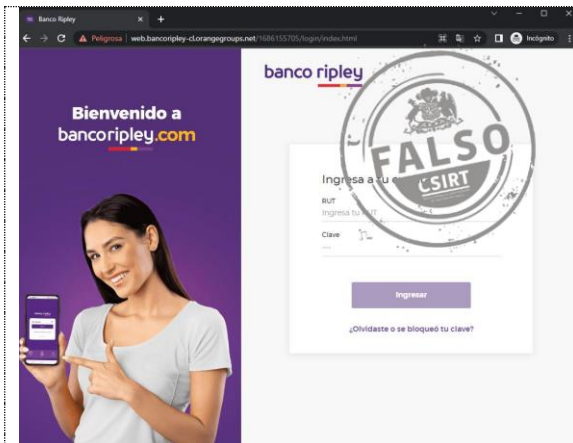


CSIRT alerta ante nuevo sitio fraudulento que suplanta al Banco de Chile

Alerta de seguridad cibernética	8FFR23-01388-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de junio de 2023
Última revisión	7 de junio de 2023
Indicadores de compromiso	
URL sitio falso	https://ayudamlbanco.cl.nabawitransport[.]com/1686154676/bchile-web/persona/login/index.html/login
Dirección IP	[153.92.10.14]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01388-01

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 un nuevo sitio fraudulento que suplanta a Banco Ripley

Alerta de seguridad cibernética	8FFR23-01389-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de junio de 2023
Última revisión	7 de junio de 2023

Indicadores de compromiso

URL sitio falso

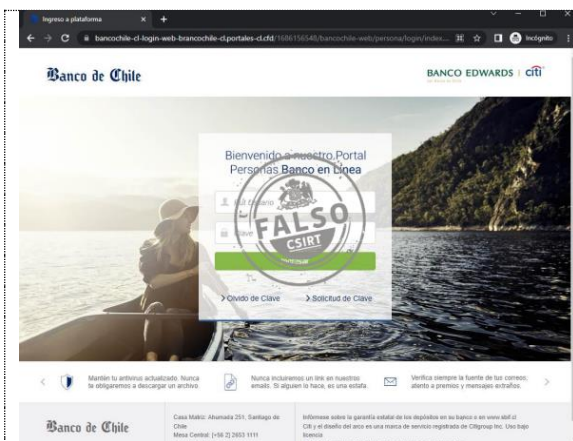
[http://www.web.bancoripley-cl.orangegroups\[.\]net/1686155705/login/index.html](http://www.web.bancoripley-cl.orangegroups[.]net/1686155705/login/index.html)

Dirección IP

[192.185.106.45]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01389-01>



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

Alerta de seguridad cibernética	8FFR23-01390-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de junio de 2023
Última revisión	8 de junio de 2023

Indicadores de compromiso

URL sitio falso

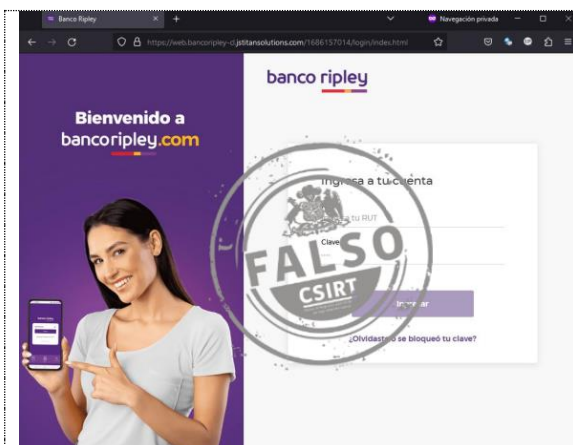
[https://bancochile-cl-login-web-brancochile-cl.portales-cl\[.\]cfd/1686156548/bancochile-web/persona/login/index.html/login](https://bancochile-cl-login-web-brancochile-cl.portales-cl[.]cfd/1686156548/bancochile-web/persona/login/index.html/login)

Dirección IP

[172.67.192.204]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01390-01>



CSIRT alerta de nueva página fraudulenta que suplanta a Banco Ripley

Alerta de seguridad cibernética	8FFR23-01391-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de junio de 2023
Última revisión	8 de junio de 2023

