



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 245

semana del 8 al 14 de marzo de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

2

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

3

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

111

Las mitigaciones son útiles en productos de Microsoft, Adobe, QNAP, Fortinet, SAP y Kubernetes.



HASH REPORTADOS

1

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



CONTENIDO

1. Phishing	3
2. Sitios fraudulentos.....	4
3. Vulnerabilidades.....	5
4. Malware.....	10
5. Noticias y concientización.....	11
6. Recomendaciones y buenas prácticas	12
7. Muro de la Fama	13


Boletín de Ciberseguridad N° 245

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



BOLETÍN 13BCS24-00254-01 | Semana del 8 de 14 de marzo de 2024

1. Phishing

<p>Acción requerida: Último recordatorio cccmarin/Último recordatorio 3/11/2024</p> <p> Para S-e-c-u-r-e-Interior <orochoa@yotateam.com.ni></p> <p><small>Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.</small></p> <p>Interior Notificación de entradas.</p> <p>Su contraseña para su cuenta Interior vence hoy 3/11/2024:</p> <p>Haga clic en el botón para conservar su inicio de sesión actual.</p> <p>MANTENERSE CON LA CONTRASEÑA ACTUAL</p> <p>La cuenta se bloqueará después de 24 horas.</p> <p>Ignore este mensaje si ya ha confirmado la solicitud anteriormente.</p>	<p>CSIRT alerta de campaña de phishing sobre falsa caducidad de cuenta de correo</p> <table border="1"><tr><td>Código de alerta</td><td>8FPH24-00939-01</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>12 de marzo, 2024</td></tr><tr><td>Última revisión</td><td>12 de marzo, 2024</td></tr></table> <p>Indicadores de compromiso</p> <p>URL del sitio falso https://careclub.or[.]ke/zti/#{correo}</p> <p>URL de redirección https://www.google[.]is/amp/s/be%E3%80%82co%E3%80%82mz%2Fsgn%2F/K3YMYGVJ_224487825%2FY2NtYXJpbkBpbnRlcmVci5nb2luY2w= https://be.co[.]mz/sgn//K3YMYGVJ_224487825/Y2NtYXJpbkBpbnRlcmVci5nb2luY2w=</p> <p>Dirección IP sitio falso [192.185.129.195]</p> <p>Enlace para revisar loC: https://csirt.gob.cl/alertas/8fph24-00939-01/</p>	Código de alerta	8FPH24-00939-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	12 de marzo, 2024	Última revisión	12 de marzo, 2024
Código de alerta	8FPH24-00939-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	12 de marzo, 2024														
Última revisión	12 de marzo, 2024														

CONTACTO Y REDES SOCIALES CSIRT

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

2. Sitios fraudulentos



CSIRT advierte nuevo sitio falso que suplanta a Amazon

Código de alerta	8FFR24-01663-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de marzo, 2024
Última revisión	11 de marzo, 2024

Indicadores de compromiso

URL del sitio falso

[https://www.de.pilladoempresas\[.\]cl/amzn_login.php?](https://www.de.pilladoempresas[.]cl/amzn_login.php?)

Dirección IP sitio falso

[186.64.119.85]

Enlace para revisar loC:

<https://csirt.gob.cl/alertas/8ffr24-01663-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

3. Vulnerabilidades



CSIRT comparte vulnerabilidades que afecta a QNAP

Código de alerta	9VSA24-00982-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 marzo, 2024
Última revisión	12 marzo, 2024

CVE

CVE-2024-21899
 CVE-2024-21900
 CVE-2024-21901

Fabricante

QNAP

Productos afectados

QTS 5.1.x
 QTS 4.5.x
 QuTS hero h5.1.x
 QuTS hero h4.5.x
 QuTScloud c5.x
 miQNAPcloud 1.0.x

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00982-01/>



CSIRT comparte vulnerabilidades parchadas en el Update Tuesday de Microsoft para marzo 2024

Código de alerta	9VSA24-00983-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 marzo, 2024
Última revisión	12 marzo, 2024

CVE

CVE-2024-26190	CVE-2024-21448	CVE-2024-21400	CVE-2024-26160
CVE-2024-21430	CVE-2024-21392	CVE-2024-26164	CVE-2024-26159
CVE-2023-28746	CVE-2024-21442	CVE-2024-26201	CVE-2024-21450
CVE-2024-26174	CVE-2024-21441	CVE-2024-26198	CVE-2024-21446
CVE-2024-26170	CVE-2024-21439	CVE-2024-26199	CVE-2024-21445
CVE-2024-26197	CVE-2024-21438	CVE-2024-26185	CVE-2024-21444
CVE-2024-21451	CVE-2024-21437	CVE-2024-26182	CVE-2024-21440
CVE-2024-21443	CVE-2024-21435	CVE-2024-26181	CVE-2024-21436
CVE-2024-21418	CVE-2024-21434	CVE-2024-26178	CVE-2024-21432
CVE-2024-21330	CVE-2024-21433	CVE-2024-26177	CVE-2024-21431
CVE-2024-26165	CVE-2024-21429	CVE-2024-26176	CVE-2024-21427
CVE-2024-21411	CVE-2024-21426	CVE-2024-26173	CVE-2024-21421
CVE-2024-26161	CVE-2024-21419	CVE-2024-26169	CVE-2024-21408
CVE-2024-26204	CVE-2024-21334	CVE-2024-26166	CVE-2024-21407
CVE-2024-26203	CVE-2024-21390	CVE-2024-26162	CVE-2024-20671

Fabricante

CONTACTO Y REDES SOCIALES CSIRT

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

	<p>Microsoft</p> <p>Productos afectados</p> <p>.NET 7.0 .NET 8.0 Azure Automation Azure Automation Update Management Azure Data Studio Azure Kubernetes Service Confidential Containers Azure SDK Azure Security Center Azure Sentinel Container Monitoring Solution Intune Company Portal for Android Log Analytics Agent Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Authenticator Microsoft Dynamics 365 (on-premises) version 9.1 Microsoft Exchange Server 2016 Cumulative Update 23 Microsoft Exchange Server 2019 Cumulative Update 13 Microsoft Exchange Server 2019 Cumulative Update 14 Microsoft Outlook for Android Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019 Microsoft SharePoint Server Subscription Edition Microsoft Teams for Android Microsoft Visual Studio 2022 version 17.4 Microsoft Visual Studio 2022 version 17.6 Microsoft Visual Studio 2022 version 17.8 Microsoft Visual Studio 2022 version 17.9 Open Management Infrastructure Operations Management Suite Agent for Linux (OMS) Skype for Consumer Software for Open Networking in the Cloud (SONiC) 201811 Software for Open Networking in the Cloud (SONiC) 201911 Software for Open Networking in the Cloud (SONiC) 202012 Software for Open Networking in the Cloud (SONiC) 202205 SQL Server backend for Django System Center Operations Manager (SCOM) 2019 System Center Operations Manager (SCOM) 2022 Visual Studio Code Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems</p>
--	---

CONTACTO Y REDES SOCIALES CSIRT

Windows 11 Version 22H2 for ARM64-based Systems
 Windows 11 Version 22H2 for x64-based Systems
 Windows 11 Version 23H2 for ARM64-based Systems
 Windows 11 Version 23H2 for x64-based Systems
 Windows Defender Antimalware Platform
 Windows Server 2008 for 32-bit Systems Service Pack 2
 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
 Windows Server 2008 for x64-based Systems Service Pack 2
 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
 Windows Server 2008 R2 for x64-based Systems Service Pack 1
 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
 Windows Server 2012
 Windows Server 2012 (Server Core installation)
 Windows Server 2012 R2
 Windows Server 2012 R2 (Server Core installation)
 Windows Server 2016
 Windows Server 2016 (Server Core installation)
 Windows Server 2019
 Windows Server 2019 (Server Core installation)
 Windows Server 2022
 Windows Server 2022 (Server Core installation)
 Windows Server 2022, 23H2 Edition (Server Core installation)

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00983-01/>



CSIRT comparte información de vulnerabilidades parchadas por Fortinet para FortiOS y FortiProxy

Código de alerta	9VSA24-00984-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 marzo, 2024
Última revisión	13 marzo, 2024

CVE

CVE-2023-42789	CVE-2023-42790	CVE-2024-23112	CVE-2023-46717
----------------	----------------	----------------	----------------

Fabricante

Fortinet

Productos afectados

FortiOS versiones 7.4.0 a 7.4.1
 FortiOS versiones 7.2.0 a 7.2.5
 FortiOS versiones 7.0.0 a 7.0.12
 FortiOS versiones 6.4.0 a 6.4.14
 FortiOS versiones 6.2.0 a 6.2.15
 FortiProxy versiones 7.4.0
 FortiProxy versiones 7.2.0 a 7.2.6
 FortiProxy versiones 7.0.0 a 7.0.12
 FortiProxy versiones 2.0.0 a 2.0.13

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00984-01/>

CONTACTO Y REDES SOCIALES CSIRT

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



INFORME DE Vulnerabilidad

9VSA24-00985-01
 CSIRT comparte vulnerabilidades parchadas en el SAP Security Patch Day marzo de 2024

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

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte vulnerabilidades parchadas por SAP en su Patch Day de marzo 2024			
Código de alerta	9VSA24-00985-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	13 marzo, 2024		
Última revisión	13 marzo, 2024		
CVE			
CVE-2019-10744	CVE-2023-44487	CVE-2024-27902	CVE-2024-25645
CVE-2024-22127	CVE-2023-50164	CVE-2024-25644	CVE-2024-27900
CVE-2023-39439	CVE-2024-22133	CVE-2024-28163	
Fabricante			
SAP			
Productos afectados			
SAP Business Client, Versions – 6.5, 7.0, 7.70			
SAP Build Apps, Versions < 4.9.145			
SAP NetWeaver AS Java (Administrator Log Viewer plug-in), Version – 7.50			
SAP Commerce, Versions – HY_COM 2105, HY_COM 2205, COM_CLOUD 2211			
SAP HANA Database, Version – 2.0			
SAP HANA Extended Application Services Advanced (XS Advanced), Version – 1.0			
SAP BusinessObjects Business Intelligence Platform (Central Management Console), Versions – 4.3			
SAP NetWeaver AS ABAP applications based on SAPGUI for HTML (WebGUI), Versions – 7.89, 7.93			
NetWeaver (WSRM), Versions – 7.50			
SAP NetWeaver (Enterprise Portal), Version – 7.50			
SAP NetWeaver Process Integration (Support Web Pages), Versions – 7.50			
SAP Fiori Front End Server, Version – 605			
SAP ABAP Platform, Versions – 758, 795			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00985-01/			



INFORME DE Vulnerabilidad

9VSA24-00986-01
 CSIRT informa vulnerabilidades parchadas por Adobe en su Patch Tuesday marzo '24

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

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT informa vulnerabilidades parchadas en Patch Tuesday de Adobe para marzo 2024			
Código de alerta	9VSA24-00986-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	14 marzo, 2024		
Última revisión	14 marzo, 2024		
CVE			
CVE-2024-26028	CVE-2024-26044	CVE-2024-26067	CVE-2024-26118
CVE-2024-26030	CVE-2024-26045	CVE-2024-26069	CVE-2024-26119
CVE-2024-26031	CVE-2024-26048	CVE-2024-26073	CVE-2024-26120
CVE-2024-26032	CVE-2024-26050	CVE-2024-26080	CVE-2024-26124
CVE-2024-26033	CVE-2024-26052	CVE-2024-26094	CVE-2024-26125
CVE-2024-26034	CVE-2024-26056	CVE-2024-26096	CVE-2024-20760
CVE-2024-26035	CVE-2024-26059	CVE-2024-26102	CVE-2024-20768
CVE-2024-26038	CVE-2024-26061	CVE-2024-26103	CVE-2024-26126
CVE-2024-26040	CVE-2024-26062	CVE-2024-26104	CVE-2024-26127
CVE-2024-26041	CVE-2024-26063	CVE-2024-26105	CVE-2024-26051

CONTACTO Y REDES SOCIALES CSIRT

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

Boletín de Ciberseguridad N° 245

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



BOLETÍN 13BCS24-00254-01 | Semana del 8 de 14 de marzo de 2024


CVE-2024-26042	CVE-2024-26064	CVE-2024-26106	CVE-2024-20767
CVE-2024-26043	CVE-2024-26065	CVE-2024-26107	
Fabricante			
Adobe			
Productos afectados			
ColdFusion 2023 Update 6 y anteriores. ColdFusion 2021 Update 12 y anteriores. Adobe Experience Manager (AEM) AEM Cloud Service (CS). Adobe Experience Manager (AEM) 6.5.19.0 y anteriores.			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00986-01/			

	CSIRT informa de vulnerabilidad que afecta a Kubernetes	
	Código de alerta	9VSA24-00987-01
	Clase de alerta	Vulnerabilidad
	Tipo de incidente	Sistema y/o Software Abierto
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	14 marzo, 2024
	Última revisión	14 marzo, 2024
	CVE	
	CVE-2023-5528	
Fabricante		
Kubernetes		
Productos afectados		
kubelet		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa24-00987-01/		

CONTACTO Y REDES SOCIALES CSIRT

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

4. Malware

<p>Re: Envío OC - PO 4500628950 Confirmar recepción</p> <p>Mai G. Santana Gutiérrez <info@araprinter.es> Para PO-4500628950.xls 38 KB</p> <p>ADVERTENCIA: REMITENTE EXTERNO</p> <p>El remitente de este correo, es externo al Ministerio del Interior y Seguridad Pública. Si no tiene certeza de su origen, por seguridad, NO abra pasando el cursor sobre éste). Ante sospechas o dudas, reporte a la mesa de ayuda.</p> <p>Buen Día,</p> <p>Adjunto nuestra referencia de orden de compra firmada para su empresa.</p> <p>Es imprescindible confirmar y aceptar la Orden de Compra de referencia por este mismo medio en un plazo NO mayor a 48 horas, indicados en la misma.</p> <p>Esperamos su confirmación con su factura proforma lo antes posible.</p> <p>Saludos.</p> 	<h3>CSIRT advierte phishing con malware con un falso pago</h3> <table border="1"><tr><td>Código de alerta</td><td>2CMV24-00450-01</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>11 de marzo, 2024</td></tr><tr><td>Última revisión</td><td>11 de marzo, 2024</td></tr></table> <h3>Indicadores de compromiso</h3> <p>SHA256</p> <pre>e645209c1eb6e2bdb67197d8b8b4e72bcf12dcd76cc7008caf3dc11d80d60231d9 e3a591c7151aeefe18a1d1c36ca895c7e91979ff491bfd7b629d4e5f4d1c89 7d1a180a18af5266c0e996e4cb16556dcd9d421e7567853d10b3e83b24ac5525 4fb683b54680e47990aafcdffbec12fcf9ed6f4b5a02609dc79cb4ac1a223d8b 9952330e3ecc4fe4aa3888e406499d44602d12c4ad029d75c4499a8edc4bfc83 78d5d3cab432a0a71ca0895155e0d7e909edc256ce81d16d109e91e42780296b c5f3007ae1d9b7804118e930eb0b1a494ba7905f74c325ebaaa7f6844833365f</pre> <p>Enlace para revisar loC:</p> <p>https://www.csirt.gob.cl/alertas/2cmv24-00450-01/</p>	Código de alerta	2CMV24-00450-01	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	11 de marzo, 2024	Última revisión	11 de marzo, 2024
Código de alerta	2CMV24-00450-01														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	11 de marzo, 2024														
Última revisión	11 de marzo, 2024														

CONTACTO Y REDES SOCIALES CSIRT

5. Noticias y concientización

Día Internacional de la Mujer | Cómo evitar la violencia digital

Consejos para protegernos de la violencia digital, en los cuales también identificamos las principales amenazas contra las mujeres en internet. Disponibles también aquí: <https://csirt.gob.cl/recomendaciones/dia-internacional-de-la-mujer-2/>.



**CIBERCONSEJOS
CÓMO EVITAR LA
VIOLENCIA DIGITAL**

La violencia digital hacia las mujeres es una forma de violencia de género que se manifiesta a través de internet, redes sociales, correo electrónico o alguna otra plataforma en línea.

Formas de violencia

- **Revenge porn:** Amenaza de compartir o publicar imágenes o videos íntimos.
- **Ciberacoso:** Acoso, hostigamiento o humillación de una persona a través de medios digitales.
- **Doxing:** Publicación de información personal en internet, sin consentimiento, con el objetivo de exponer a riesgos, vergüenza o daño a una persona.
- **Ciberacecho:** Vigilancia o seguimiento reiterado a través de internet, incluyendo el uso de localización en tiempo real u otros métodos para controlar y asustar.

Cómo protegerse:

- Configura la privacidad en tus redes sociales para controlar quién puede ver o compartir tu información.
- Nunca compartas tus contraseñas, ni siquiera a tus amigos o pareja.
- No publiques tu ubicación en las redes sociales.
- Denuncia en la plataforma digital o red social en la que se está realizando la violencia.
- En caso de ser víctima de violencia digital, guarda la prueba de la violencia, acoso, amenaza o abuso y realiza la denuncia a la PDI.

CONTACTO Y REDES SOCIALES CSIRT

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

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.

- | | |
|--------------------------------|----------------|
| • Adolfo Estefanor Olave Arias | Suplantación |
| • David Soto | Vulnerabilidad |
| • Alonso Villalobos Gonzalez | Vulnerabilidad |

CONTACTO Y REDES SOCIALES CSIRT