



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 252

semana del 26 de abril al 3 de mayo de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

3

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

5

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

13

Las mitigaciones son útiles en productos de Aruba y Google.



HASH REPORTADOS

3

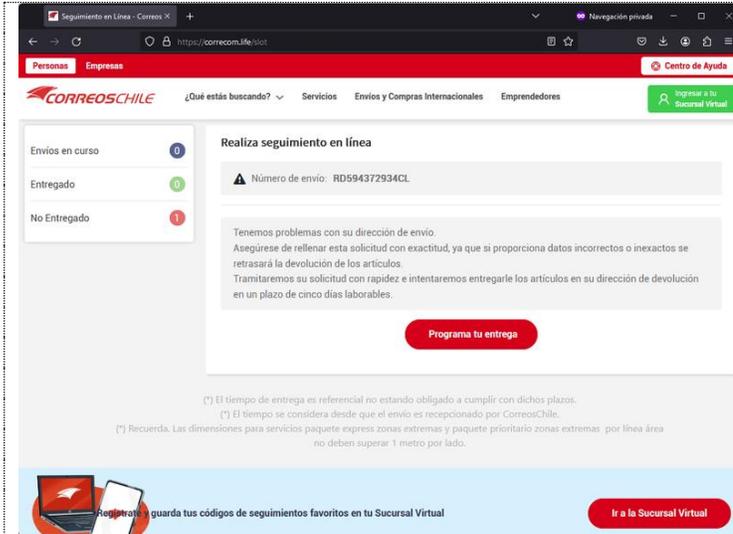
Hashes asociados a múltiples campañas de phishing con archivos que contienen malware.



CONTENIDO

1.	Sitios fraudulentos.....	3
2.	Malware.....	4
3.	Phishing	5
4.	Vulnerabilidades.....	6
4.	Noticias y concientización.....	7
5.	Recomendaciones y buenas prácticas	9
5.	Muro de la Fama	10

1. Sitios fraudulentos



CorreosChile - Falsificación

Código de alerta	FFR24-01683
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de abril de 2024
Última revisión	29 de abril de 2024

Indicadores de compromiso

URL del sitio falso

<https://correcom.life/slot>

URL sitio redirección

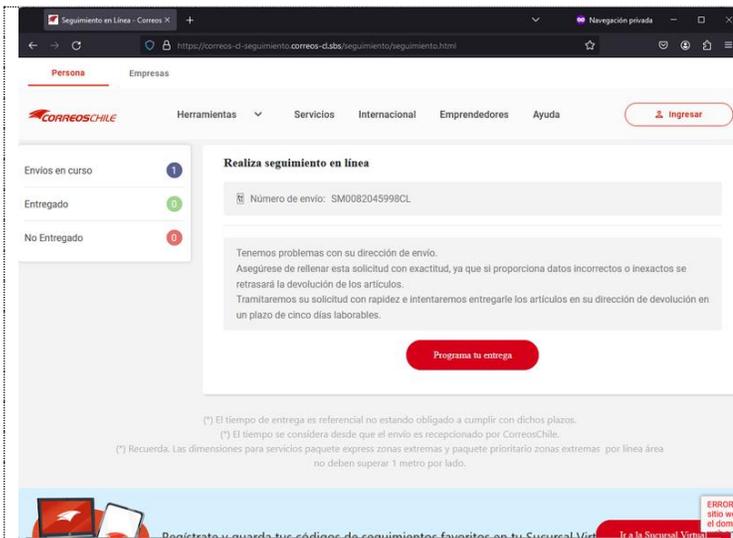
<https://qrco.de/bf0ema>

Dirección IP sitio falso

[162.62.53.33]

Enlace para revisar loC:

<https://csirt.gob.cl/alertas/8ffr24-01683/>



CorreosChile - Falsificación

Código de alerta	FFR24-01684
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de abril de 2024
Última revisión	29 de abril de 2024

Indicadores de compromiso

URL del sitio falso

<https://correos-cl-seguimiento.correos-cl.sbs/seguimiento/seguimiento.html>

Dirección IP sitio falso

[172.67.131.228]

Enlace para revisar loC:

<https://csirt.gob.cl/alertas/8ffr24-01684/>

CONTACTO Y REDES SOCIALES CSIRT

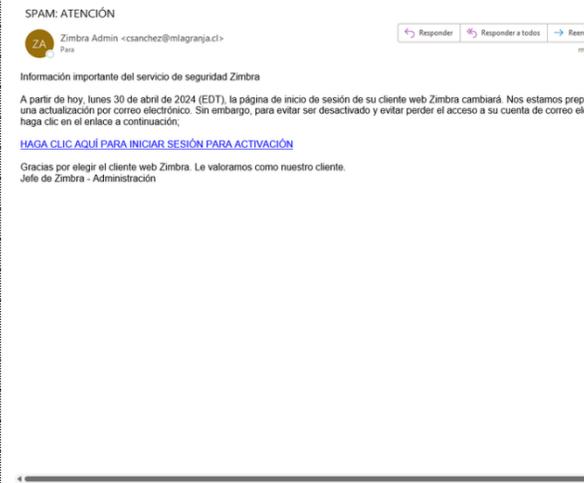
<https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
<https://www.linkedin.com/company/csirt-gob>

3. Malware

 <p>CFDI Manager Emission 188000422560 4/29/2024</p> <p>boleto@smtplw-13.com 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>Envío de Comprobante CFDI Manager Emission</p> <p>Estimado Cliente:</p> <p>Le notificamos: Que se le ha enviado su Comprobante Fiscal Digital a través del envío automático de correos.</p> <p>Adjunto encontrará el formato XML con su respectivo Archivo PDF.</p> <p>visualizarla necesitas el software Adobe Reader</p> <p>Disponible sólo en DESKTOP</p> <p>Saludos Cordiales,</p> <p>Ver PDF Ver XML</p>	Falso comprobante fiscal digital por internet - Suplantación con malware	
	Código de alerta	CMV24-00460
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	30 de abril de 2024
	Última revisión	30 de abril de 2024
	Indicadores de compromiso	
	Asunto	
CFDI Manager Emission 188000422560 4/29/2024		
URL descarga		
https://livmallsusps.apanemyster.com/Y1Kz2PEvOUBWGVKRBFVAMcUesmafWJK CpC1x4iaW1scUgOwu6HQcDtS5clVPFyO2zeKZkj9vrLVxQ7hxNfZLvs/yzQTZKkC5xV59fCC1o/CaqbtuFPPUnYQzY9zknph40LVKXHpAXX/QVJI4fZOUHEAz3coRIH9p/svefyVo1R9DkgJT3B3		
SHA256		
5e6e4b921c30e9b12e65e110b4833c84c7f2621d7fe16fd890dd511308634bbfbd098ae264b4ac2097867132ee29b23af5b21d200abd77f033d343fcd2cbd37ed5c740ccdb8e748282de69f20e58eb7860f2174d6bfe43d50851ad32df4ac002		
Enlace para revisar IoC:		
https://csirt.gob.cl/alertas/cmv24-00460/		

CONTACTO Y REDES SOCIALES CSIRT

4. Phishing

 <p>SPAM: ATENCIÓN</p> <p>Zimbra Admin <csanchez@mlagranja.cl></p> <p>Información importante del servicio de seguridad Zimbra</p> <p>A partir de hoy, Lunes 30 de abril de 2024 (EDT), la página de inicio de sesión de su cliente web Zimbra cambiará. Nos estamos preparando una actualización por correo electrónico. Sin embargo, para evitar ser desactivado y evitar perder el acceso a su cuenta de correo electrónico, haga clic en el enlace a continuación:</p> <p>HAGA CLIC AQUÍ PARA INICIAR SESIÓN PARA ACTIVACIÓN</p> <p>Gracias por elegir el cliente web Zimbra. Le valoramos como nuestro cliente.</p> <p>Jefe de Zimbra - Administración</p>	Zimbra - Phishing	
	Alerta de seguridad cibernética	FPH24-00956
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	30 de abril de 2024
	Última revisión	30 de abril de 2024
	Indicadores de compromiso	
	URL del sitio falso	
	https://ipfs.io/ipfs/bafybeih4wwljr3lg6fxunpfgmjppqlwhihybtvbn5wesic6ii6wdjizfm/eso.com.mk.htm	
	Dirección IP sitio falso	
	[209.94.90.1]	
	Enlace para revisar loC:	
https://csirt.gob.cl/alertas/fph24-00956/		

CONTACTO Y REDES SOCIALES CSIRT

5. Vulnerabilidades



**VULNERABILIDADES
GOOGLE CHROME**

VSA24-01010 CSIRT COMPARTE INFORMACIÓN DE VULNERABILIDADES PARCHADAS EN GOOGLE CHROME 124.0.6367.78/79



Busca el informe de los productos afectados y el enlace para la mitigación de la vulnerabilidad en: csirt.gob.cl/vulnerabilidades

Google Chrome - Vulnerabilidades		
Código de alerta	VSA24-01010	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	2 de mayo de 2024	
Última revisión	2 de mayo de 2024	
CVE, puntaje CVSS y EPSS al momento de la publicación		
CVE-2024-4058	8.8	0.04%
CVE-2024-4059	6.5	0.04%
CVE-2024-4060	8.8	0.04%
Fabricante		
Google		
Productos afectados		
Google Chrome 124		
Enlaces para revisar el informe:		
https://csirt.gob.cl/alertas/vsa24-01010/		



**VULNERABILIDADES
ARUBA**

VSA24-01011 CSIRT COMPARTE INFORMACIÓN DE VULNERABILIDADES PARCHADAS POR ARUBA EN ARUBAOS



a Hewlett Packard
Enterprise company

Busca el informe de los productos afectados y el enlace para la mitigación de la vulnerabilidad en: csirt.gob.cl/vulnerabilidades

ArubaOS - Vulnerabilidades		
Código de alerta	VSA24-01011	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	2 de mayo de 2024	
Última revisión	2 de mayo de 2024	
CVE, puntaje CVSS y EPSS al momento de la publicación		
CVE-2024-26304	9.8	0.04%
CVE-2024-26305	9.8	0.04%
CVE-2024-33511	9.8	0.04%
CVE-2024-33512	9.8	0.04%
CVE-2024-33513	5.9	0.04%
CVE-2024-33514	5.9	0.04%
CVE-2024-33515	5.9	0.04%
CVE-2024-33516	5.3	0.04%
CVE-2024-33517	5.3	0.04%
CVE-2024-33518	5.3	0.04%
Fabricante		
Aruba		
Productos afectados		
ArubaOS		
10.5.1.0 y anteriores.		
10.4.1.0 y anteriores.		
8.11.2.1 y anteriores.		
8.10.0.10 y anteriores.		
Todas las versiones que alcanzaron su fin de vida (EoL), para las cuales no se entregó parches.		
Enlaces para revisar el informe:		
https://csirt.gob.cl/alertas/vsa24-01011		

CONTACTO Y REDES SOCIALES CSIRT

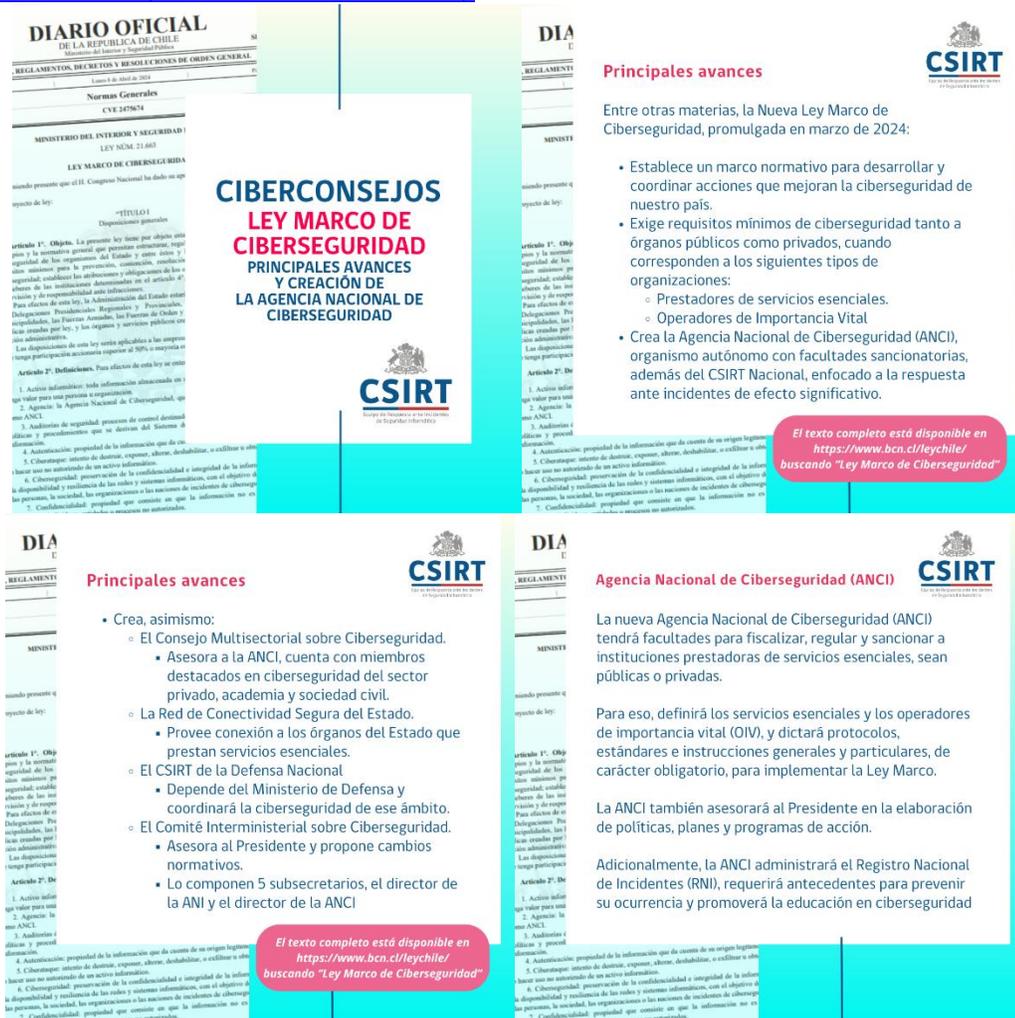
<https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
<https://www.linkedin.com/company/csirt-gob>

6. Noticias y concientización

Ciberconsejos | Ley Marco de Ciberseguridad: sus principales avances y atribuciones de la ANCI

Esta es la primera de una serie de Ciberconsejos en las que compartiremos los principales avances contenidos en la nueva Ley Marco de Ciberseguridad (de la que pueden encontrar el texto completo en el enlace del cuadro azul con el nombre "Enlaces Relacionados"). Para comenzar, compartimos datos generales de esta nueva legislación, como la definición de los conceptos de prestadores de servicios esenciales y operadores de importancia vital, y revisamos las principales atribuciones de la nueva Agencia Nacional de Ciberseguridad (ANCI).

La campaña completa, para descargar y compartir con sus trabajadores, amigos y familiares, aquí: <https://ciberseguridad.gob.cl/ciberconsejos/ciberconsejos-ley-marco-de-ciberseguridad-sus-principales-avances-y-atribuciones-de-la-anci/>



Principales avances

Entre otras materias, la Nueva Ley Marco de Ciberseguridad, promulgada en marzo de 2024:

- Establece un marco normativo para desarrollar y coordinar acciones que mejoran la ciberseguridad de nuestro país.
- Exige requisitos mínimos de ciberseguridad tanto a órganos públicos como privados, cuando corresponden a los siguientes tipos de organizaciones:
 - Prestadores de servicios esenciales.
 - Operadores de Importancia Vital
- Crea la Agencia Nacional de Ciberseguridad (ANCI), organismo autónomo con facultades sancionatorias, además del CSIRT Nacional, enfocado a la respuesta ante incidentes de efecto significativo.

Principales avances

- Crea, asimismo:
 - El Consejo Multisectorial sobre Ciberseguridad.
 - Asesora a la ANCI, cuenta con miembros destacados en ciberseguridad del sector privado, academia y sociedad civil.
 - La Red de Conectividad Segura del Estado.
 - Provee conexión a los órganos del Estado que prestan servicios esenciales.
 - El CSIRT de la Defensa Nacional
 - Depende del Ministerio de Defensa y coordinará la ciberseguridad de ese ámbito.
 - El Comité Interministerial sobre Ciberseguridad.
 - Asesora al Presidente y propone cambios normativos.
 - Lo componen 5 subsecretarios, el director de la ANI y el director de la ANCI

Principales avances

La nueva Agencia Nacional de Ciberseguridad (ANCI) tendrá facultades para fiscalizar, regular y sancionar a instituciones prestadoras de servicios esenciales, sean públicas o privadas.

Para eso, definirá los servicios esenciales y los operadores de importancia vital (OIV), y dictará protocolos, estándares e instrucciones generales y particulares, de carácter obligatorio, para implementar la Ley Marco.

La ANCI también asesorará al Presidente en la elaboración de políticas, planes y programas de acción.

Adicionalmente, la ANCI administrará el Registro Nacional de Incidentes (RNI), requerirá antecedentes para prevenir su ocurrencia y promoverá la educación en ciberseguridad.

El texto completo está disponible en <https://www.bcn.cl/leychile/> buscando "Ley Marco de Ciberseguridad"

CONTACTO Y REDES SOCIALES CSIRT

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

Ciberguía Devolución de Impuestos 2024

En esta ocasión, lo hacemos centrados en el período recientemente comenzado de devolución de impuestos. Para eso, les recordamos los conceptos de ingeniería social, phishing, vishing y smishing.

Disponible en <https://ciberseguridad.gob.cl/ciberconsejos/ciberguia-devolucion-de-impuestos-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>

7. 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

8. 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.

- Esteban Olivares
- Vicente Jesús Flores Martínez
- Manuel Alejandro Varela Mancilla
- Andrés Peñailillo
- Héctor Prieto Tabilo
- Luis Felipe Segura Cerda
- Alonso Villalobos González

CONTACTO Y REDES SOCIALES CSIRT