Indicadores de compromiso

URL sitio falso

[https://web.bancoripley-cl.jstiansolutions\[.\]com/1686157014/login/index.html](https://web.bancoripley-cl.jstiansolutions[.]com/1686157014/login/index.html)

Dirección IP

[192.185.188.9]

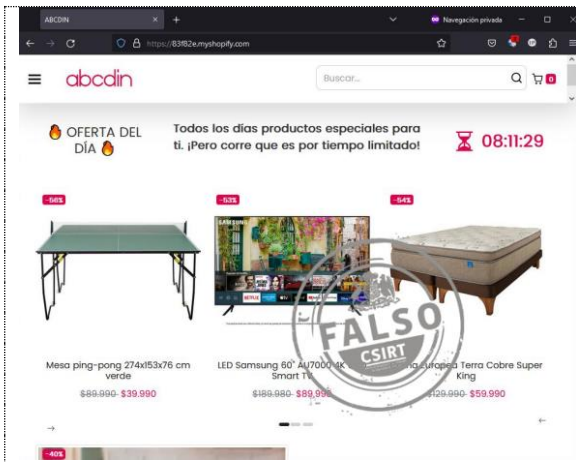
Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01391-01>

Boletín de Seguridad Cibernética N° 205

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

BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023



CSIRT alerta de nuevo sitio fraudulento que suplanta a ABCDin

Alerta de seguridad cibernética	8FFR23-01392-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de junio de 2023
Última revisión	8 de junio de 2023

Indicadores de compromiso

URL sitio falso

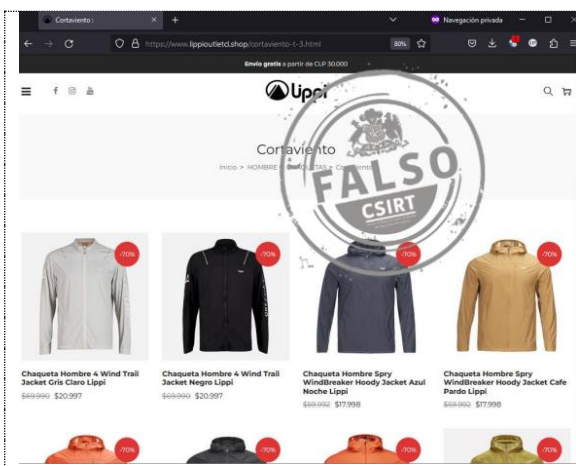
[https://83f82e.myshopify\[.\]com/](https://83f82e.myshopify[.]com/)

Dirección IP

[23.227.38.74]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01392-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01393-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de junio de 2023
Última revisión	8 de junio de 2023

Indicadores de compromiso

URL sitio falso

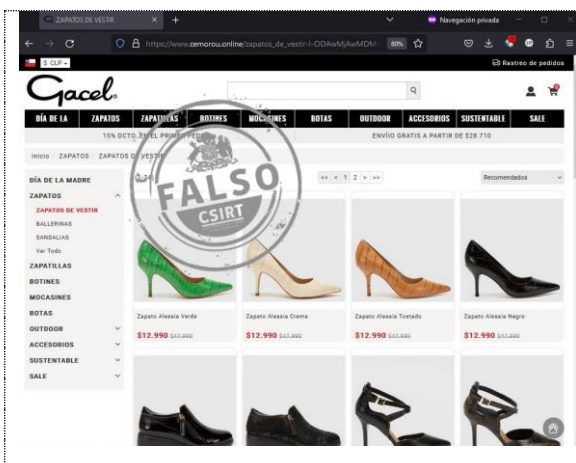
[https://www.lippioutlet\[.\]jshop/](https://www.lippioutlet[.]jshop/)

Dirección IP

[172.67.193.147]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01393-01>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Gacel

Alerta de seguridad cibernética	8FFR23-01394-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de junio de 2023
Última revisión	8 de junio de 2023

Indicadores de compromiso

URL sitio falso

[https://bancoribley-personas.c.naistudio\[.\]ec/1686233848/login/index.html](https://bancoribley-personas.c.naistudio[.]ec/1686233848/login/index.html)

