



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 188

SEMANA DEL 3 AL 9 de FEBRERO 2023

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

8

Las mitigaciones son útiles en productos de Cisco, Atlassian, F5, Open SSH y Open SSL.



IP INFORMADAS

6

Listado de IP advertidas en múltiples campañas de phishing y de malware.



URL ADVERTIDAS

12

Asociadas a sitios fraudulentos y campañas de phishing y malware



HASH REPORTADOS

9

Asociadas a múltiples campañas de phishing con archivos que contienen malware



CONTENIDO

1.	Sitios fraudulentos.....	3
2.	Phishing.....	4
3.	Malware	7
4.	Vulnerabilidades.....	8
5.	Concientización	11
6.	Recomendaciones y buenas prácticas	14
7.	Muro de la Fama	15



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

1. Sitios fraudulentos

Imagen del sitio



CSIRT alerta ante página fraudulenta que suplanta a BancoEstado

Alerta de seguridad cibernética	8FFR23-01206-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de febrero de 2023
Última revisión	8 de febrero de 2023

Indicadores de compromiso

URL sitio falso

[https://ahorros-banestado.web\[.\]app/WqTvcFQDmpdBcgzG/url?source=usg&ref_=pgqoldiikl2](https://ahorros-banestado.web[.]app/WqTvcFQDmpdBcgzG/url?source=usg&ref_=pgqoldiikl2)

Dirección IP

[199.36.158.100]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01206-01/>

<https://www.csirt.gob.cl/media/2023/02/8FFR23-01206-01.pdf>

2. Phishing

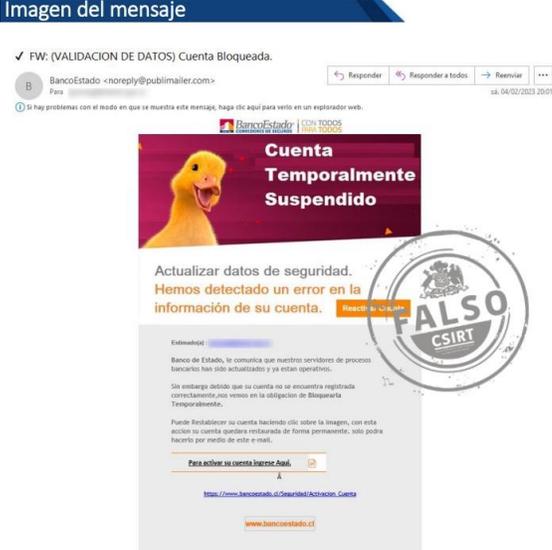
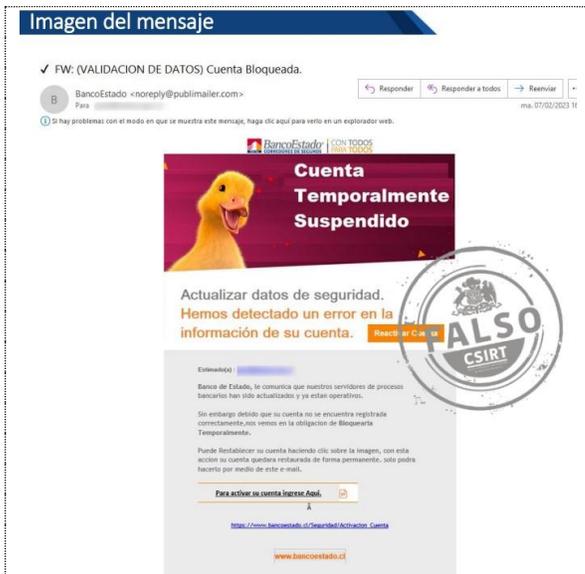
Imagen del mensaje		CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado			
		Alerta de seguridad cibernética	8FPH23-00740-01		
		Clase de alerta	Fraude		
		Tipo de incidente	Phishing		
		Nivel de riesgo	Alto		
		TLP	Blanco		
		Fecha de lanzamiento original	6 de febrero de 2023		
		Última revisión	6 de febrero de 2023		
		Indicadores de compromiso			
		URL redirección		https://ucmstudio[.]info/activacion/cuenta-vbvq/	
		URL sitio falso		https://smsrstado[.]site/1675687283/imagenes/_personas/home/default.asp	
Dirección IP		[202.89.39.41]			
Enlaces para revisar el informe:		https://www.csirt.gob.cl/alertas/8fph23-00740-01/			
		https://www.csirt.gob.cl/media/2023/02/8FPH23-00740-01.pdf			

