



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 250

semana del 12 al 18 de abril de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

6

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

7

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

2

Las mitigaciones son útiles en productos de Palo Alto y PuTTY.



HASH REPORTADOS

4

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



CONTENIDO

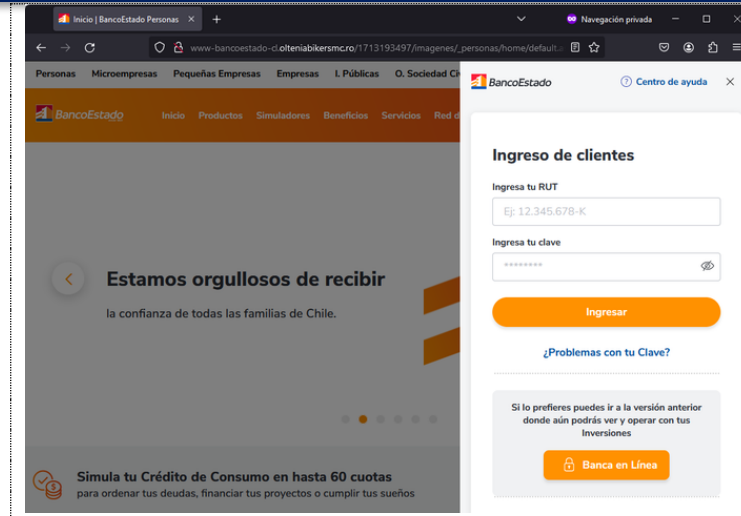
1.	Sitios fraudulentos.....	3
2.	Malware.....	4
3.	Phishing	5
4.	Vulnerabilidades.....	7
4.	Noticias y concientización.....	8
5.	Recomendaciones y buenas prácticas	10
5.	Muro de la Fama	11

Boletín de Ciberseguridad N° 250

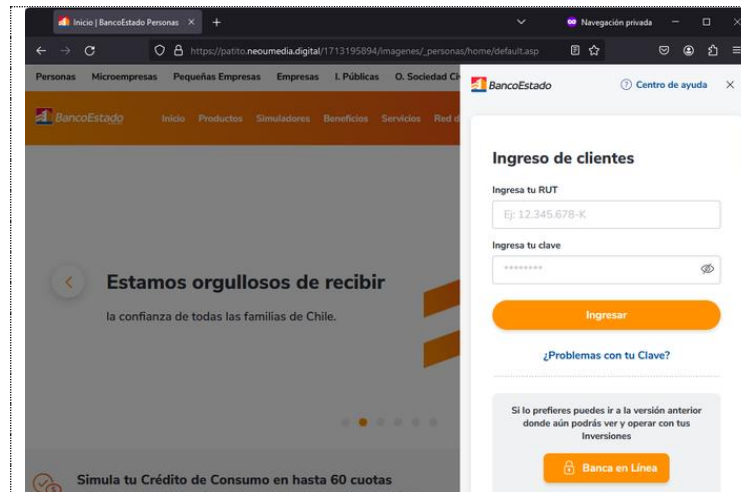
Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

BOLETÍN 13BCS24-00259-01 | Semana del 12 al 18 de abril de 2024

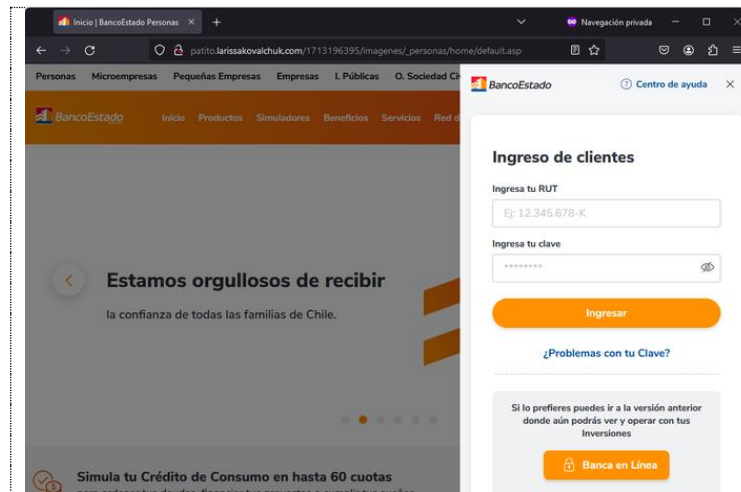
1. Sitios fraudulentos



BancoEstado - Falsificación	
Código de alerta	FFR24-01677
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2024
Última revisión	15 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
http://www-bancoestado-cl.olteniabikersmc.ro/1713193497/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[37.156.180.190]	
Enlace para revisar loC:	
https://csirt.gob.cl/alertas/8ffr24-01677/	