Dirección IP

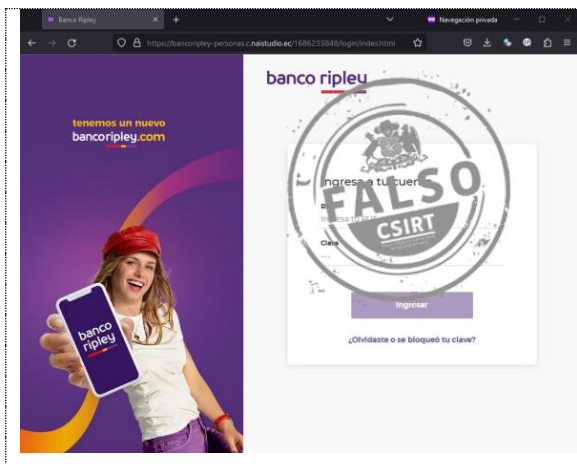
[162.0.235.13]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01394-01>

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 de nuevo sitio fraudulento que suplanta a Gacel

Alerta de seguridad cibernética	8FFR23-01395-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de junio de 2023
Última revisión	8 de junio de 2023

Indicadores de compromiso

URL sitio falso

[https://www.cemorou\[.\]online](https://www.cemorou[.]online)

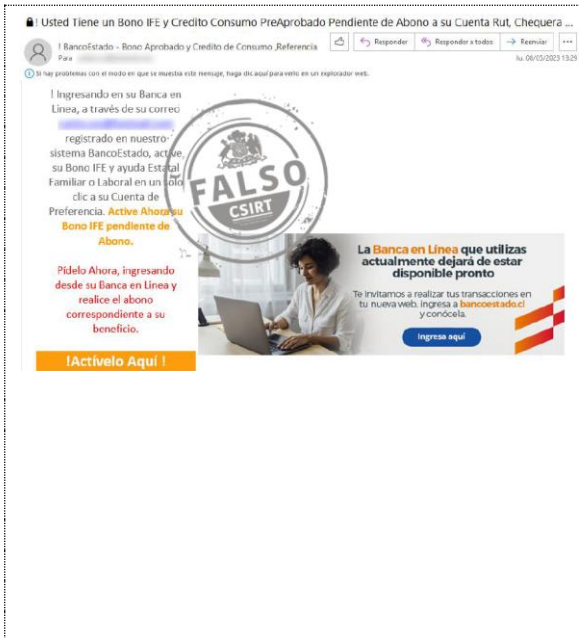
Dirección IP

[162.0.235.13]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01395-01>

2. Phishing



CSIRT alerta de una nueva campaña de phishing, que suplanta a BancoEstado con falsa oferta de bono IFE

Alerta de seguridad cibernética	8FPH23-00828-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2023
Última revisión	2 de junio de 2023

URL redirección

<https://bit.ly/3omdStp>
[http://170.64.146\[.\]220/3da178ffaff64760255ee13d7a50ebdc/17e73d73e9595a4b3f1ea12f791664ff?p=est](http://170.64.146[.]220/3da178ffaff64760255ee13d7a50ebdc/17e73d73e9595a4b3f1ea12f791664ff?p=est)

URL sitio falso

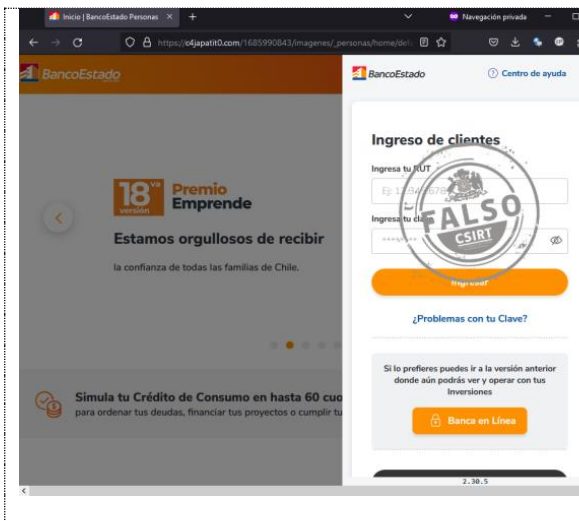
[https://banestado-atencion.web\[.\]japp/ziv2SmWMqyaNqAzrCTvxAvAvj9Lgix/sim?source=usg&node=1f7f14fq7i](https://banestado-atencion.web[.]japp/ziv2SmWMqyaNqAzrCTvxAvAvj9Lgix/sim?source=usg&node=1f7f14fq7i)

