



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 249

semana del 5 al 11 de abril de 2024

# LA SEMANA EN CIFRAS

## IP INFORMADAS

4

IP advertidas en múltiples campañas de phishing y de fraude.



## URL ADVERTIDAS

6

URL asociadas a sitios fraudulentos y campañas de phishing y malware



## PARCHES COMPARTIDOS

199

Las mitigaciones son útiles en productos de Microsoft, Adobe, SAP, Fortinet, Ivanti y Progress.



## HASH REPORTADOS

20

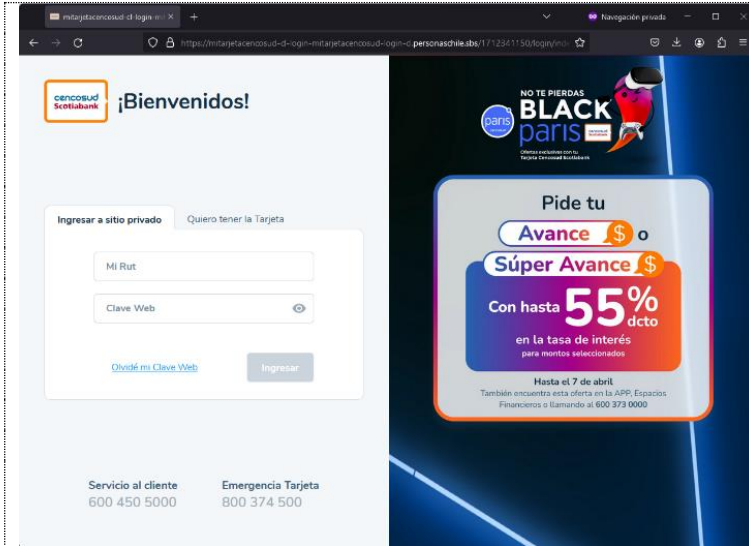
Hashes asociados a múltiples campañas de phishing con archivos que contienen malware.



# CONTENIDO

1.	Sitios fraudulentos.....	3
2.	Malware.....	4
3.	Phishing .....	7
4.	Vulnerabilidades.....	9
4.	Noticias y concientización.....	17
5.	Recomendaciones y buenas prácticas .....	22
5.	Muro de la Fama .....	23

## 1. Sitios fraudulentos



### Cencosud Scotiabank - Falsificación

Código de alerta	FFR24-01676
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2024
Última revisión	5 de abril de 2024

### Indicadores de compromiso

#### URL del sitio falso

<https://mitarjetacenosud-cl-login-mitarjetacenosud-login-cl.personaschile.sbs/1712341150/login/index.html>

#### Dirección IP sitio falso

[172.67.142.101]

#### Enlace para revisar loC:

<https://csirt.gob.cl/alertas/8ffr24-01676/>

### 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>

# Boletín de Ciberseguridad N° 249

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



BOLETÍN 13BCS24-00258-01 | Semana del 5 al 11 de abril de 2024

## 2. Malware

<p>Fw: REQUERIMIENTO PARA RESOLVER EL TRÁMITE - Últimos días. - ( 7322458 )</p> <p>Sii - Servicio de Impuestos Internos &lt;informe-11426568@Sii.info&gt;</p> <p>Estimado contribuyente. Rut:  Nombre:  Le informamos que encontramos problemas en la información de emisión de sus boletas electrónicas, queremos recordar que a partir del 2024, usted deberá presentar declaraciones Jurada(s) relativa(s) al régimen fiscal al que está sujeto. En adjunto a continuación de su correo con error.</p> <ul style="list-style-type: none"><li>Informe detallado: 11426568.PDF (PDF - Acrobat Reader)</li><li>Informe detallado: 11426568.excel (excel - Microsoft Word)</li></ul> <p>Usted tiene hasta el 18 de abril de 2024 para anular lo que emitió mal, la factura, con los mismos datos. Después de esta fecha, no podrá hacer ningún cambio.</p> <p>Superintendencia Nacional de Administración Tributaria. Nuestro compromiso es facilitar su aporte al desarrollo del país.</p>	<h3>Servicio de Impuestos Internos - Malware</h3> <table border="1"><tr><td>Código de alerta</td><td>CMV24-00453</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>5 de abril de 2024</td></tr><tr><td>Última revisión</td><td>5 de abril de 2024</td></tr></table> <h3>Indicadores de compromiso</h3> <p><b>Asunto</b> REQUERIMIENTO PARA RESOLVER EL TRÁMITE- Últimos días. - ( 7322458 )</p> <p><b>Correo de salida</b> pwanmaxe@6859004.hostengines.com</p> <p><b>SHA256</b> 054b7fb5c8aece945a0162b21dad6ad0436c07201e20f17db9f5d0628958a7857e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910aac789666d9867918d589bcacfe0fded5300026ff019ccba122f73e7cf634e431e28e34bdaff077669586dcd4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7</p> <p><b>Enlace para revisar IoC:</b> <a href="https://csirt.gob.cl/alertas/cmv24-00453/">https://csirt.gob.cl/alertas/cmv24-00453/</a></p>	Código de alerta	CMV24-00453	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	5 de abril de 2024	Última revisión	5 de abril de 2024
Código de alerta	CMV24-00453														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	5 de abril de 2024														
Última revisión	5 de abril de 2024														

<p>orden compra</p> <p>Tienda castellana (Facturación) &lt;ventas@psidobrasil.com.br&gt;</p> <p>Orden Compra.pdf.html 852 KB</p> <p>Saludos cordiales,</p> <p>Adjunto cotización y orden de compra.</p> <p>Quedo atenta a sus comentarios.</p> <p><b>Favor de confirmar recepción de correo</b></p> <p>Cordialmente me despido, y, me coloco sus órdenes.</p> <p>Saludos,</p>	<h3>Alerta general - Suplantación con malware</h3> <table border="1"><tr><td>Código de alerta</td><td>CMV24-00454</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>5 de abril de 2024</td></tr><tr><td>Última revisión</td><td>5 de abril de 2024</td></tr></table> <p><b>Asunto</b> Orden compra</p> <p><b>Correo de salida</b> ventas@psidobrasil.com.br</p> <p><b>Indicadores de compromiso</b></p> <p><b>SHA256</b> 1837ea1589add133e71cee9186650e173858f803c1d22c35379e0942d237972c2af73b4896049b091a2ef506dee893208ec548eb9236568c9f793c709efcf30777238aaa93306c3b06c4284434492ada5acf0e160c0097970080dabad38a4ba5add1a0e5cf249b22e6873a930149429ceb82e535fcd66b892fc8bfff16df3f099e110f2c1139aa5b879c3288ece8c485a0af16d14be2a7c0eed78970d75efafea</p> <p><b>Enlace para revisar IoC:</b> <a href="https://csirt.gob.cl/alertas/cmv24-00454/">https://csirt.gob.cl/alertas/cmv24-00454/</a></p>	Código de alerta	CMV24-00454	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	5 de abril de 2024	Última revisión	5 de abril de 2024
Código de alerta	CMV24-00454														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	5 de abril de 2024														
Última revisión	5 de abril de 2024														

### CONTACTO Y REDES SOCIALES CSIRT

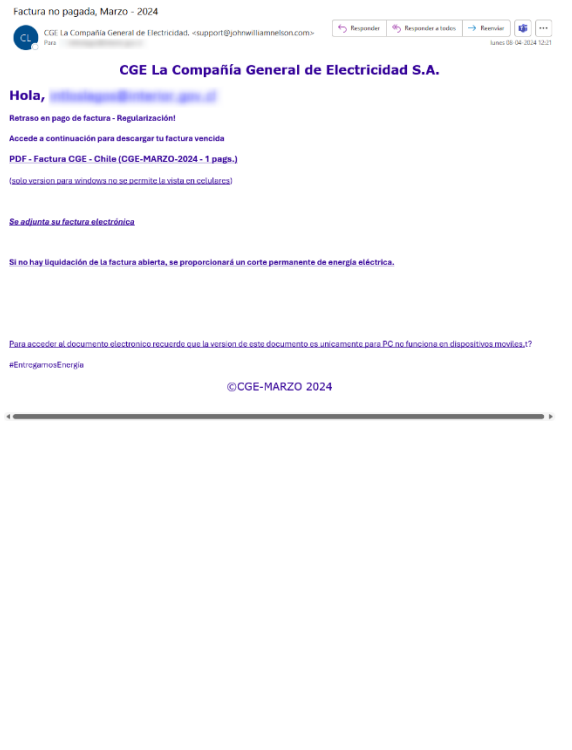
<https://www.csirt.gob.cl>  
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl  
@csirtgob  
<https://www.linkedin.com/company/csirt-gob>

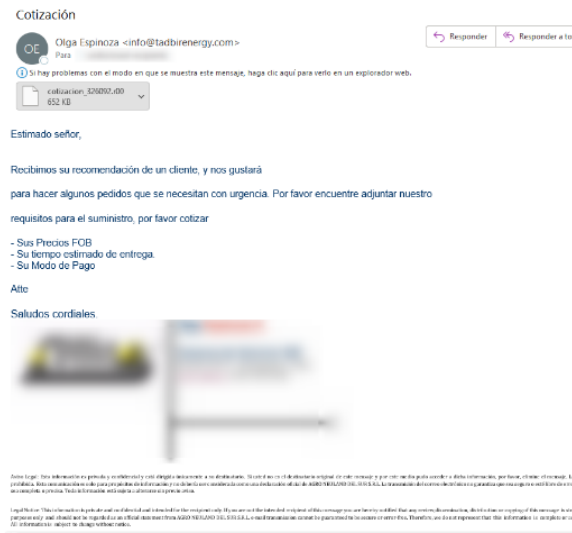
# Boletín de Ciberseguridad N° 249

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



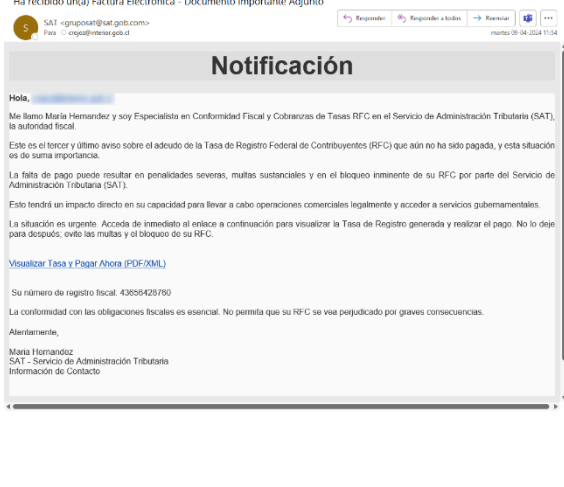
BOLETÍN 13BCS24-00258-01 | Semana del 5 al 11 de abril de 2024

 <p>Factura no pagada, Marzo - 2024</p> <p>Hola,</p> <p>Retraso en pago de factura - Regularización</p> <p>Accede a continuación para descargar tu factura vencida</p> <p>PDF - Factura CGE - Chile (CGE-MARZO-2024 - 1 page)</p> <p>Se adjunta su factura electrónica</p> <p>Si no hay liquidación de la factura abierta, se proporcionará un corte permanente de energía eléctrica.</p> <p>Para acceder al documento electrónico recuerda que la versión de este documento es únicamente para PC se funciona en dispositivos móviles?</p> <p>#EntregamosEnergía</p> <p>@CGE-MARZO 2024</p>	<h3>Compañía General de Electricidad (CGE) - Suplantación con malware</h3> <table border="1"><tr><td>Código de alerta</td><td>CMV24-00455</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>8 de abril de 2024</td></tr><tr><td>Última revisión</td><td>8 de abril de 2024</td></tr></table> <p><b>Asunto</b> Factura no pagada, Marzo - 2024</p> <p><b>Correo de salida</b> support@uww-reg.ru support@uncutmaza.club support@lot.ziy.cc support@johnwilliamnelson.com support@ikaglm.com support@banglachotigolpo.top support@augustineformayor.ca</p> <p><b>SHA256</b> 19ef6dcc8257fc55032aa97eb5613a8dc35cfd41bf4804d239ee349d03b7129c5cc97524d9ab2d29019d545b06f8ef8fc5b9fb8ee257d7352a619f8950f54497e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910ae28e34fdbaff077669586dcd4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7</p> <p><b>Enlace para revisar IoC:</b> <a href="https://csirt.gob.cl/alertas/cmv24-00455">https://csirt.gob.cl/alertas/cmv24-00455</a></p>	Código de alerta	CMV24-00455	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	8 de abril de 2024	Última revisión	8 de abril de 2024
Código de alerta	CMV24-00455														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	8 de abril de 2024														
Última revisión	8 de abril de 2024														

 <p>Cotización</p> <p>Olga Espinoza &lt;info@tadbirenergy.com&gt;</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>Estimado señor,</p> <p>Recibimos su recomendación de un cliente, y nos gustaría para hacer algunos pedidos que se necesitan con urgencia. Por favor encuentre adjuntar nuestro requisitos para el suministro, por favor cotizar</p> <ul style="list-style-type: none"><li>- Sus Precios FOB</li><li>- Su tiempo estimado de entrega.</li><li>- Su Modo de Pago</li></ul> <p>Atte</p> <p>Saludos cordiales</p>	<h3>Email con falsa cotización - Suplantación con malware</h3> <table border="1"><tr><td>Código de alerta</td><td>CMV24-00456</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>8 de abril de 2024</td></tr><tr><td>Última revisión</td><td>8 de abril de 2024</td></tr></table> <p><b>Asunto</b> Cotización</p> <p><b>Correos de salida</b> info@tadbirenergy.com</p> <p><b>SHA256</b> 34f838011c9242be21fc440f803dbc271a19e7cbf35dd585b68566df577e0cea96ad1146eb96877eab5942ae0736b82d8b5e2039a80d3d6932665c1a4c87dcf7cbceb77aad2e48791ffca911e04cb4fafad3d29545535b11c08d26e4dda971d</p> <p><b>Enlace para revisar IoC:</b> <a href="https://csirt.gob.cl/alertas/cmv24-00456">https://csirt.gob.cl/alertas/cmv24-00456</a></p>	Código de alerta	CMV24-00456	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	8 de abril de 2024	Última revisión	8 de abril de 2024
Código de alerta	CMV24-00456														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	8 de abril de 2024														
Última revisión	8 de abril de 2024														

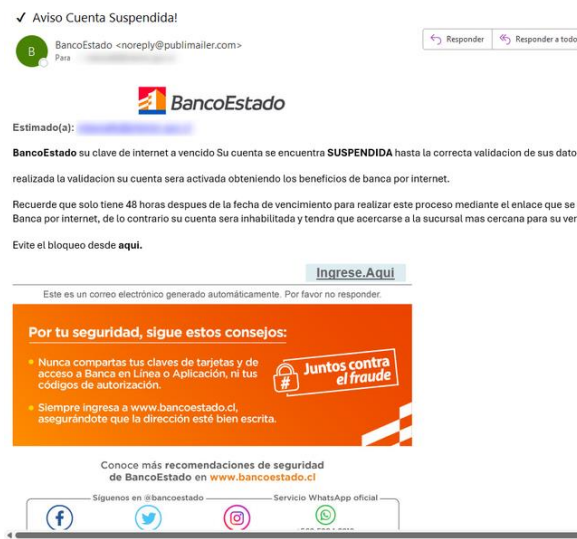
## CONTACTO Y REDES SOCIALES CSIRT

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

 <p>Ha recibido un(a) Factura Electronica - Documento importante- Adjunto</p> <p>SAT &lt;gruposat@sat.gob.mx&gt; Para: cngob@interior.gob.cl</p> <h3>Notificación</h3> <p>Hola,</p> <p>Me llamo Mariana Hernández y soy Especialista en Conformidad Fiscal y Cobranzas de Tesas RFC en el Servicio de Administración Tributaria (SAT), la autoridad fiscal.</p> <p>Este es el tercer y último aviso sobre el adeudo de la Tasa de Registro Federal de Contribuyentes (RFC) que aún no ha sido pagada, y esta situación es de suma importancia.</p> <p>La falta de pago puede resultar en penalidades severas, multas sustanciales y en el bloqueo inminente de su RFC por parte del Servicio de Administración Tributaria (SAT).</p> <p>Esto tendrá un impacto directo en su capacidad para llevar a cabo operaciones comerciales legalmente y acceder a servicios gubernamentales.</p> <p>La situación es urgente. Acceda de inmediato al enlace a continuación para visualizar la Tasa de Registro generada y realizar el pago. No lo deje para después, evite las multas y el bloqueo de su RFC.</p> <p><a href="#">Visualizar Tasa y Pagar Ahora (PDF/XML)</a></p> <p>Su número de registro fiscal: 43629429780</p> <p>La conformidad con las obligaciones fiscales es esencial. No permita que su RFC se vea perjudicado por graves consecuencias.</p> <p>Atentamente,</p> <p>Mariana Hernández SAT - Servicio de Administración Tributaria Información de Contacto</p>	<h3>Servicio de Administración Tributaria (México) - Suplantación con malware</h3> <table border="1"><tr><td>Código de alerta</td><td>CMV24-00457</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>9 de abril de 2024</td></tr><tr><td>Última revisión</td><td>9 de abril de 2024</td></tr></table> <p><b>Asunto</b></p> <p>Ha recibido un(a) Factura Electronica</p> <p><b>SHA256</b></p> <p>1ec5aec6e629d8a9c3bf75e3c425bef10c25e1557283029745c434c7c9ee6389 67059e589ebd10e14640ccbe0c166a72eaf131697fe9ac63237609a23048b67 eeb1f2843f4e17352a324385145e58dfa6c843b74e5384fff643bc48be50faa2 f2d850025dd7b65c44d979ec74a3f5a77e1c15b4070812be5656887cee95dc59</p> <p><b>Enlace para revisar loC:</b></p> <p><a href="https://csirt.gob.cl/alertas/cmv24-00457">https://csirt.gob.cl/alertas/cmv24-00457</a></p>	Código de alerta	CMV24-00457	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	9 de abril de 2024	Última revisión	9 de abril de 2024
Código de alerta	CMV24-00457														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	9 de abril de 2024														
Última revisión	9 de abril de 2024														

## 3. Phishing

	<b>Netflix - Phishing</b>	
	Alerta de seguridad cibernética	FPH24-00946
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	5 de abril de 2024
	Última revisión	5 de abril de 2024
	<b>Indicadores de compromiso</b>	
	<b>URL del sitio falso</b> <a href="https://jemi.so/nitwatchflex-24">https://jemi.so/nitwatchflex-24</a>	
<b>URL de redirección</b> <a href="https://yekx619z.dreamwp.com/wp-admin/css/colors/blue/daz/update/payment-method.php">https://yekx619z.dreamwp.com/wp-admin/css/colors/blue/daz/update/payment-method.php</a>		
<b>Dirección IP sitio falso</b> [76.76.21.93]		
<b>Enlace para revisar IoC:</b> <a href="https://csirt.gob.cl/alertas/fph24-00946/">https://csirt.gob.cl/alertas/fph24-00946/</a>		

	<b>BancoEstado - Phishing</b>	
	Alerta de seguridad cibernética	FPH24-00947
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	5 de abril de 2024
	Última revisión	5 de abril de 2024
	<b>Indicadores de compromiso</b>	
	<b>URL del sitio falso</b> <a href="https://invitad0smnhomstado.com/1712345279/imagenes/_personas/home/default.asp">https://invitad0smnhomstado.com/1712345279/imagenes/_personas/home/default.asp</a>	
<b>URL de redirección</b> <a href="https://solucionesregistrars.com/activacion/cuenta-bwln/">https://solucionesregistrars.com/activacion/cuenta-bwln/</a>		
<b>Dirección IP sitio falso</b> [198.27.78.113]		
<b>Enlace para revisar IoC:</b> <a href="https://csirt.gob.cl/alertas/fph24-00947/">https://csirt.gob.cl/alertas/fph24-00947/</a>		

### CONTACTO Y REDES SOCIALES CSIRT



# Boletín de Ciberseguridad N° 249

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



BOLETÍN 13BCS24-00258-01 | Semana del 5 al 11 de abril de 2024

<p>Your Email: vguenulg@interior.gob.cl will be blocked</p> <p>support@interior.gob.cl Para [redacted]</p> <p>Due to new security updates on our server your Email: [redacted] will be stopped from sending e</p> <p>If you wish to keep using your email, kindly verify below .</p> <p><b>VERIFY EMAIL</b></p> <p>The verification process takes few seconds only. Failure to verify email would lead to closure.</p> <p>Thank You, interior.gob.cl Support</p>	<b>Cambio de contraseña - Phishing</b>	
	Alerta de seguridad cibernética	FPH24-00948
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	5 de abril de 2024
	Última revisión	5 de abril de 2024
	<b>Indicadores de compromiso</b>	
	<b>URL del sitio falso</b> <a href="https://online.evaluater.rest/international.html?mode={Email}">https://online.evaluater.rest/international.html?mode={Email}</a>	
<b>Dirección IP sitio falso</b> [54.39.196.148]		
<b>Enlace para revisar loC:</b> <a href="https://csirt.gob.cl/alertas/fph24-00948/">https://csirt.gob.cl/alertas/fph24-00948/</a>		

<p>Factura impagada, actuar pronto</p> <p>AD Aviso de posible suspension &lt;cobranzas@email.claro.com&gt; Para [redacted]</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><b>Claro</b></p> <p>Hola, [redacted]</p> <p>Factura impagada, actuar pronto 10/04/2024</p> <p><b>TUS DATOS:</b></p> <p><b>Número de cuenta:</b> 76500447551</p> <p><b>Vencimiento:</b> 05/04/2024</p>	<b>Phishing con malware, suplantación de Claro - Phishing</b>	
	Alerta de seguridad cibernética	FPH24-00949
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	10 de abril de 2024
	Última revisión	10 de abril de 2024
	<b>Enlace para revisar loC:</b> <a href="https://csirt.gob.cl/alertas/fph24-00949/">https://csirt.gob.cl/alertas/fph24-00949/</a>	

## 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. Vulnerabilidades



**VULNERABILIDADES  
PROGRESS**

**VSA24-00996 CSIRT INFORMA DE VULNERABILIDAD CRÍTICA EN PROGRESS FLOWMON**



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

Progress Flowmon - Vulnerabilidad	
Código de alerta	VSA24-00996
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2024
Última revisión	5 de abril de 2024
<b>CVE</b>	
CVE-2024-2389	
<b>Fabricante</b>	
Progress	
<b>Productos afectados</b>	
Progress Flowmon 11.x, 12.x. Anteriores a la 11.0 no afectadas	
<b>Enlaces para revisar el informe:</b>	
<a href="https://csirt.gob.cl/alertas/vsa24-00996/">https://csirt.gob.cl/alertas/vsa24-00996/</a>	




**VULNERABILIDADES  
IVANTI**

**VSA24-00997 CSIRT INFORMA DE VULNERABILIDADES EN IVANTI CONNECT SECURE Y EN IVANTI POLICY SECURE GATEWAYS**




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

Ivanti Connect Secure (ICS) y otros - Vulnerabilidad	
Código de alerta	VSA24-00997
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de abril de 2024
Última revisión	9 de abril de 2024
<b>CVE</b>	
CVE-2024-21894	CVE-2024-22053
CVE-2024-22052	CVE-2024-22023
<b>Fabricante</b>	
Ivanti	
<b>Productos afectados</b>	
Ivanti Connect Secure (ICS) 9.x, 22.x, Ivanti Policy Secure 9.x, 22.x	
<b>Enlaces para revisar el informe:</b>	
<a href="https://csirt.gob.cl/alertas/vsa24-00997/">https://csirt.gob.cl/alertas/vsa24-00997/</a>	



**VULNERABILIDADES  
MICROSOFT**





**VSA24-00998 CSIRT COMPARTE INFORMACIÓN DE ACTUALIZACIÓN MICROSOFT UPDATE TUESDAY CORRESPONDIENTE A ABRIL 2024**



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

Ivanti Connect Secure (ICS) y otros - Vulnerabilidad		
Código de alerta	VSA24-00998	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	9 de abril de 2024	
Última revisión	9 de abril de 2024	
<b>CVE</b>		
CVE-2024-20665	CVE-2024-26226	CVE-2024-28921
CVE-2024-20669	CVE-2024-26227	CVE-2024-28922
CVE-2024-20670	CVE-2024-26228	CVE-2024-28923
CVE-2024-20678	CVE-2024-26229	CVE-2024-28924
CVE-2024-20685	CVE-2024-26230	CVE-2024-28925

### CONTACTO Y REDES SOCIALES CSIRT

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

# Boletín de Ciberseguridad N° 249

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



BOLETÍN 13BCS24-00258-01 | Semana del 5 al 11 de abril de 2024

CVE-2024-20688	CVE-2024-26231	CVE-2024-28926
CVE-2024-20689	CVE-2024-26232	CVE-2024-28927
CVE-2024-20693	CVE-2024-26233	CVE-2024-28929
CVE-2024-21322	CVE-2024-26234	CVE-2024-28930
CVE-2024-21323	CVE-2024-26235	CVE-2024-28931
CVE-2024-21324	CVE-2024-26236	CVE-2024-28932
CVE-2024-21409	CVE-2024-26237	CVE-2024-28933
CVE-2024-21424	CVE-2024-26239	CVE-2024-28934
CVE-2024-21447	CVE-2024-26240	CVE-2024-28935
CVE-2024-2201	CVE-2024-26241	CVE-2024-28936
CVE-2024-23593	CVE-2024-26242	CVE-2024-28937
CVE-2024-23594	CVE-2024-26243	CVE-2024-28938
CVE-2024-26158	CVE-2024-26244	CVE-2024-28939
CVE-2024-26168	CVE-2024-26245	CVE-2024-28940
CVE-2024-26171	CVE-2024-26248	CVE-2024-28941
CVE-2024-26172	CVE-2024-26250	CVE-2024-28942
CVE-2024-26175	CVE-2024-26251	CVE-2024-28943
CVE-2024-26179	CVE-2024-26252	CVE-2024-28944
CVE-2024-26180	CVE-2024-26253	CVE-2024-28945
CVE-2024-26183	CVE-2024-26254	CVE-2024-29043
CVE-2024-26189	CVE-2024-26255	CVE-2024-29044
CVE-2024-26193	CVE-2024-26256	CVE-2024-29045
CVE-2024-26194	CVE-2024-26257	CVE-2024-29046
CVE-2024-26195	CVE-2024-28896	CVE-2024-29047
CVE-2024-26200	CVE-2024-28897	CVE-2024-29048
CVE-2024-26202	CVE-2024-28898	CVE-2024-29050
CVE-2024-26205	CVE-2024-28900	CVE-2024-29052
CVE-2024-26207	CVE-2024-28901	CVE-2024-29053
CVE-2024-26208	CVE-2024-28902	CVE-2024-29054
CVE-2024-26209	CVE-2024-28903	CVE-2024-29055
CVE-2024-26210	CVE-2024-28904	CVE-2024-29056
CVE-2024-26211	CVE-2024-28905	CVE-2024-29061
CVE-2024-26212	CVE-2024-28906	CVE-2024-29062
CVE-2024-26213	CVE-2024-28907	CVE-2024-29063
CVE-2024-26214	CVE-2024-28908	CVE-2024-29064
CVE-2024-26215	CVE-2024-28909	CVE-2024-29066
CVE-2024-26216	CVE-2024-28910	CVE-2024-29982
CVE-2024-26217	CVE-2024-28911	CVE-2024-29983
CVE-2024-26218	CVE-2024-28912	CVE-2024-29984
CVE-2024-26219	CVE-2024-28913	CVE-2024-29985
CVE-2024-26220	CVE-2024-28914	CVE-2024-29988
CVE-2024-26221	CVE-2024-28915	CVE-2024-29989
CVE-2024-26222	CVE-2024-28917	CVE-2024-29990
CVE-2024-26223	CVE-2024-28919	CVE-2024-29992
CVE-2024-26224	CVE-2024-28920	CVE-2024-29993

#### Fabricante

Microsoft

#### Productos afectados





.NET 6.0  
.NET 7.0  
.NET 8.0  
Azure AI Search  
Azure Compute Gallery  
Azure Arc Cluster microsoft.azstackhci.operator Extension  
Azure Arc Cluster microsoft.azure.hybridnetwork Extension

## 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>

Azure Arc Cluster microsoft.azurekeyvaultsecretsprovider Extension  
Azure Arc Cluster microsoft.iotoperations.mq Extension  
Azure Arc Cluster microsoft.networkfabricsserviceextension Extension  
Azure Arc Cluster microsoft.openservicemesh Extension  
Azure Arc Cluster microsoft.videoindexer Extension  
Azure Identity Library for .NET  
Azure Kubernetes Service Confidential Containers  
Azure Migrate  
Azure Migrate  
Azure Monitor Agent  
Azure Private 5G Core  
Microsoft .NET Framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8, 4.7.2, 4.8.1  
Microsoft 365 Apps for Enterprise for 32-bit Systems  
Microsoft 365 Apps for Enterprise for 64-bit Systems  
Microsoft Defender for IoT  
Microsoft ODBC Driver 17 for SQL Server on Linux  
Microsoft ODBC Driver 17 for SQL Server on MacOS  
Microsoft ODBC Driver 17 for SQL Server on Windows  
Microsoft ODBC Driver 18 for SQL Server on Linux  
Microsoft ODBC Driver 18 for SQL Server on MacOS  
Microsoft ODBC Driver 18 for SQL Server on Windows  
Microsoft Office LTSC for Mac 2021  
Microsoft OLE DB Driver 18 for SQL Server  
Microsoft OLE DB Driver 19 for SQL Server  
Microsoft SharePoint Server 2016  
Microsoft SharePoint Server 2019  
Microsoft SharePoint Server Subscription Edition  
Microsoft SQL Server 2019 for x64-based Systems (CU 25)  
Microsoft SQL Server 2019 for x64-based Systems (GDR)  
Microsoft SQL Server 2022 for x64-based Systems (CU 12)  
Microsoft SQL Server 2022 for x64-based Systems (GDR)  
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)  
Microsoft Visual Studio 2022  
Outlook for Windows  
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  
Windows 11 Version 22H2 for ARM64-based Systems  
Windows 11 Version 22H2 for x64-based Systems  
Windows 11 Version 23H2 for ARM64-based Systems

## 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>

Windows 11 Version 23H2 for x64-based Systems  
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  
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 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://csirt.gob.cl/alertas/vsa24-00998/>



**VULNERABILIDADES FORTINET**

VSA24-00999 CSIRT COMPARTIÓ INFORMACIÓN DE VULNERABILIDADES QUE AFECTAN A PRODUCTOS DE FORTINET, INCLUYENDO UNA CRÍTICA EN FORTICLIENTLINUX



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

**Fortinet, varios productos - Vulnerabilidades**

Código de alerta	VSA24-00999
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de abril de 2024
Última revisión	10 de abril de 2024

**CVE y puntaje CVSS**

CVE-2023-45590	9.4
CVE-2024-21756	8.6
CVE-2024-21755	8.6
CVE-2024-23671	7.9
CVE-2023-45588	7.8
CVE-2024-31492	7.8
CVE-2023-41677	7.5
CVE-2023-48784	6.1
CVE-2024-23662	5

**Fabricante**

Fortinet

**Productos afectados**

FortiClientLinux  
7.2.0  
7.0.6 a 7.0.10  
7.0.3 a 7.0.4  
FortiOS

**CONTACTO Y REDES SOCIALES CSIRT**

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

# Boletín de Ciberseguridad N° 249

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



BOLETÍN 13BCS24-00258-01 | Semana del 5 al 11 de abril de 2024

7.4.0 a 7.4.1  
7.2.0 a 7.2.6  
7.0.0 a 7.0.12  
6.4.0 a 6.4.14  
6.2.0 a 6.2.15  
6.0  
7.4.0 a 7.4.1  
7.2.0 a 7.2.7  
7.0.0 a 7.0.13  
2.0  
1.2  
1.1  
1.0  
FortiClientMac  
7.2.0 a 7.2.3  
7.0.6 a 7.0.10  
FortiSandbox  
4.0.0 a 4.0.4  
4.2.0 a 4.2.6  
4.4.0 a 4.4.3

#### Enlaces para revisar el informe:

<https://csirt.gob.cl/alertas/vsa24-00999>

 <b>VULNERABILIDADES ADOBE</b> VSA24-01000 CSIRT COMPARTI INFORMACIÓN DE VULNERABILIDADES QUE AFECTAN A PRODUCTOS DE ADOBE, INCLUYENDO UNA CRÍTICA	 Busca el informe de los productos afectados y el enlace para la mitigación de la vulnerabilidad en: <a href="https://csirt.gob.cl/vulnerabilidades">csirt.gob.cl/vulnerabilidades</a>	<b>Adobe, varios productos - Vulnerabilidades</b>	
		Código de alerta	VSA24-01000
		Clase de alerta	Vulnerabilidad
		Tipo de incidente	Sistema y/o Software Abierto
		Nivel de riesgo	Alto
		TLP	Blanco
		Fecha de lanzamiento original	11 de abril de 2024
		Última revisión	11 de abril de 2024
		<b>CVE y puntaje CVSS</b>	
		CVE-2024-20758	9
		CVE-2024-20759	8.1
		CVE-2024-26046	5.4
		CVE-2024-26047	5.4
		CVE-2024-26079	5.4
		CVE-2024-26084	5.4
		CVE-2024-26087	5.4
		CVE-2024-26097	5.4
		CVE-2024-26098	5.4
		CVE-2024-26122	5.4
		CVE-2024-20778	5.4
		CVE-2024-20779	5.4
		CVE-2024-20780	5.4
		CVE-2024-26076	5.3
		CVE-2024-30271	7.8
		CVE-2024-30272	7.8
		CVE-2024-30273	7.8
		CVE-2024-20798	5.5
		CVE-2024-20771	5.5
		CVE-2024-20737	5.5
		CVE-2024-20770	5.5
		CVE-2024-20766	5.5

## CONTACTO Y REDES SOCIALES CSIRT

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

# Boletín de Ciberseguridad N° 249

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



BOLETÍN 13BCS24-00258-01 | Semana del 5 al 11 de abril de 2024

CVE-2024-20772 7.8

## Fabricante

Adobe





## Productos afectados


Adobe Commerce  
2.4.7-beta3 y anteriores  
2.4.6-p4 y anteriores  
2.4.5-p6 y anteriores  
2.4.4-p7 y anteriores  
2.4.3-ext-6 y anteriores  
2.4.2-ext-6 y anteriores  
2.4.1-ext-6 y anteriores  
2.4.0-ext-6 y anteriores  
2.3.7-p4-ext-6 y anteriores  
Magento Open Source  
2.4.7-beta3 y anteriores  
2.4.6-p4 y anteriores  
2.4.5-p6 y anteriores  
2.4.4-p7 y anteriores  
Adobe Experience Manager (AEM)  
AEM Cloud Service (CS)  
6.5.19 y anteriores  
Adobe Animate  
2023 23.0.4 y anteriores  
2024 24.0.1 y anteriores  
Adobe Illustrator  
28.3 y anteriores  
27.9.2 y anteriores  
Adobe Bridge  
13.0.6 y anteriores  
14.0.2 y anteriores  
Adobe After Effects  
24.1 y anteriores  
23.6.2 y anteriores  
Adobe Photoshop  
24.7.2 y anteriores  
25.3.1 y anteriores  
Adobe InDesign  
ID19.2 y anteriores  
ID18.5.1 y anteriores  
Adobe Media Encoder  
24.2.1 y anteriores  
23.6.4 y anteriores

## Enlaces para revisar el informe:

<https://csirt.gob.cl/alertas/vsa24-01000>


## CONTACTO Y REDES SOCIALES CSIRT

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



**VULNERABILIDADES  
SAP**

**VSA24-01001 CSIRT COMPARTO  
INFORMACIÓN DE VULNERABILIDADES  
PARCHADAS POR SAP EN SU SAP  
SECURITY PATCH DAY DE ABRIL 2024**



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

### SAP Security Patch Day Abril 2024 - Vulnerabilidades

Código de alerta	VSA24-01001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de abril de 2024
Última revisión	11 de abril de 2024

#### CVE y puntaje CVSS

CVE-2024-27899	8.8
CVE-2024-25646	7.7
CVE-2024-27901	7.2
CVE-2024-30218	6.5
CVE-2024-28167	6.5
CVE-2022-29613	6.5
CVE-2023-40306	6.1
CVE-2024-27898	5.3
CVE-2024-30214	4.8
CVE-2024-30215	4.8
CVE-2024-30216	4.3
CVE-2024-30217	4.3





#### Fabricante

SAP

#### Productos afectados

SAP NetWeaver AS Java User Management Engine  
 SERVERCORE 7.50  
 J2EE-APPS 7.50  
 UMEADMIN 7.50  
 SAP BusinessObjects Web Intelligence  
 4.2  
 4.3  
 SAP Asset Accounting  
 SAP\_APPL 600  
 SAP\_FIN617  
 SAP\_FIN 618  
 SAP\_FIN700  
 SAP Edge Integration Cell  
 Anteriores a 8.13.5  
 SAP NetWeaver AS ABAP and ABAP Platform  
 KRNL64NUC 7.22  
 KRNL64NUC 7.22EXT  
 KRNL64UC 7.22  
 KRNL64UC 7.22EXT  
 KRNL64UC 7.53  
 KERNEL 7.22  
 KERNEL 7.53  
 KERNEL 7.77  
 KERNEL 7.85  
 KERNEL 7.89  
 KERNEL 7.54  
 KERNEL 7.93  
 SAP Group Reporting Data Collection (Enter Package Data)  
 S4CORE 104  
 S4CORE 105  
 S4CORE 106

## CONTACTO Y REDES SOCIALES CSIRT

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



# Boletín de Ciberseguridad N° 249

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







BOLETÍN 13BCS24-00258-01 | Semana del 5 al 11 de abril de 2024

S4CORE 107  
S4CORE 108  
SAP\_GRDC\_CLOUD 1.0.0  
SAP Employee Self Service (Fiori My Leave Request)  
605  
SAP S/4HANA (Manage Catalog Items and Cross-Catalog search)  
S4CORE 103  
S4CORE 104  
S4CORE 105  
S4CORE 106  
SAP NetWeaver (tc~esi~esp~grmg~wshealthcheck~ear)  
7.50  
SAP Business Connector  
4.8  
SAP S/4 HANA (Cash Management)  
S4CORE 103  
S4CORE 104  
S4CORE 105  
S4CORE 106  
S4CORE 107  
S4CORE 108

**Enlaces para revisar el informe:**

<https://csirt.gob.cl/alertas/vsa24-01001>

## CONTACTO Y REDES SOCIALES CSIRT

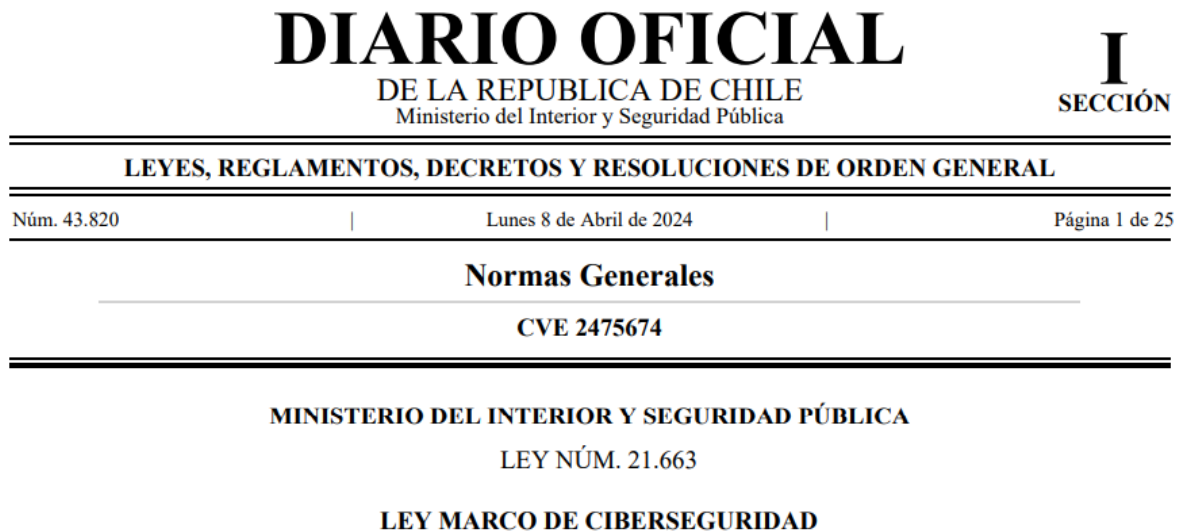
 <https://www.csirt.gob.cl>  
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl  
 @csirtgob  
 <https://www.linkedin.com/company/csirt-gob>

## 4. Noticias y concientización

### Ley Marco de Ciberseguridad es publicada en el Diario Oficial

Este lunes 8 de abril fue publicada la nueva ley marco, que tiene por objetivo establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y de los particulares que prestan servicios esenciales para el funcionamiento del país..

La nota completa aquí: <https://ciberseguridad.gob.cl/noticias/ley-marco-de-ciberseguridad-es-publicada-en-el-diario-oficial/>



The image shows a thumbnail of the official Chilean newspaper page. At the top, it reads "DIARIO OFICIAL DE LA REPUBLICA DE CHILE" and "Ministerio del Interior y Seguridad Pública". To the right, it says "I SECCIÓN". Below this, it states "LEYES, REGLAMENTOS, DECRETOS Y RESOLUCIONES DE ORDEN GENERAL". The page number is "Núm. 43.820", the date is "Lunes 8 de Abril de 2024", and it is "Página 1 de 25". The main title of the law is "Normas Generales" with the identifier "CVE 2475674". At the bottom, it reads "MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA", "LEY NÚM. 21.663", and "LEY MARCO DE CIBERSEGURIDAD".

Con la publicación en el Diario Oficial, la Ley N°21.663 Marco de Ciberseguridad se convierte en ley el modelo de gobernanza en ciberseguridad, lo que representa un avance importante en materia de seguridad digital para todos los ciudadanos, y un paso que pone a Chile en la vanguardia a nivel latinoamericano.

En la ley se se crean las siguientes capacidades:

- La Agencia Nacional de Ciberseguridad (ANCI)
- El Consejo Multisectorial, mientras que se mantiene el Comité Interministerial de Ciberseguridad
- La Red de Conectividad Segura del Estado
- El CSIRT Nacional y el CSIRT de Defensa

Además, la nueva ley define los servicios esenciales, es decir, aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional, los prestados bajo concesión de servicio público y por aquellas instituciones privadas que realicen las siguientes actividades: generación, transmisión

### CONTACTO Y REDES SOCIALES CSIRT

o distribución eléctrica; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios digitales y servicios de tecnología de la información gestionados por terceros; transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios postales y de mensajería; y prestación institucional de salud por entidades tales como hospitales y clínicas.

Así también, la agencia podrá designar otros servicios como esenciales cuando su afectación cause un grave daño a la vida o integridad física de la población o a su abastecimiento.

Cabe destacar que los servicios esenciales tendrán dos obligaciones: el deber de adoptar medidas permanentes para prevenir, reportar y resolver incidentes de ciberseguridad: protocolos y estándares de la ANCI o sectoriales; y el deber de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos.

Por otra parte, **la ANCI designará a algunos prestadores de servicios esenciales como Operadores de Importancia Vital (OIV)** cuando cumplan con los siguientes requisitos:

Que la provisión de dicho servicio dependa de las redes y sistemas informáticos, y  
Que la afectación, interceptación, interrupción o destrucción de sus servicios tenga un impacto significativo en la seguridad y el orden público, en la provisión continua y regular de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado o, en general, de los servicios que éste debe proveer o garantizar. Así también, la Agencia podrá calificar como operadores de importancia vital a instituciones privadas que, aunque no tengan la calidad de prestadores de servicios esenciales, reúnan los requisitos y sean indispensables por haber adquirido un rol crítico en el abastecimiento de la población, la distribución de bienes o la producción de aquéllos indispensables o estratégicos para el país.

## Obligaciones

### Reportar

Una vez que se publiquen el o los decretos con fuerza de Ley por parte del Presidente de la República, todas las instituciones públicas y privadas (definidas en el artículo 4°) tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que tengan un efecto significativo en plazo máximo de tres horas contado desde que se tiene conocimiento del incidente, en un esquema progresivo donde los servicios tendrán 72 horas para enviar una descripción más detallada del incidente, y luego 15 días corridos para enviar un informe completo del incidente.

### Deberes generales

Las instituciones obligadas por la Ley Marco de Ciberseguridad deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

## SheSecures Chile: En busca de aumentar la participación de mujeres en ciberseguridad

“Me parece genial que existan este tipo de iniciativas para motivar no solo a que más mujeres aprendan respecto a ciberseguridad, sino para ayudarnos a entender el verdadero impacto que puede tener usar prácticas poco seguras”, asegura María Ignacia Sánchez, una de las ganadoras de SheSecure, la competencia internacional de ciberseguridad que se llevó a cabo por primera vez en Chile entre el 28 y 30 de marzo.

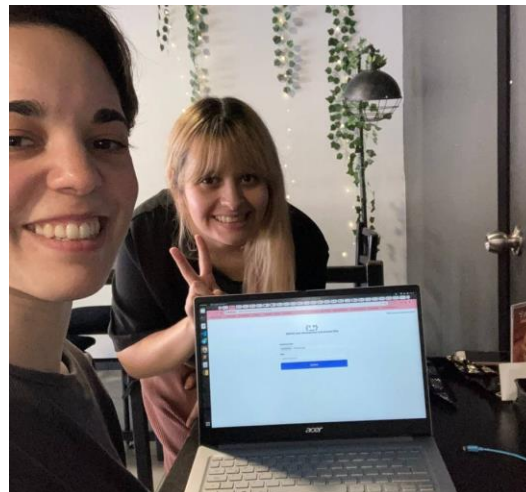
La actividad es una iniciativa que impulsa la Organización de los Estados Americanos (OEA) con el fin de contribuir a aumentar la participación de las mujeres en ciberseguridad. Comprometidos con este objetivo, el CSIRT de Gobierno colaboró en la realización de este evento para así motivar y generar espacios de aprendizaje y colaboración en las mujeres.

La nota completa: <https://ciberseguridad.gob.cl/noticias/shesecures-chile-2024/>.

Michelle Bordachar, asesora jurídica y legislativa de la Coordinación Nacional de Ciberseguridad, dio la bienvenida a las participantes, enfatizando en que esta iniciativa “contribuye a disminuir la brecha de género en ciberseguridad y a promover la diversidad en esta industria, incentivando e inspirando mujeres y niñas a desarrollar sus habilidades técnicas y aprender más sobre este campo”. Y agregó que es necesario que “el Estado genere las condiciones para disminuir estas brechas, incentivando que una mayor cantidad de mujeres escoja estudiar carreras relacionadas con ciberseguridad y promoviendo un aumento de la participación femenina del sector, especialmente considerando que las mujeres representan un 52.4% de la población chilena”.

La competencia duró dos días y reunió a 41 equipos, siendo “Cyberia” compuesto por María Ignacia Sánchez y Constanza Villegas, “Rainbow Warriors” (a la derecha) con Paola de la Vega y Gabriela Mayro, como integrantes; “Azuka Unap” de Bárbara Callejas y “Endémicas”, conformado por María Jesús Pérez, estuvieron disputando los tres primeros lugares.

Finalmente, Cyberia tomó la delantera, coronándose como ganadoras del certamen con 325 puntos. El segundo lugar lo obtuvo “Rainbow Warriors” y el tercero “Azuka Unap”.



## CONTACTO Y REDES SOCIALES CSIRT





## Ciberguía Operación Renta 2024

Como CSIRT de Gobierno entregamos a la comunidad una nueva ciberguía con las principales recomendaciones y ciberconsejos para evitar caer en estafas y fraudes digitales esta Operación Renta. Para esto, incluimos también algunos ejemplos típicos de phishing donde se suplanta a las instituciones más relevantes.

Pueden encontrar la ciberguía completa aquí, para descargar en formato PDF: <https://ciberseguridad.gob.cl/ciberconsejos/ciberguia-operacion-renta-2024/>



### CONTACTO Y REDES SOCIALES CSIRT

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

## Ciberconsejos | Phishing, smishing y vishing

En esta ocasión, desde el CSIRT de Gobierno les explicamos en qué consiste un phishing y dos de sus variantes, el smishing y el vishing. El phishing es la forma más usada por los ciberdelincuentes para engañar a las personas, y consiste en intentar convencer al destinatario de un mensaje de descargar un malware, hacer clic en un link malicioso, o entregar al remitente información confidencial, como datos bancarios, de la persona o su empresa.

Los consejos completos: <https://ciberseguridad.gob.cl/ciberconsejos/ciberconsejos-operacion-renta-2024/>



**CIBERCONSEJOS**  
**PHISHING**  
**SMISHING**  
**VISHING**  
**¡CONOCE LAS DIFERENCIAS!**

**Phishing: la amenaza más común**

Es la forma más usada por los ciberdelincuentes para engañar a las personas. Consiste en intentar convencer al destinatario de un mensaje de descargar un malware, hacer clic en un link malicioso, o entregar al remitente información confidencial, como datos bancarios, de la persona o su empresa.

Para lograrlo, los delincuentes se hacen pasar por personas o instituciones de confianza para el receptor del mensaje.

Nunca respondas o hagas clic en enlaces no solicitados, especialmente si emplean mensajes alarmantes. Fíjate en el remitente y si tienes dudas, llama directamente a la persona o institución

**Smishing: phishing en SMS y mensajería**

Se envían mensajes fraudulentos de texto (SMS) o por apps de mensajería que parecen provenir de fuentes legítimas, como bancos o empresas, solicitando información confidencial o haciendo que la víctima haga clic en enlaces maliciosos.

**Un ejemplo de smishing**

Corre0sChile: Por favor actualice su información de dirección dentro de 24 horas o perderemos su artículo: [arco.de/bepws8](https://arco.de/bepws8)

**Vishing: phishing por voz**

Su nombre es una combinación entre voz y phishing. Constituye una variante del phishing en la cual los delincuentes utilizan llamadas telefónicas (o de voz, en apps de ese tipo) para engañar a sus víctimas.

Para ello, se hacen pasar por representantes de instituciones financieras u otras entidades legítimas, con el objetivo de obtener información personal o financiera por teléfono.

Puede combinarse con el envío de mensajes, por ejemplo, para lograr un clic en un sitio malicioso

## CONTACTO Y REDES SOCIALES CSIRT

## 5. 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

## 5. 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.

- Francisco Planzer Cárdenas
- Mauricio Andrés Alarcón Jara
- Pablo Cornejo Pérez
- Alexi Contreras
- Yerdí Carreño Valencia
- Camilo Esteban Pinto Rojas

### CONTACTO Y REDES SOCIALES CSIRT