BancoEstado - Falsificación	
Código de alerta	FFR24-01678
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2024
Última revisión	15 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://patito.neoumedia.digital/1713195894/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[203.161.53.92]	
Enlace para revisar loC:	
https://csirt.gob.cl/alertas/8ffr24-01678/	



BancoEstado - Falsificación	
Código de alerta	FFR24-01679
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2024
Última revisión	15 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
http://patito.larissakovalchuk.com/1713196395/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[122.201.66.57]	
Enlace para revisar loC:	
https://csirt.gob.cl/alertas/8ffr24-01679/	

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>

2. Malware

<p>Factura no pagada, Marzo - 2024</p> <p>CL CGE La Compañía General de Electricidad. <support@bvgo.nl> Para [redacted]</p> <p>CGE La Compañía General de Electricidad S.A.</p> <p>Hola, [redacted]</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 pags.) <small>(solo versión para windows no se permite la vista en celulares)</small></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 recuerde que la versión de este documento es únicamente para PC no funciona en dispositivos móviles.</p> <p>#EntregamosEnergía</p> <p>©CGE-MARZO 2024</p>	<p>Compañía General de Electricidad (CGE) - Suplantación con malware</p> <table border="1"><tr><td>Código de alerta</td><td>CMV24-00458</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>Indicadores de compromiso</p> <p>Asunto REQUERIMIENTO PARA RESOLVER EL TRÁMITE- Últimos días. - (7322458)</p> <p>Correo de salida support@bvgo.nl support@the-californian.digipreprod.fr support@cynthiashomesonline.com support@thenonproffitimes.com</p> <p>SHA256 0b54964ac1a1b50ba932561aee89eb9e21c388a2f1ce8034399b79dc078cf28971e76703ed27e2360577c159daf60e2b26d470090f80dce9fa0ecaf07139075e7e643c188a1ee3b0251b7dfcab000b7c48fd840eff35189e8a45901852e3910ae28e34fbdaff077669586dcd4e10f0ba2ca6c9973ed4d372a5c3ec3b8ad20e7</p> <p>Enlace para revisar loC: https://csirt.gob.cl/alertas/cmV24-00458/</p>	Código de alerta	CMV24-00458	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	CMV24-00458														
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


Boletín de Ciberseguridad N° 250

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

BOLETÍN 13BCS24-00259-01 | Semana del 12 al 18 de abril de 2024

3. Phishing

<p>CUENTA SUSPENDIDA</p> <p>BancoEstado <noreply@publlmailer.com> Para [Redacted]</p>  <p>Estimado(a): [Redacted]</p> <p>BancoEstado su clave de internet a vencido Su cuenta se encuentra SUSPENDIDA hasta la correcta validación de sus datos. realizada la validación su cuenta sera activado obteniendo los beneficios de banca por internet.</p> <p>Recuerda que solo tiene 48 horas despues de la fecha de vencimiento para realizar este proceso mediante el enlace que se le proporciona sera inhabilitada y tendra que acercarse a la sucursal mas cercana para su verificación respectiva.</p> <p>Evite el bloqueo desde aquí.</p> <p style="text-align: center;">Ingrese Aquí</p> <p>Este es un correo electrónico generado automáticamente. Por favor no responder.</p> <p>Por tu seguridad, sigue estos consejos:</p> <ul style="list-style-type: none"> Nunca compartas tus claves de tarjetas y de acceso a Banca en Línea o Aplicación, ni tus códigos de autorización. Siempre ingresa a www.bancoestado.cl, asegurándote que la dirección esté bien escrita. <p>Conoce más recomendaciones de seguridad de BancoEstado en www.bancoestado.cl</p> <p>Síguenos en @bancoestado Servicio WhatsApp oficial +569 5094 2279</p>	<p>BancoEstado - Phishing</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>FPH24-00950</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>15 de abril de 2024</td> </tr> <tr> <td>Última revisión</td> <td>15 de abril de 2024</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL del sitio falso https://fogape.larissakovalchuk.com/1713187838/imagenes/_personas/home/default.asp</p> <p>URL de redirección https://panavalpaiso.com/activacion/cuenta-raij/</p> <p>Dirección IP sitio falso [122.201.66.57]</p> <p>Enlace para revisar IoC: https://csirt.gob.cl/alertas/fph24-00950/</p>	Alerta de seguridad cibernética	FPH24-00950	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	15 de abril de 2024	Última revisión	15 de abril de 2024
Alerta de seguridad cibernética	FPH24-00950														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	15 de abril de 2024														
Última revisión	15 de abril de 2024														