Dirección IP

[199.36.158.100]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00828-01/>



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH23-00829-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de junio de 2023
Última revisión	5 de junio de 2023

Indicadores de compromiso

URL redirección

[https://reachercontact\[.\]com/activacion/cuenta-zksc/](https://reachercontact[.]com/activacion/cuenta-zksc/)

URL sitio falso

[https://c4japatit0\[.\]com/1685990843/imagenes/_personas/home/default.asp](https://c4japatit0[.]com/1685990843/imagenes/_personas/home/default.asp)

Dirección IP sitio falso

[72.29.91.210]

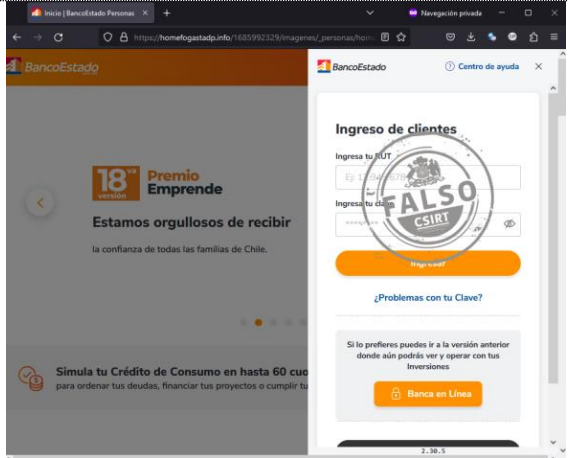
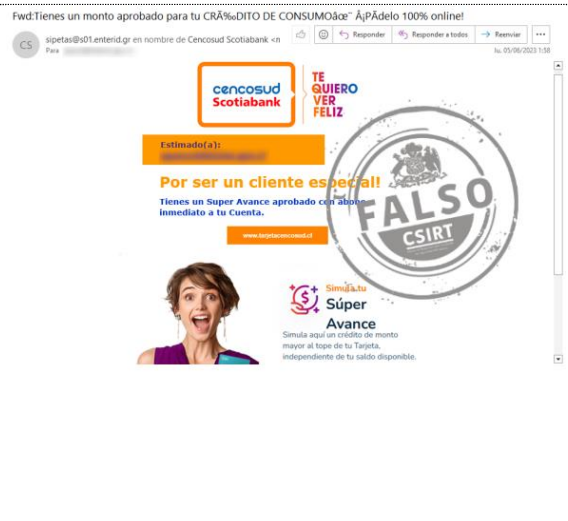

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00829-01/>

Boletín de Seguridad Cibernética N° 205

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


BOLETÍN 13BCS23-00214-01 | Semana del 2 al 8 de junio de 2023

	<p>CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado</p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00830-01</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>5 de junio de 2023</td></tr> <tr><td>Última revisión</td><td>5 de junio de 2023</td></tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección https://hopgia[.]vn/core/activacion/cuenta-kyhu/</p> <p>URL sitio falso https://homefogastadp[.]info/1685992329/imagenes/_personas/home/default.asp</p> <p>Dirección IP sitio falso [213.136.93.171]</p> <p>Enlace para revisar loC: https://www.csirt.gob.cl/alertas/8fph23-00830-01/</p>	Alerta de seguridad cibernética	8FPH23-00830-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	5 de junio de 2023	Última revisión	5 de junio de 2023
Alerta de seguridad cibernética	8FPH23-00830-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	5 de junio de 2023														
Última revisión	5 de junio de 2023														
	<p>CSIRT alerta de nueva campaña de phishing que suplanta a Cencosud Scotiabank</p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00831-01</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>5 de junio de 2023</td></tr> <tr><td>Última revisión</td><td>5 de junio de 2023</td></tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección https://bit[.]ly/3oFJDyb?l=www.tarjetacencosud.cl</p> <p>URL sitio falso https://mitarjetacencosud-cl.martinezlawaz[.]com/</p> <p>Dirección IP sitio falso [50.87.145.149]</p> <p>Enlace para revisar loC: https://www.csirt.gob.cl/alertas/8fph23-00831-01/</p>	Alerta de seguridad cibernética	8FPH23-00831-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	5 de junio de 2023	Última revisión	5 de junio de 2023
Alerta de seguridad cibernética	8FPH23-00831-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	5 de junio de 2023														
Última revisión	5 de junio de 2023														
	<p>CSIRT alerta ante nuevo sitio fraudulento que suplanta a BancoEstado</p> <table border="1"> <tr><td>Alerta de seguridad cibernética</td><td>8FPH23-00832-01</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>7 de junio de 2023</td></tr> <tr><td>Última revisión</td><td>7 de junio de 2023</td></tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección https://bit[.]ly/43roLty?l=www.bancoestado.cl http://amazon1234[.]com/banestado/cuenta-blje/</p> <p>URL sitio falso https://bancoestado-cl.malkcons[.]co.tz/1686152706/imagenes/_personas/home/default.asp</p> <p>Dirección IP sitio falso [192.185.74.77]</p> <p>Enlace para revisar loC: https://www.csirt.gob.cl/alertas/8fph23-00832-01/</p>	Alerta de seguridad cibernética	8FPH23-00832-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	7 de junio de 2023	Última revisión	7 de junio de 2023
Alerta de seguridad cibernética	8FPH23-00832-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	7 de junio de 2023														
Última revisión	7 de junio de 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://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

3. Malware

Imagen del Mensaje	CSIRT alerta de nueva campaña de phishing con malware, que suplanta al SII	
 <p>Factura no pagada, resuelve tu situación.</p> <p>SII - Servicio de Impuestos Internos <support@followthetroley.com></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>SII - Servicio de Impuestos Internos</p> <p>Estimado Contribuyente</p> <p>Nos estamos comunicando con usted a través del correo electrónico registrado en el sistema.</p> <p>Le informamos mediante este medio que hay una factura que se encuentra en estado de NO PAGADA. Le invitamos a regularizar esta situación a través del siguiente enlace.</p> <p>Por favor realice el pago lo más pronto posible, a fin de evitar las molestias de un cobro judicial, que pueda implicar embargo o suspensión temporal o definitiva depende el caso.</p> <p>Puede consultar el estado de su deuda actual mediante el siguiente enlace.</p> <p>FACTURA Acceso Regularizar</p> <p>Marzo - 2022 Consultar Factura abierta Regularizar situación</p> <p>(Para acceder al documento electrónico recuerde que la versión de este documento es únicamente para PC no funciona en dispositivos móviles.)</p> <p>Asegúrese de consultar su situación con SII para evitar problemas legales.</p> <p>Servicio de Impuestos Internos - 2023</p>	Alerta de seguridad cibernética	2CMV23-00417-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	8 de junio de 2023
	Última revisión	8 de junio de 2023
	Indicadores de compromiso	
	URL-Dominio	
	https://gscjgn[.]org/marzosiiifact/nopagada/Factsii/ https://cmg-technology[.]ro/zpNuevo/ 103.235.105[.]113 188.240.2[.]189 50.116.72.199 158.69.109.191 162.214.157.170	
SHA256		
203d8a6e596cad036eae854e7484509a11ee35547ca5e1f2b2249ae825ec714f3d5f0dbce1204d0db72b9574800bef878015fdbbe7b24dc5b553caed5da4dc5a6d2f67ddd2438baa14e2565e02e015296db31daf3d03410e7c783e89c785e6143d5f0dbce1204d0db72b9574800bef878015fdbbe7b24dc5b553caed5da4dc5af178861e00b0a2ba7d50c103ac41ac6eb89e7c6232bd25bd1fa8752a8871e4453d5f0dbce1204d0db72b9574800bef878015fdbbe7b24dc5b553caed5da4dc5a		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/alertas/2cmv23-00417-01/		

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>

4. Vulnerabilidades



CSIRT comparte vulnerabilidades parchadas en Android (patch level 2023-06-05)

Alerta de seguridad cibernética	9VSA23-00841-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de junio de 2023
Última revisión	6 de junio de 2023

