



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 194

SEMANA DEL 17 AL 23 DE MARZO 2023

INFORMACION IMPORTANTE

El CSIRT de Gobierno informa que debido a problemas técnicos no ha sido posible publicar las alertas de seguridad cibernéticas y campañas de concientización en nuestro sitio web.

Por lo tanto, los informes e indicadores de compromiso los podrán encontrar en el repositorio de GitHub del CSIRT de Gobierno: www.github.com/csirtcl

LA SEMANA EN CIFRAS

IP INFORMADAS

9

IP advertidas en múltiples campañas de phishing y de malware.



URL ADVERTIDAS

13

asociadas a sitios fraudulentos y campañas de phishing y malware



HASH REPORTADOS

8

asociadas a múltiples campañas de phishing con archivos que contienen malware



PARCHES COMPARTIDOS

36

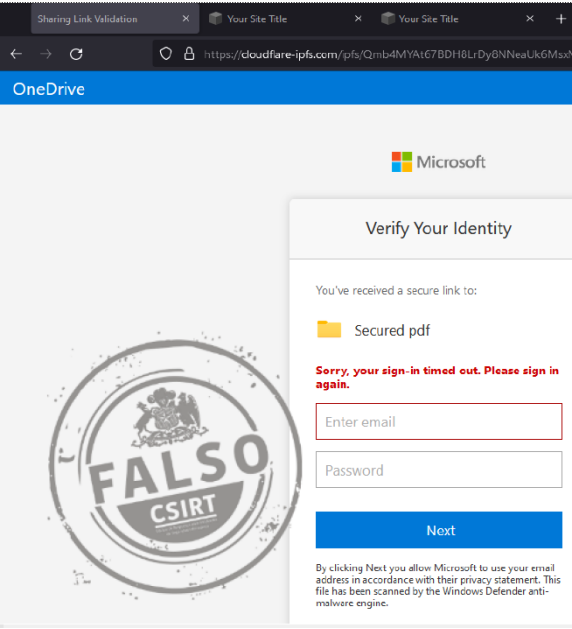
Las mitigaciones son útiles en productos de Adobe, SAP y Mozilla.

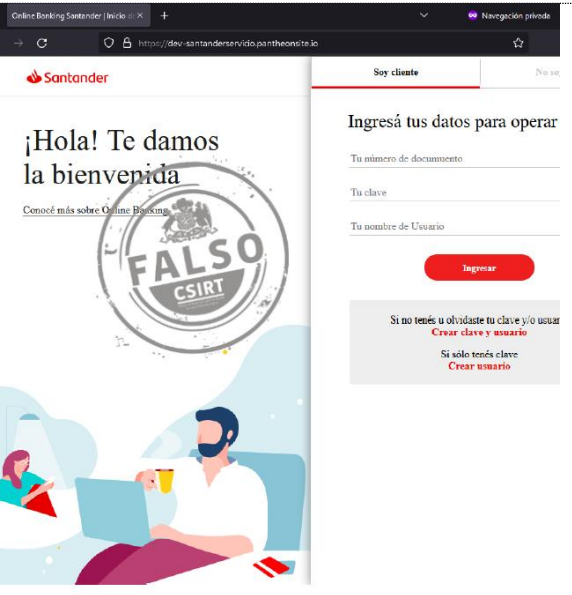


CONTENIDO

1.	Sitios fraudulentos	4
2.	Phishing	6
3.	Malware.....	7
4.	Vulnerabilidades	8
5.	Concientización.....	10
6.	Recomendaciones y buenas prácticas	12
7.	Muro de la Fama	13