Imagen del mensaje		CSIRT alerta de nueva campaña de phishing que suplanta a la Superintendencia de Pensiones			
		Alerta de seguridad cibernética	8FPH23-00741-01		
		Clase de alerta	Fraude		
		Tipo de incidente	Phishing		
		Nivel de riesgo	Alto		
		TLP	Blanco		
		Fecha de lanzamiento original	6 de febrero de 2023		
		Última revisión	6 de febrero de 2023		
		Indicadores de compromiso			
		URL redirección		https://retiro10[.]click/?23HaAdZgVeRoAJHr3WEtcnQnzsYD5A3HX6Kij9UH	
		URL sitio falso		https://www.sxconstructions.com[.]au/wp-content/img2/?ew98yfe8w7fhewiugfghpesr78gerhi	
Dirección IP		[173.254.29.24]			
Enlaces para revisar el informe:		https://www.csirt.gob.cl/alertas/8fph23-00741-01/			
		https://www.csirt.gob.cl/media/2023/02/8FPH23-00741-01.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>



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH23-00742-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de febrero de 2023
Última revisión	7 de febrero de 2023

Indicadores de compromiso

URL redirección

[https://ucmstudio\[.\]info/activacion/cuenta-vbvq/](https://ucmstudio[.]info/activacion/cuenta-vbvq/)

URL sitio falso

[https://smsrstado\[.\]site/1675798784/imagenes/_personas/home/default.asp](https://smsrstado[.]site/1675798784/imagenes/_personas/home/default.asp)

Dirección IP

[202.89.39.41]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph23-00742-01/>

<https://www.csirt.gob.cl/media/2023/02/8FPH23-00742-01.pdf>



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

Alerta de seguridad cibernética	8FPH23-00743-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de febrero de 2023
Última revisión	9 de febrero de 2023

Indicadores de compromiso

URL redirección

[https://bit\[.\]ly/3HNSJhA?l=www.bancoripley.cl](https://bit[.]ly/3HNSJhA?l=www.bancoripley.cl)

[https://sam-tech\[.\]jpp/bancoripley/cuenta-zrgq/](https://sam-tech[.]jpp/bancoripley/cuenta-zrgq/)

URL sitio falso

[https://web.bancoripley.cl.latintopjobspanama\[.\]com/1675945406/login](https://web.bancoripley.cl.latintopjobspanama[.]com/1675945406/login)

Dirección IP

[50.28.39.119]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph23-00743-01/>

<https://www.csirt.gob.cl/media/2023/02/8FPH23-00743-01.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>

Imagen del mensaje



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado con falso crédito Fogape

Alerta de seguridad cibernética	8FPH23-00744-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de febrero de 2023
Última revisión	9 de febrero de 2023

Indicadores de compromiso

URL redirección

[https://ucmstudio\[.\]info/activacion/cuenta-kzho/](https://ucmstudio[.]info/activacion/cuenta-kzho/)

URL sitio falso

[https://fogapestables\[.\]store/1675949342/imagenes/_personas/home/default.asp](https://fogapestables[.]store/1675949342/imagenes/_personas/home/default.asp)

Dirección IP

[202.89.39.2]

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph23-00744-01/>

<https://www.csirt.gob.cl/media/2023/02/8FPH23-00744-01.pdf>

3. Malware

Imagen del mensaje

Solicitud de retiro 10% AFP iniciado.

Notificaciones <retiros@mail.spensiones.cl>

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Detalle_Retiro_78047.html



CSIRT alerta de campaña de phishing con malware, que suplanta a la Superintendencia de Pensiones

Alerta de seguridad cibernética	2CMV23-00399-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de febrero de 2023
Última revisión	6 de febrero de 2023

Indicadores de compromiso

Asunto

Solicitud de retiro 10% AFP iniciado.

Correo de Salida

retiros@mail.spensiones.cl

SHA256

082d50bdaa7400e1e9c1e4c38e7c854ee28f03ec7fe8b9db36e0b60fd0bb06ee8f9
bfff6c9819040a6ebe473017a84640bd365c219559c0e416162f2b33ee9bef
ee70262f3d132d4b7b0475f1e8f865ae0eae4c5c45f79e7db9d33ab01fb90278
b3ce811fb696b94f9117ee7fe725ae6b907d695636beceeb1672d5d5eeb81df4
09c938d64248a8ddd18b5e1cea2c7376a3f5caa967bc760050ce84617c0587c2
6af0c5267d221d7972611ded914ede25d188d046278aceb94d9ada0ff87de153
de1c86d0d942570fbd63ac3dcd2e397cf0df0a677abc01588a6e9a2591e07ad6
d6fbabfea8eeecd4436d5de5113e057215f7f31e1725aedc1fb125e086d63e2d
98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv23-00399-01/>

<https://www.csirt.gob.cl/media/2023/02/2CMV23-00399-01.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>

4. Vulnerabilidades



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00781-01
CSIRT informa vulnerabilidades en Jira Service Management, de Atlassian

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



CSIRT alerta de vulnerabilidad crítica en Atlassian Jira Service Management

Alerta de seguridad cibernética	9VSA23-00781-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	3 de febrero de 2023
Última revisión	3 de febrero de 2023

CVE

CVE-2023-22501

Fabricantes

Atlassian

Productos afectados

Jira Service Management Server y Data Center 5.3.0, 5.3.1, 5.3.2, 5.4.0, 5.4.1, 5.5.0.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00781-01/>
<https://www.csirt.gob.cl/media/2023/02/9VSA23-00781-01.pdf>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00782-01
CSIRT informa de vulnerabilidad de alta severidad en F5 BIG-IP

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



CSIRT informa de vulnerabilidad severa en BIG-IP de F5

Alerta de seguridad cibernética	9VSA23-00782-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	3 de febrero de 2023
Última revisión	3 de febrero de 2023

CVE

CVE-2023-22374

Fabricantes

F5

Productos afectados

BIG-IP 13.1.5, 14.1.4.6 a 14.1.5, 15.1.5.1 a 15.1.8, 16.1.2.2 a 16.1.3 y 17.0.0.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00782-01/>
<https://www.csirt.gob.cl/media/2023/02/9VSA23-00782-01.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>



CSIRT alerta de vulnerabilidad severa que afecta a algunos productos de Cisco

Alerta de seguridad cibernética	9VSA23-00783-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	3 de febrero de 2023
Última revisión	3 de febrero de 2023

CVE

CVE-2023-20076

Fabricantes

Cisco

Productos afectados

Aparatos Cisco que corran software Cisco IOS XE, si tienen activada la función Cisco IOx.

800 Series Industrial ISRs

Catalyst Access Points

CGR1000 Compute Modules

IC3000 Industrial Compute Gateways

IR510 WPAN Industrial Routers

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00783-01/>

<https://www.csirt.gob.cl/media/2023/02/9VSA23-00783-01.pdf>



CSIRT informa de vulnerabilidad en OpenSSH server (sshd)

Alerta de seguridad cibernética	9VSA23-00784-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	6 de febrero de 2023
Última revisión	6 de febrero de 2023

CVE

CVE-2023-25136

Fabricantes

OpenSSH

Productos afectados

OpenSSH 9.1

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00784-01/>

<https://www.csirt.gob.cl/media/2023/02/9VSA23-00784-01.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>



CSIRT alerta de nuevas vulnerabilidades parchadas para OpenSSL

Alerta de seguridad cibernética	9VSA23-00785-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	8 de febrero de 2023
Última revisión	8 de febrero de 2023