<p>Email Service Request - Action Alert for interior.gov.cl Final Warning!!!</p> <p>MD Mail Delivery System <mailer-daemon@host214dots.com> 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>interior.gov.cl Password Center!</p>  <p>Your interior.gov.cl Password has expired and must be validated, as you want to continue</p> <p style="text-align: center;">Keep Current Password</p> <p>This email was sent to dsantander@interior.gov.cl © 2024 interior.gov.cl</p>	<p>Ministerio del Interior y Seguridad Pública - Phishing</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>FPH24-00951</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>15 de abril de 2024</td> </tr> <tr> <td>Última revisión</td> <td>15 de abril de 2024</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL del sitio falso https://cloudflare-ipfs.com/ipfs/bafybeidihzirqfqlcmm3hlceu4wshnbxk5m7cjrraps73rzwwam2rtphom/login-update%281%29.html#{Correoelectronico}</p> <p>Dirección IP sitio falso [104.17.96.13]</p> <p>Enlace para revisar IoC: https://csirt.gob.cl/alertas/fph24-00951/</p>	Alerta de seguridad cibernética	FPH24-00951	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	15 de abril de 2024	Última revisión	15 de abril de 2024
Alerta de seguridad cibernética	FPH24-00951														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	15 de abril de 2024														
Última revisión	15 de abril de 2024														

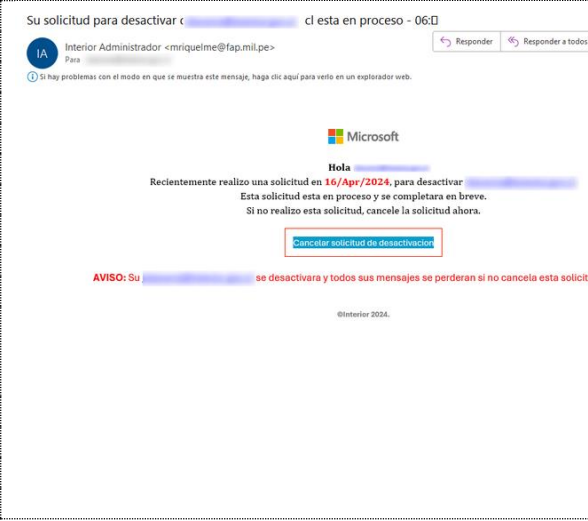
CONTACTO Y REDES SOCIALES CSIRT

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





Boletín de Ciberseguridad N° 250

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


BOLETÍN 13BCS24-00259-01 | Semana del 12 al 18 de abril de 2024

	Microsoft - Phishing	
	Alerta de seguridad cibernética	FPH24-00952
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	16 de abril de 2024
	Última revisión	16 de abril de 2024
	Indicadores de compromiso	
	URL del sitio falso	
https://cloudflare-ipfs.com/ipfs/QmfCzd6H3fmoowa2wiURc3W2nttyE6A4pzKDLL1kFfnyqL/#{Correo electronico}		
Dirección IP sitio falso		
[104.17.96.13]		
Enlace para revisar IoC:		
https://csirt.gob.cl/alertas/fph24-00952/		

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 PALO ALTO

VSA24-01002 CSIRT COMPARTIÓ INFORMACIÓN DE VULNERABILIDAD CRÍTICA QUE AFECTA A PALO ALTO PAN OS




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

Palo Alto Networks PAN-OS – Vulnerabilidades	
Código de alerta	VSA24-01002
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2024
Última revisión	12 de abril de 2024
CVE	
CVE-2024-3400	
Fabricante	
Palo Alto	
Productos afectados	
Palo Alto Networks PAN-OS	
<ul style="list-style-type: none"> • Anteriores a 11.1.2-h3 • Anteriores a 11.0.4-h1 • Anteriores a 10.2.9-h1 	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/vsa24-01002/	



VULNERABILIDADES PUTTY

VSA24-01003 CSIRT COMPARTIÓ INFORMACIÓN DE VULNERABILIDAD CRÍTICA QUE AFECTA A PUTTY



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

PuTTY y otros - Vulnerabilidades	
Código de alerta	VSA24-01003
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de abril de 2024
Última revisión	17 de abril de 2024
CVE	
CVE-2024-31497	
Fabricante	
Varios	
Productos afectados	
PuTTY 0.68 a 0.80	
FileZilla 3.24.1 a 3.66.5	
WinSCP 5.9.5 a 6.3.2	
TortoiseGit 2.4.0.2 a 2.15.0	
TortoiseSVN 1.10.0 a 1.14.6	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/vsa24-01003/	

CONTACTO Y REDES SOCIALES CSIRT

4. Noticias y concientización

Coordinador Nacional presentó en Panamá los avances legislativos de ciberseguridad

“Hoy, Chile está a la vanguardia en Latinoamérica en seguridad digital. La reciente publicación en el Diario Oficial de la Ley Marco de Ciberseguridad insta un modelo de gobernanza que no existe en América Latina, que representa un orgullo y un desafío. Esto, ya que la implementación de la ley traerá importantes beneficios a nuestro país en materia de regulación, coordinación, prevención y contención de incidentes”, aseguró Daniel Álvarez, Coordinador Nacional de Ciberseguridad de Chile.



Álvarez fue uno de los expositores del nuevo capítulo de las IV Jornadas STIC, actividad que organiza el Centro Criptológico Nacional (CCN-CNI), el Instituto Nacional de Ciberseguridad (INCIBE), el Mando Conjunto del Ciberespacio (MCCE) y RootedCON, todas de España, en conjunto con el Gobierno de Panamá, el Banco Interamericano de Desarrollo y la Organización de Estados Americanos.

En la instancia, el Coordinador Nacional indicó que “considerando el actual escenario, es necesario fomentar y fortalecer la colaboración entre los países en temas de ciberseguridad, y este tipo de actividades nos permite generar esos lazos y alianzas para que juntos trabajemos en soluciones que nos ayuden a incrementar el nivel de seguridad en el ciberespacio”.

Adicionalmente, el Coordinador Nacional de Ciberseguridad participó en el panel sobre “El rol del CSIRT en las Estrategias Nacionales de Ciberseguridad” en conjunto al responsable del CSIRT de República Dominicana y en el panel titulado “Marcos institucionales - Colaboración intersectorial” junto a los responsables de los gobiernos de Brasil, Uruguay y un representante del BID.

CONTACTO Y REDES SOCIALES CSIRT

Ciberconsejos | Cinco consejos básicos de ciberseguridad

Recomendaciones que todos debemos conocer para navegar de manera más cibersegura. ¡Compártelo con tus amigos y familiares! Pueden encontrar la campaña completa aquí, para descargar en formato PDF: <https://ciberseguridad.gob.cl/ciberconsejos/ciberconsejos-cinco-consejos-basicos-de-ciberseguridad/>



CINCO CIBERCONSEJOS BÁSICOS DE CIBERSEGURIDAD



1. Gestiona tus contraseñas

- No uses contraseñas fáciles de adivinar ni las repitas para distintas cuentas.
- Nunca envíes contraseñas por correo electrónico, ni las guardes en archivos en tu dispositivo.

Puedes probar si tu contraseña es segura en este sitio:
<https://www.security.org/how-secure-is-my-password/>

También se puede acceder a ese sitio al escanear el siguiente código QR:



2. Ten ojo con las direcciones

Cuando visitas una página web o recibes un e-mail, siempre pon atención al dominio y la dirección web sean correctos. ¡Cuidado! Suplantar páginas web y enviar correos falsos son de las formas más usadas por los ciberdelincuentes para estafar a las personas.



Aquí vemos una dirección falsa en un sitio que imita a la perfección la imagen de una web real.



3. Presta atención a las redes wifi

Desconfía de las redes wifi públicas. Las redes wifi desconocidas pueden ser intervenidas o configuradas para espiar su tráfico y extraer información como las contraseñas bancarias. Por lo mismo, evita hacer transacciones financieras en wifi públicas y en lo posible utiliza el plan de datos de tu smartphone.



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.

- Mauricio Andrés Alarcón Jara
- Jaime Rodrigo Pérez Lahaye
- Alejandra Rubilar Peña
- Nelson Salas
- Alexis Daneri

CONTACTO Y REDES SOCIALES CSIRT