1. Sitios fraudulentos

	<p>CSIRT advierte sitio que suplanta a Microsoft</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FFR23-01266-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Falsificación de Registros o Identidad</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>21 de marzo de 2023</td> </tr> <tr> <td>Última revisión</td> <td>21 de marzo de 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL sitio falso</p> <p>https://cloudflare-ipfs.com/pfs/Qmb4MYAt67BDH8LrDy8NNeaUk6MsxM6eqKAnq5KQrpM77V https://pufferfish-plums-7rn7.squarespace.com/ https://mandolin-bamboo-pj26.squarespace.com/ https://bobcat-hexagon-m62r.squarespace.com/ https://snobods.z13.web.core.windows.net/</p> <p>Dirección IP</p> <p>198.49.23[.]177 104.17.64[.]14 52.239.170[.]165</p> <p>Enlace para revisar IoC:</p> <p>https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01266-01.txt</p>	Alerta de seguridad cibernética	8FFR23-01266-01	Clase de alerta	Fraude	Tipo de incidente	Falsificación de Registros o Identidad	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	21 de marzo de 2023	Última revisión	21 de marzo de 2023
Alerta de seguridad cibernética	8FFR23-01266-01														
Clase de alerta	Fraude														
Tipo de incidente	Falsificación de Registros o Identidad														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	21 de marzo de 2023														
Última revisión	21 de marzo de 2023														

	<p>CSIRT alerta página web que suplanta a Santander</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FFR23-01267-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Falsificación de Registros o Identidad</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>22 de marzo de 2023</td> </tr> <tr> <td>Última revisión</td> <td>22 de marzo de 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL sitio falso</p> <p>https://dev-santanderservicio.pantheonsite.io/</p> <p>Dirección IP</p> <p>[23.185.0.4]</p> <p>Enlace para revisar IoC:</p> <p>https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01267-01.txt</p>	Alerta de seguridad cibernética	8FFR23-01267-01	Clase de alerta	Fraude	Tipo de incidente	Falsificación de Registros o Identidad	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	22 de marzo de 2023	Última revisión	22 de marzo de 2023
Alerta de seguridad cibernética	8FFR23-01267-01														
Clase de alerta	Fraude														
Tipo de incidente	Falsificación de Registros o Identidad														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	22 de marzo de 2023														
Última revisión	22 de marzo de 2023														

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO



CSIRT alerta página web que suplanta a CorreosChile

Alerta de seguridad cibernética	8FFR23-01268-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de marzo de 2023
Última revisión	22 de marzo de 2023

Indicadores de compromiso

URL sitio falso

[https://unsla\[.\]org/CorreosChili/app/index.php?&userid=32e8e16f1b2f304b1f5f19c1fca2b265&ue=ff4c2bab217bfbdafa7cdeaa10f0e9053](https://unsla[.]org/CorreosChili/app/index.php?&userid=32e8e16f1b2f304b1f5f19c1fca2b265&ue=ff4c2bab217bfbdafa7cdeaa10f0e9053)

Dirección IP

[190.92.141.191]

Enlace para revisar loC:

https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01268-01.txt



CSIRT advierte sitio que suplanta a Banco Falabella

Alerta de seguridad cibernética	8FFR23-01269-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de marzo de 2023
Última revisión	23 de marzo de 2023

Indicadores de compromiso

URL sitio falso

[https://marzo-gennials.firebaseio\[.\]com/online/plazo](https://marzo-gennials.firebaseio[.]com/online/plazo)

Dirección IP

[199.36.158.100]

Enlace para revisar loC:

https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01269-01.txt



CSIRT alerta de página web que suplanta a Banco Falabella

Alerta de seguridad cibernética	8FFR23-01270-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de marzo de 2023
Última revisión	23 de marzo de 2023

Indicadores de compromiso

URL sitio falso

[https://bonos-emergencia.firebaseio\[.\]com/acceso/plazo](https://bonos-emergencia.firebaseio[.]com/acceso/plazo)

Dirección IP

[199.36.158.100]

Enlace para revisar loC:

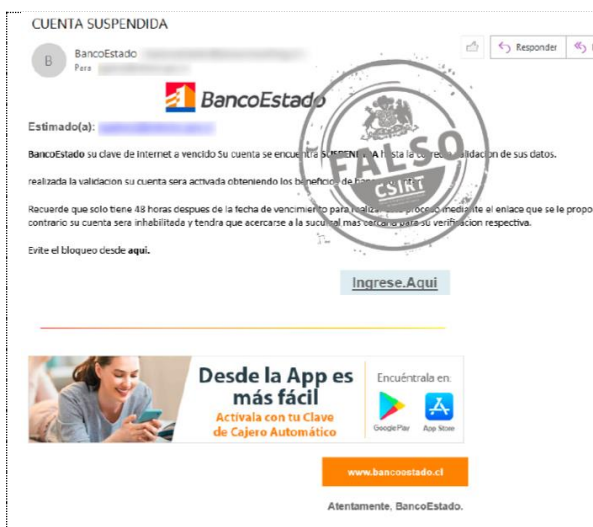
https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01270-01.txt

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

	<p>CSIRT alerta de campaña de phishing que suplanta a BancoEstado</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00776-01</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>21 de marzo de 2023</td> </tr> <tr> <td>Última revisión</td> <td>21 de marzo de 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección https://containd3structible[.]com/activacion/cuenta-ffca/</p> <p>URL sitio falso https://korinpatito[.]top/1679400178/imagenes/_personas/home/default.asp</p> <p>Dirección IP [172.67.164.157]</p> <p>Enlace para revisar IoC: https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00776-01.txt</p>	Alerta de seguridad cibernética	8FPH23-00776-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	21 de marzo de 2023	Última revisión	21 de marzo de 2023
Alerta de seguridad cibernética	8FPH23-00776-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	21 de marzo de 2023														
Última revisión	21 de marzo de 2023														

	<p>CSIRT alerta campaña de phishing que suplanta a BancoEstado</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00777-01</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>22 de marzo de 2023</td> </tr> <tr> <td>Última revisión</td> <td>22 de marzo de 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección https://mapacontact[.]com/activacion/cuenta-vnrp/</p> <p>URL sitio falso https://patitotravel[.]com/1679509523/imagenes/_personas/home/default.asp</p> <p>Dirección IP [138.128.182.130]</p> <p>Enlace para revisar IoC: https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00777-01.txt</p>	Alerta de seguridad cibernética	8FPH23-00777-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	22 de marzo de 2023	Última revisión	22 de marzo de 2023
Alerta de seguridad cibernética	8FPH23-00777-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	22 de marzo de 2023														
Última revisión	22 de marzo de 2023														

3. Malware

<p>3-Tercera_Notificación_Del_Proceso_Llevado_En_Contra_Referencia_Nro°_29873893_21_Radicado_#93903030...</p> <p>Para luisa.fernanda.sierra <luisa.9117.sierra@gmail.com></p> <p>NOTIFICACIÓN ELECTRÓNICA EN CURSO</p> <p>Estimado/a</p> <p>Señor(a)</p> <p>En atención a lo estipulado en el artículo segundo del Decreto 105 de 2011 y en cumplimiento de lo ordenado por el Juzgado 01 Penal - Me permito notificarle del fallo de primera instancia proferido en el curso de la acción de nulidad radicada con el código 8076.1058.137.2021</p> <p>DETALLES DEL PROCESO EN CURSO SENTENCIA Y OFICIO REMISORIO.</p> <p>CÓDIGO DE ACCESO AL ADJUNTO: 2525</p> <p>atentamente</p> <p>Contáctenos a nuestro PBX # 00174184 EXT 122.</p> 	<p>CSIRT advierte campaña de phishing con malware con falsa citación judicial</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>2CMV23-00406-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Malware</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>16 de marzo de 2023</td> </tr> <tr> <td>Última revisión</td> <td>16 de marzo de 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>Asunto</p> <p>3-Tercera_Notificación_Del_Proceso_Llevado_En_Contra_Referencia_Nro°_29873893_21_Radicado_#93903030-32</p> <p>Correo de Salida</p> <p>luisa.9117.sierra@gmail.com</p> <p>SHA256</p> <p>d94424e9b0a9bb26db36fa4c44633ca0a312c03da3c2354264029be85b1eb8300f25e73c85e2f183591d514636625fb5484b61ae309d5c3c3905cefbf29cce030f25e73c85e2f183591d514636625fb5484b61ae309d5c3c3905cefbf29cce03bdd02b6a38a5d23d1a4c96fd33623cd727b5b4e40f178e50b349910e19ef4757</p> <p>Enlace para revisar IoC:</p> <p>https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00406-01.txt</p>	Alerta de seguridad cibernética	2CMV23-00406-01	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	16 de marzo de 2023	Última revisión	16 de marzo de 2023
Alerta de seguridad cibernética	2CMV23-00406-01														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	16 de marzo de 2023														
Última revisión	16 de marzo de 2023														