CVE

CVE-2023-0286
CVE-2022-4304
CVE-2023-0401
CVE-2023-0217
CVE-2023-0216
CVE-2022-4450
CVE-2023-0215
CVE-2023-4203

Fabricantes

OpenSSL

Productos afectados

OpenSSL 1.0.2, 1.1.1 y 3.0.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00785-01/>

<https://www.csirt.gob.cl/media/2023/02/9VSA23-00785-01.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>

5. Concientización

Ciberconsejos para evitar ser víctimas del spoofing

Los ataques a las conexiones inalámbricas son muy comunes, y los ciberdelincuentes se sirven de diversos software y herramientas para saltarse las medidas de seguridad, infectar o tomar control de nuestros dispositivos.

Un ataque de spoofing ocurre cuando una persona pretende ser otra con el fin de inducir a su víctima a que comparta sus datos personales o para que haga alguna acción en nombre del falsificador. Normalmente, el timador se esforzará en establecer una relación de confianza con su objetivo, para asegurarse de que comparta sus datos sensibles con más facilidad.

Ver más: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-ser-victimas-del-spoofing-2/>



Ciberguía para protegernos en línea | Día Internacional de la Internet Segura 2023

El martes 7 de febrero se conmemoró el Día Internacional de Internet Segura 2023. Aprovechando esta efeméride, el CSIRT de Gobierno, Entel y la fundación País Digital elaboramos una guía de consejos para navegar seguros por Internet, proteger la información en redes sociales, cómo evitar las estafas, el grooming, ciberbullying y la sextorsión, entre otros, la que pueden encontrar aquí: <https://www.csirt.gob.cl/recomendaciones/ciberguia-dia-internet-segura-2023/>



Día Internacional de Internet Segura

Ciberconsejos para navegar por internet



Ciberdiccionario Volumen 29

¿De qué hablamos cuando decimos clonación, control parental, passwordless y sextorsión en un contexto de ciberseguridad? Para ayudarnos a entender mejor estos conceptos decidimos definirlos en esta semana de nuestro tradicional ciberdiccionario. Esperamos les sea de utilidad.



Ciber diccionario

Sextorsión

Forma de chantaje que, sin usar fuerza física, exige a la víctima contenido o favores sexuales, o pagos en dinero o criptomonedas, a cambio de no revelar contenido sexual o sensible de carácter privado, que el delincuente ha conseguido o dice tener (aunque no sea cierto). Este tipo de extorsión suele realizarse a través de internet.



Ciber diccionario

Passwordless

"Sin contraseña", en inglés, son sistemas de autenticación que descartan el uso de claves y en su lugar emplean otros métodos para reconocer a sus usuarios. Entre los mecanismos usados está el reconocimiento biométrico (huellas dactilares o cara) y el uso de aplicaciones o tokens de autenticación, que deben ser registradas previamente.



Ciber diccionario

Control parental

Función de algunos aparatos, aplicaciones y programas que permite limitar el contenido que pueden ver o al que pueden acceder los menores de edad, por parte de sus padres o tutores. Hoy en día permiten además establecer límites de tiempo de consumo de ciertos programas o canales de TV, por ejemplo, y crear un registro de lo visto o visitado en internet.



Ciber diccionario

Clonación

Tal como al usarlo en otros contextos, en ciberseguridad la clonación se refiere a la copia de un original, en este caso un sitio web, de la forma más fiel posible, para robar datos de usuarios o instalar programas maliciosos en sus equipos. Los sitios clonados sirven para el phishing, facilitando hacer creer a las personas que interactúan con una persona legítima, en lugar de delincuentes.



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.

- Claudio Vargas Méndez
- José Luis Peña Donoso
- Andrea Balocchi
- Juan Andrés Salazar Pino
- Gustavo Marambio Figueroa
- Carola Gutiérrez Orrego
- Pía Olivares López
- Fernando Flores Tobar
- Lorena Díaz Asenjo
- Mathias Roco Fernandez
- Ana María Milla Espejo
- Cristóbal Herrera Jara
- Alexis Venegas Palacios
- Paula Riumallo
- Michael Díaz Ibeas

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>