CVE

CVE-2021-0701	CVE-2022-48390	CVE-2023-21131
CVE-2021-0945	CVE-2022-48391	CVE-2023-21135
CVE-2022-22060	CVE-2022-48392	CVE-2023-21136
CVE-2022-22706	CVE-2022-48438	CVE-2023-21137
CVE-2022-28349	CVE-2023-21095	CVE-2023-21138
CVE-2022-33251	CVE-2023-21101	CVE-2023-21139
CVE-2022-33257	CVE-2023-21105	CVE-2023-21141
CVE-2022-33264	CVE-2023-21108	CVE-2023-21142
CVE-2022-33292	CVE-2023-21115	CVE-2023-21143
CVE-2022-40516	CVE-2023-21120	CVE-2023-21144
CVE-2022-40517	CVE-2023-21121	CVE-2023-21628
CVE-2022-40520	CVE-2023-21122	CVE-2023-21656
CVE-2022-40521	CVE-2023-21123	CVE-2023-21657
CVE-2022-40523	CVE-2023-21124	CVE-2023-21658
CVE-2022-40529	CVE-2023-21126	CVE-2023-21659
CVE-2022-40533	CVE-2023-21127	CVE-2023-21661
CVE-2022-40536	CVE-2023-21128	CVE-2023-21669
CVE-2022-40538	CVE-2023-21129	CVE-2023-21670
CVE-2022-46781	CVE-2023-21130	

Fabricantes

Google

Productos afectados

Android 11, 12 y 13.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00841-01/>



CSIRT comparte información de vulnerabilidad día cero parchada en Google Chrome

Alerta de seguridad cibernética	9VSA23-00842-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de junio de 2023
Última revisión	6 de junio de 2023

CVE

CVE-2023-3079

Fabricante

Google

Productos afectados: Google Chrome

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00842-01/>

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.instagram.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00843-01
CSIRT comparte vulnerabilidades parchadas para Aria Operations for Networks

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl



CSIRT comparte vulnerabilidades parchadas por VMware para Aria Operations for Networks

Alerta de seguridad cibernética	9VSA23-00843-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de junio de 2023
Última revisión	7 de junio de 2023

CVE

CVE-2023-20887, CVE-2023-20888 y CVE-2023-20889

Fabricantes

VMware

Productos afectados

Aria Operations for Networks, antes conocido como vRealize Network Insight.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00843-01/>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00844-01
CSIRT comparte información de vulnerabilidad en Microsoft ISS que está siendo explotada

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl



CSIRT comparte información de vulnerabilidad en Microsoft ISS, que está siendo explotada

Alerta de seguridad cibernética	9VSA23-00844-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de junio de 2023
Última revisión	8 de junio de 2023

CVE

CVE-2023-34362

Fabricantes

Microsoft

Productos afectados

Microsoft ISS	MOVEit Transfer 2021.1.x
MOVEit Transfer 2023.0.0	MOVEit Transfer 2021.0.x
MOVEit Transfer 2022.1.x	MOVEit Transfer 2020.1.x
MOVEit Transfer 2022.0.x	MOVEit Transfer 2020.0.x

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00844-01/>

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 información de vulnerabilidades críticas parchadas por Cisco

Alerta de seguridad cibernética	9VSA23-00845-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de junio de 2023
Última revisión	8 de junio de 2023

CVE

CVE-2023-20105
CVE-2023-20192

Fabricantes

Cisco

Productos afectados

Cisco Expressway Series and Cisco TelePresence VCS.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00845-01/>