<p>Aviso de Transferencia de fondos</p> <p>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>BancoChile Comprobante de pago INT_EMP221226.20230320_52763325.PDF.gz</p> <p>Banco de Chile</p> <p>AVISO DE TRANSFERENCIA DE FONDOS</p> <p>Estimado señor:</p> <p>Banco de Chile informa que el día de hoy 20/03/2023 se ha enviado una transferencia electrónica de fondos a su cuenta bancaria a pedido de nuestro cliente a través de banca por internet.</p> <p>Se adjunta el comprobante de pago número 34654880 para su confirmación.</p> <p>Si tiene alguna duda, puede ponerse en contacto con su cliente que ordenó el pago.</p> 	<p>CSIRT advierte campaña de phishing con malware que suplanta al Banco de Chile</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>2CMV23-00407-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Malware</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>21 de marzo de 2023</td> </tr> <tr> <td>Última revisión</td> <td>21 de marzo de 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>Asunto</p> <p>Aviso de Transferencia de fondos</p> <p>Correo de Salida</p> <p>167933736637.9248.5108207612344084682@divabercom01.vdeploy.net</p> <p>SHA256</p> <p>7f9c328cddd0b8593519310ba0ff155312934c068cca6727fb8422762c7ef6116fef888e6f662744463a37949ee1df183c279e42baf355319484293748ded41bad475a285edf2aa6ff28b845bb29f7bb0da366e5bf8ba1f4ad25ec4a16c440dc96ad1146eb96877eab5942ae0736b82d8b5e2039a80d3d6932665c1a4c87dcf7</p> <p>Enlace para revisar IoC:</p> <p>https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00407-01.txt</p>	Alerta de seguridad cibernética	2CMV23-00407-01	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	21 de marzo de 2023	Última revisión	21 de marzo de 2023
Alerta de seguridad cibernética	2CMV23-00407-01														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	21 de marzo de 2023														
Última revisión	21 de marzo de 2023														

4. Vulnerabilidades



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00804-01
CSIRT comparte vulnerabilidades en varios productos de SAP

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



CSIRT alerta de vulnerabilidad crítica en productos de SAP

Alerta de seguridad cibernética	9VSA23-00804-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	17 de marzo de 2023
Última revisión	17 de marzo de 2023

CVE

CVE-2023-25616	CVE-2023-26459	CVE-2023-27894
CVE-2023-25617	CVE-2023-27498	CVE-2023-26457
CVE-2023-23857	CVE-2023-26461	CVE-2023-27895
CVE-2023-27269	CVE-2023-25615	CVE-2023-0021
CVE-2023-27500	CVE-2023-27270	CVE-2023-27268
CVE-2023-27893	CVE-2023-27271	CVE-2023-26460
CVE-2023-27501	CVE-2023-27896	

Fabricantes

SAP

Productos afectados

SAP Business Objects Business Intelligence Platform (CMC), versiones 420, 430
SAP NetWeaver AS for Java, versión 7.50.
SAP NetWeaver Application Server para ABAP y ABAP Platform, versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791.
SAP NetWeaver Application Server para ABAP y ABAP Platform (SAPRSBRO Program), versiones 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791.
SAP Business Objects (Adaptive Job Server), versiones 420, 430.

Enlaces para revisar el informe:

<https://github.com/csirtcl/Vulnerabilidades/blob/main/9VSA23-00804-01.pdf>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00805-01
CSIRT comparte vulnerabilidades en Adobe ColdFusion

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



CSIRT alerta de vulnerabilidades en Adobe ColdFusion

Alerta de seguridad cibernética	9VSA23-00805-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	17 de marzo de 2023
Última revisión	17 de marzo de 2023

CVE

CVE-2023-26359
CVE-2023-26360
CVE-2023-26361

Fabricantes

Adobe

Productos afectados

ColdFusion 2018 Update 15 y anteriores versiones.
ColdFusion 2021 Update 5 y versiones anteriores.

Enlaces para revisar el informe:





<https://github.com/csirtcl/Vulnerabilidades/blob/main/9VSA23-00805-01.pdf>

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>

 <p>INFORME DE Vulnerabilidad</p> <p>9VSA23-00806-01 CSIRT comparte vulnerabilidades parchadas en Mozilla Firefox 111</p> <p>PARA REGISTRAR 15 10 UN INCIDENTE www.csirt.gob.cl</p> 	CSIRT alerta de vulnerabilidades parchadas en Mozilla Firefox 111		
	Alerta de seguridad cibernética	9VSA23-00806-01	
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Crítico		
TLP	Blanco		
Fecha de lanzamiento original	23 de marzo de 2023		
Última revisión	23 de marzo de 2023		
CVE			
CVE-2023-28159	CVE-2023-28160	CVE-2023-25752	
CVE-2023-25748	CVE-2023-28164	CVE-2023-28163	
CVE-2023-25749	CVE-2023-28161	CVE-2023-28176	
CVE-2023-25750	CVE-2023-28162	CVE-2023-28177	
CVE-2023-25751			
Fabricantes			
Mozilla			
Productos afectados			
Firefox Firefox for Android			
Enlaces para revisar el informe:			
https://github.com/csirtcl/Vulnerabilidades/blob/main/9VSA23-00806-01.pdf			

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>

5. Concientización

Simulación de ataque cibernético en tiempo real realizada por Microsoft y el CSIRT de Gobierno

Hoy viernes 24 de marzo tuvo lugar en el Edificio Moneda Bicentenario, sede del CSIRT de Gobierno, una actividad realizada en conjunto con Microsoft, en la cual presentamos la situación de una empresa que está sufriendo un ciberataque, mostrando los pasos y decisiones que toman diferentes áreas de la compañía y presentando a debate de los invitados estas acciones, consultándoles qué harían en su lugar, con lo que se logra una edificante conversación sobre ciberseguridad.

La instancia contó con las palabras de bienvenida de Ingrid Inda, jefa de la División de Redes y Seguridad Informática de la Subsecretaría del Interior, Carlos Silva, jefe del CSIRT de Gobierno, y María Francisca Yáñez, National Technology Officer en Microsoft Chile.



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>

Video explicativo para identificar un sitio fraudulento con suplantación

Publicamos en nuestras cuentas de Instagram y Twitter un video que muestra cómo identificar un sitio malicioso que suplanta a una empresa conocida fijandose en su URL, llamando a tener cuidado y fijarnos en este dato antes de interactuar con una página de internet.

Twitter: <https://twitter.com/CSIRTConciencia/status/1638529239430447106?s=20>

Instagram: <https://www.instagram.com/reel/CqEH2KVABic/?igshid=YmMyMTA2M2Y>




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>

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://twitter.com/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.

- Manuel Eduardo Muñoz Contreras
- Pablo Meneses
- Francisco Javier Gutiérrez
- Rodrigo González Azolas
- Cristián Casanova Rivera
- Ernesto Alonso Riquelme Arroyo
- María José Lorca Ugalde
- Francisco Aravena

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO