CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 229

semana del 17 al 23 de noviembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

14

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

26

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

1

Las mitigaciones son útiles en productos de Fortinet.

HASHES COMPARTIDOS

3

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

CONTENIDO

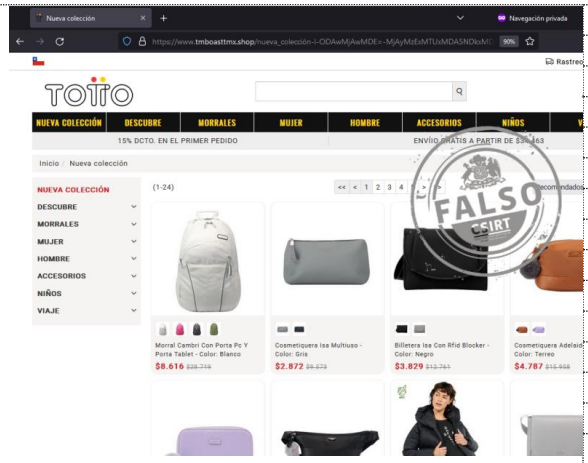
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Phishing

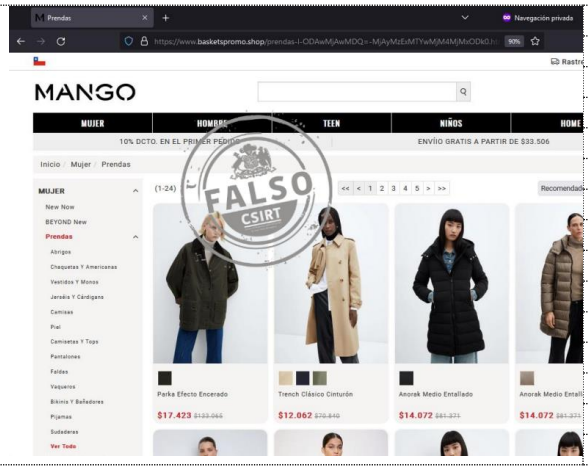
CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00909-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://serviestadohome[.]info/1699967769/imagenes/_personas/home/default.asp	
URL redirección	
https://controltotalpro[.]com/activacion/cuenta-gokl/	
Dirección IP sitio falso	
[192.185.120.230]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00909-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00910-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://patito.universalsantiveri[.]com/1700234370/imagenes/_personas/home/default.asp	
URL de redirección	
https://controltotalpro[.]com/activacion/cuenta-gokl/	
Dirección IP sitio falso	
[192.185.120.230]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00910-01/	

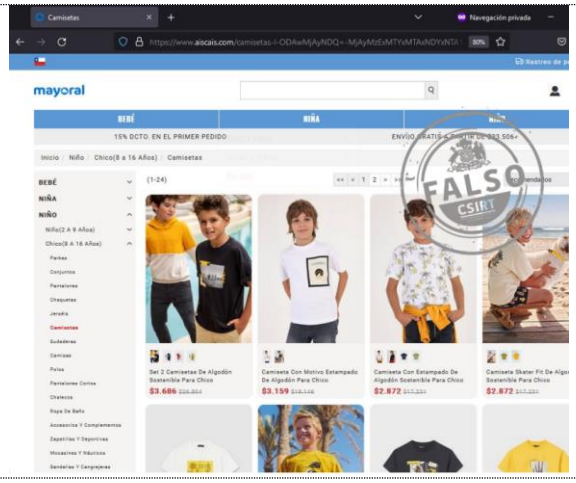
2. Sitios fraudulentos



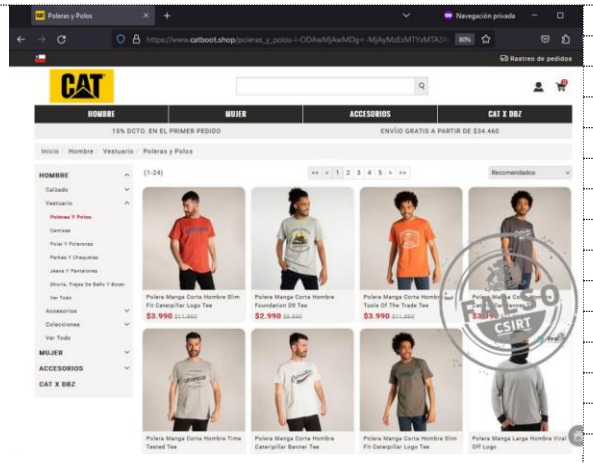
CSIRT alerta de un nuevo sitio fraudulento que suplanta a Totto	
Alerta de seguridad cibernética	8FFR23-01570-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.tmboasttmx[.]shop/	
Dirección IP sitio falso	
[198.144.149.124]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01570-01/	



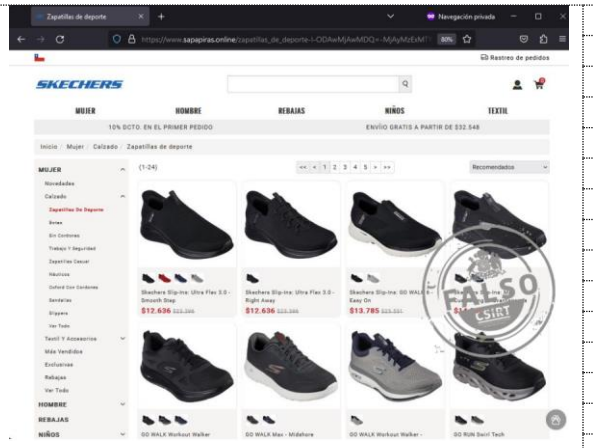
CSIRT alerta de nuevo sitio fraudulento que suplanta a Mango	
Alerta de seguridad cibernética	8FFR23-01571-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.basketspromo[.]shop/	
Dirección IP sitio falso	
[198.144.149.124]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01571-01/	



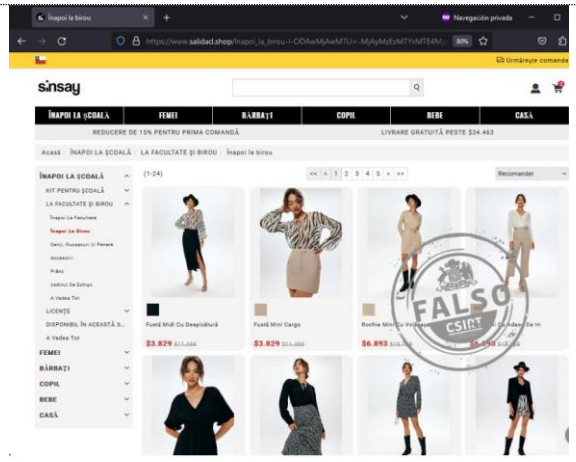
CSIRT alerta de una nueva página fraudulenta que suplanta a Mayoral	
Alerta de seguridad cibernética	8FFR23-01572-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.aiscais[.]com	
Dirección IP sitio falso	
[199.21.150.15]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01572-01/	



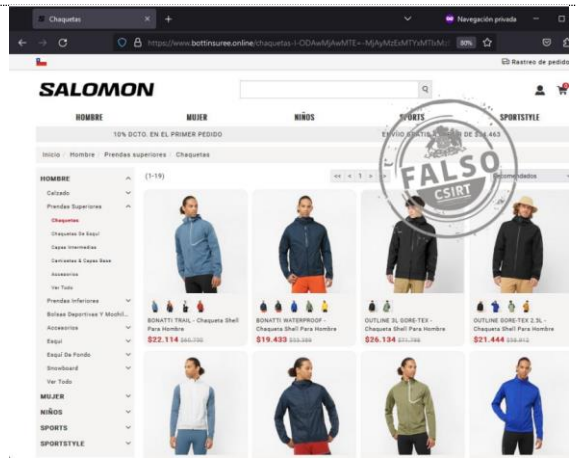
CSIRT alerta de nueva página fraudulenta que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01573-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.catboot[.]shop/	
Dirección IP sitio falso	
[199.21.150.15]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01573-01/	



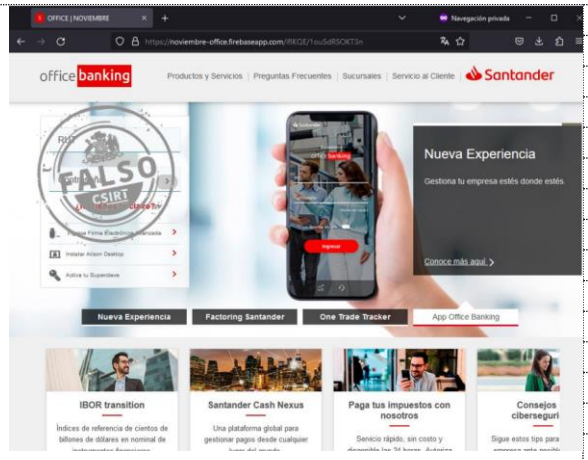
CSIRT alerta de un nuevo sitio fraudulento que suplanta a Skechers	
Alerta de seguridad cibernética	8FFR23-01574-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.sapapiras[.]online	
Dirección IP sitio falso	
[199.21.150.15]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01574-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Sinsay	
Alerta de seguridad cibernética	8FFR23-01575-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.salidacl[.]shop	
Dirección IP sitio falso	
[199.21.150.15]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01575-01/	

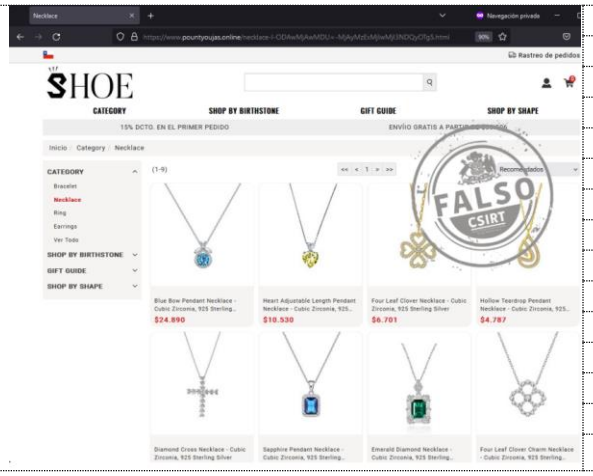


CSIRT alerta de una nueva página fraudulenta que suplanta a Salomon	
Alerta de seguridad cibernética	8FFR23-01576-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.bottinsuree[.]online/	
Dirección IP sitio falso	
[199.21.150.15]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01576-01/	

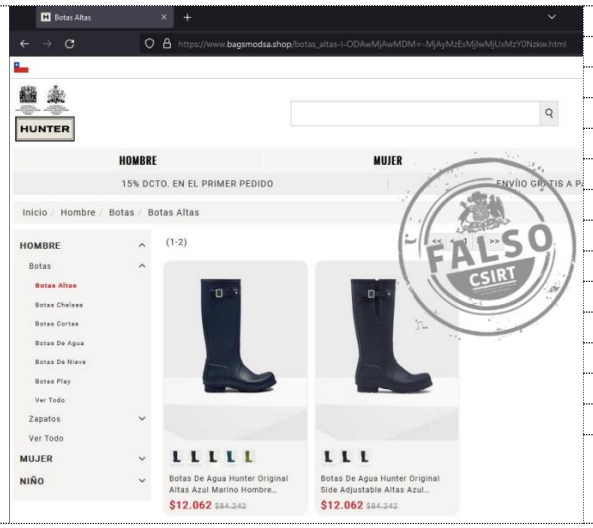


CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01577-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 noviembre, 2023
Última revisión	21 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://noviembre-office.firebaseapp[.]com/iflKQE/1ou5dRSOKT3n	
Dirección IP sitio falso	
[199.36.158.100]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01577-01/	

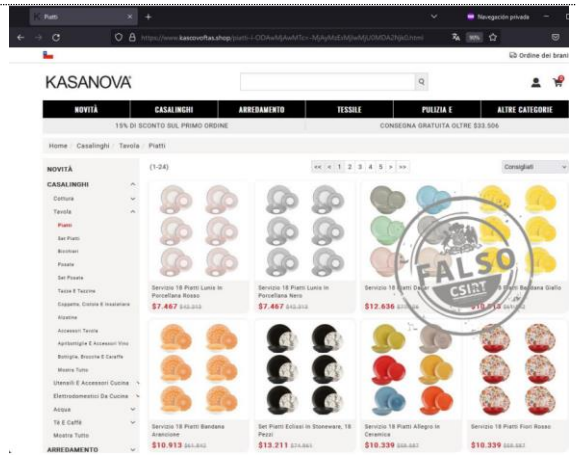
CSIRT alerta de nueva página fraudulenta que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01578-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 noviembre, 2023
Última revisión	21 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www-bancofalabella-cl.wesea-it[.]com/1700511073/home	
Dirección IP sitio falso	
[95.111.243.75]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01578-01/	



CSIRT alerta de página fraudulenta que simula ser una página de ventas online	
Alerta de seguridad cibernética	8FFR23-01579-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 noviembre, 2023
Última revisión	21 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.pountyoujas[.]online/	
Dirección IP sitio falso	
[45.141.156.98]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01579-01/	



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Hunter	
Alerta de seguridad cibernética	8FFR23-01580-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 noviembre, 2023
Última revisión	21 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.bagsmodsa[.]shop	
Dirección IP sitio falso	
[45.141.156.98]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01580-01/	



CSIRT alerta de una nueva página fraudulenta que suplanta a Kasanova	
Alerta de seguridad cibernética	8FFR23-01581-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 noviembre, 2023
Última revisión	21 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.kascovoftas[.]shop	
Dirección IP sitio falso	
[198.144.149.119]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01581-01/	

3. Malware


Acciones requeridas tras el Veredicto de Archivamiento - 606072

CA Convocatoria a Revision <info@gob.bo>
Para

Mensaje enviado con importancia Alta.

Estimado/a:

Me dirijo a usted como Laura Ramírez, **Analista de Procesos en el Área de Selección de Person**

Veredicto de Archivado Temporal: 665179.xls (8116 KB)

Cualquier pregunta que surja tras revisar el Veredicto, por favor, hágamela saber.

El no cumplimiento de las obligaciones en el plazo establecido acarreará intereses y recargos s

Agradezco su atención,

13:16:48 - 16/11/2023

CSIRT alerta de la activación de una nueva campaña de phishing con el malware Grandoreiro	
Alerta de seguridad cibernética	2CMV23-00435-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 noviembre, 2023
Última revisión	17 noviembre, 2023
Indicadores de compromiso	
URL-Dominio	
https://visualizacionrnavegadorseguro.koreacentral.cloudapp[.]azure.com/visualizacion/ https://www.dropbox[.]com/scl/fi/aelie5ljeqzmp3rzsm89k/RELACFFuobrSXHCmtjptkzg.zip?rlkey=sn2od5814mebqr0w797z5vfta&dl=1 http://54.232.33[.]91:40887/VsQHNzxx.xml http://ip-api[.]com/json 208.95.112[.]1 54.232.33[.]91	
SHA256	
429b7d4e94a270bbc55aad6c59e797d0604d4407d615a72b996f33ed9a837d266d34b216f9c95549b9e9be006e8bf15815ab437cd444ee7d2a0bafb165589a7bf2d850025dd7b65c44d979ec74a3f5a77e1c15b4070812be5656887cee95dc59	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00435-01/	

4. Vulnerabilidades

CSIRT comparte información de vulnerabilidad crítica que afecta a FortiSIEM	
Alerta de seguridad cibernética	9VSA23-00936-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 noviembre, 2023
Última revisión	21 noviembre, 2023
CVE	
CVE-2023-36553	
Fabricante	
Fortinet	
Productos afectados	
FortiSIEM 5.4 en todas sus versiones	
FortiSIEM 5.3 en todas sus versiones	
FortiSIEM 5.2 en todas sus versiones	
FortiSIEM 5.1 en todas sus versiones	
FortiSIEM 5.0 en todas sus versiones	
FortiSIEM 4.10 en todas sus versiones	
FortiSIEM 4.9 en todas sus versiones	
FortiSIEM 4.7 en todas sus versiones	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00936-01/	

5. Noticias y concientización

Ciberconsejos para una pyme segura

Desde las grandes a las medianas y pequeñas empresas, la ciberseguridad debe ser una prioridad, ya que algunos de los riesgos a los que están expuestos son:

- Robo de propiedad industrial o intelectual, poniendo en riesgo la sobrevivencia de la empresa.
- Pérdida temporal de acceso a archivos, impactando en su operación cotidiana.
- Disrupción de sitios web, afectando su presencia en internet y su reputación.
- Corrupción de programas o sistemas, incidiendo en sus desempeño operacional.
- Pérdida permanente de archivos y del acceso a servicios.

Cómo proteger a tu empresa de estos riesgos, te contamos aquí:
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-pyme/

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.

6. 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.

- Alonso Ignacio Villalobos González
- Felipe Ignacio del Rio
- Diego Bardalez Plaza

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.24 16:34:28 -03'00'