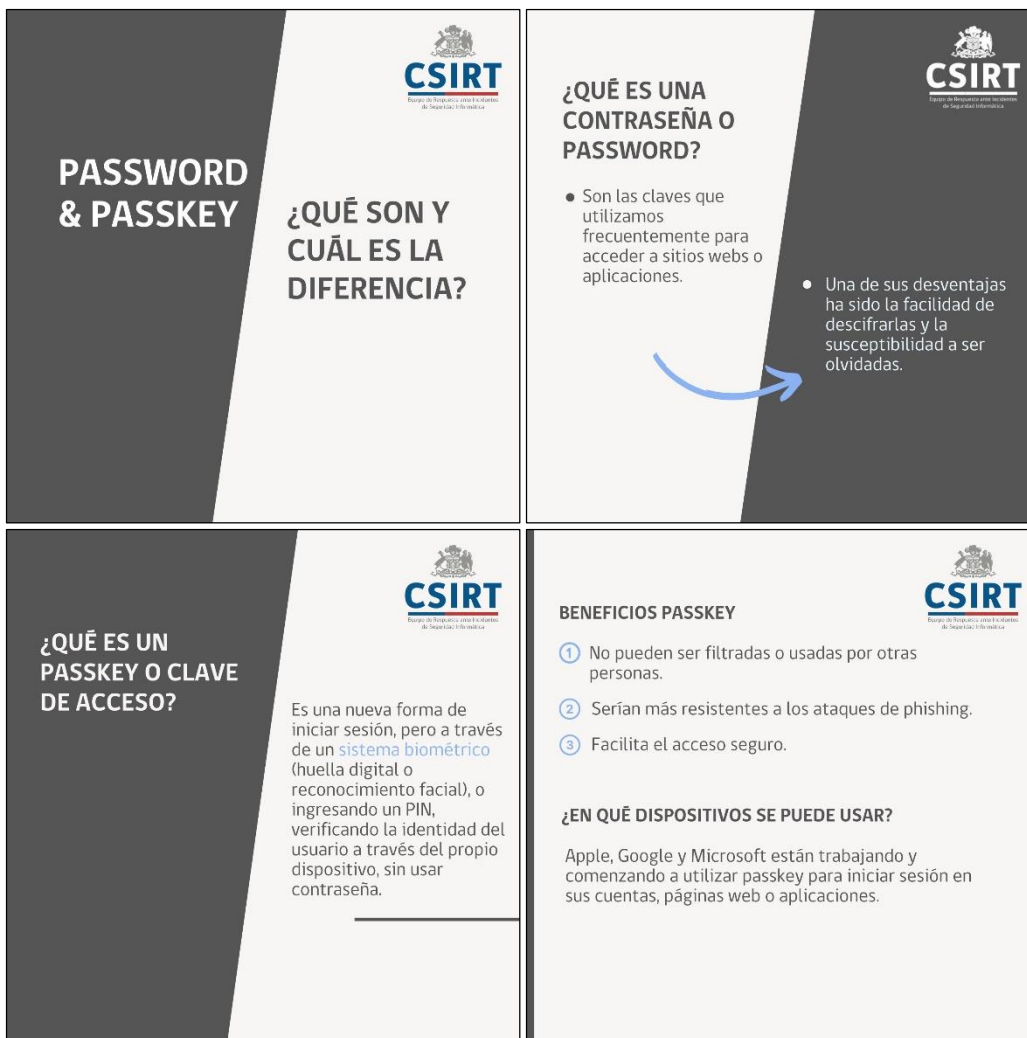
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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>

5. Concientización

Passkey y password

Grandes marcas están implementando los passkeys, una nueva forma de ingresar a sitios y cuentas sin contraseña. Publicamos la definición de passkey y su diferencia con una contraseña, aquí: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-passkeys/>



The infographic is divided into four quadrants, each with the CSIRT logo in the top right corner.

- Top Left:** Titled "PASSWORD & PASSKEY" and "¿QUÉ SON Y CUÁL ES LA DIFERENCIA?".
- Top Right:** Titled "¿QUÉ ES UNA CONTRASEÑA O PASSWORD?". It lists two points: "Son las claves que utilizamos frecuentemente para acceder a sitios webs o aplicaciones." and "Una de sus desventajas ha sido la facilidad de descifrarlas y la susceptibilidad a ser olvidadas." A blue arrow points from the first point to the second.
- Bottom Left:** Titled "¿QUÉ ES UN PASSKEY O CLAVE DE ACCESO?". It describes it as a new login method using biometric systems (digital fingerprint or facial recognition) or a PIN, verifying the user's identity through the device without a password.
- Bottom Right:** Titled "BENEFICIOS PASSKEY". It lists three benefits: "1 No pueden ser filtradas o usadas por otras personas.", "2 Serían más resistentes a los ataques de phishing.", and "3 Facilita el acceso seguro." Below this, it asks "¿EN QUÉ DISPOSITIVOS SE PUEDE USAR?" and states that Apple, Google, and Microsoft are working on using passkeys to start sessions on their accounts, websites, or applications.

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.

- María José Morales
- Carlos Araneda
- Paula Torres García
- Pablo Ignacio Pizarro Cortínez
- Diego Villalobos
- Bárbara Palacios Cabezas
- Roberto Carlos Arévalo Díaz
- Michel Díaz
- Exequiel Moisés Medina Parra
- Diego Javier González Figueroa
- Nora Moretti
- Cristóbal Ramón Herrera Jara
- Carlos David Escalona

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO