CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 240

semana del 2 al 8 de febrero de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

7

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

49

Las mitigaciones son útiles en productos de Google, Cisco y Mastodon.

HASH REPORTADOS

6

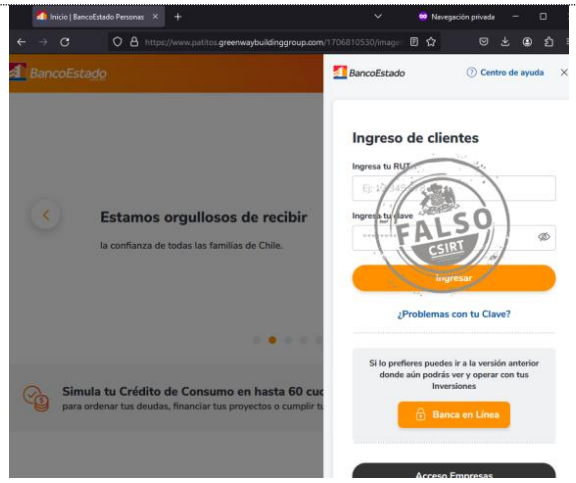
Hashes asociados a múltiples campañas de phishing con archivos que contienen malware.

CONTENIDO

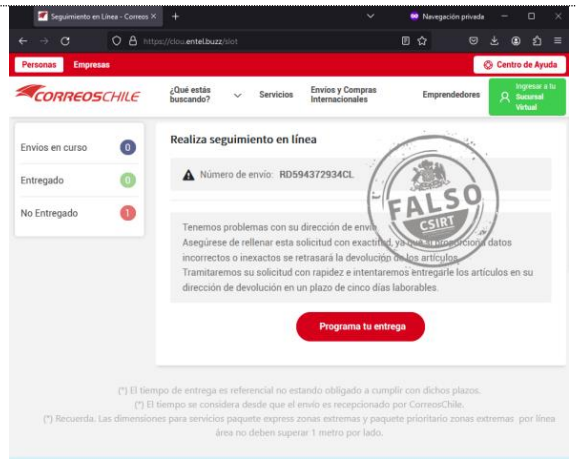
1|||||<

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

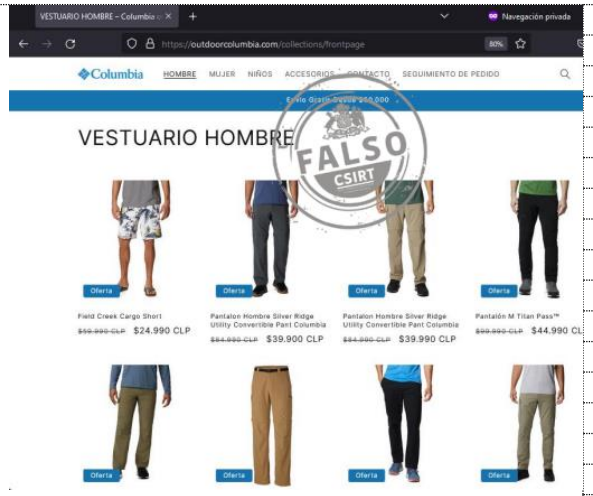
1. Sitios fraudulentos



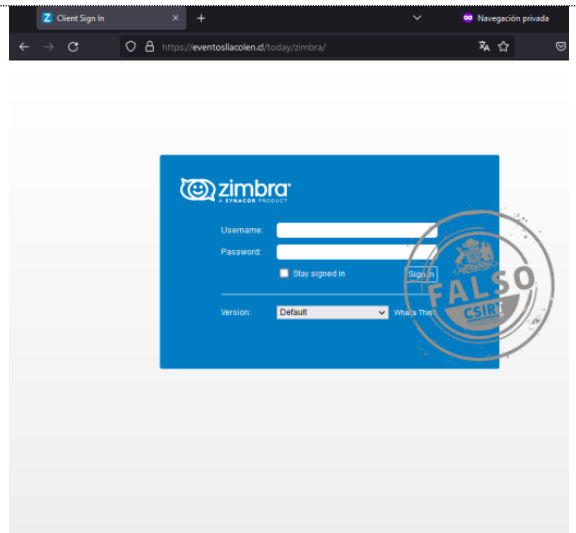
CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR24-01640-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 febrero, 2024
Última revisión	2 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.patitos.greenwaybuildinggroup[.]com/1706810530/imagenes/_personas/home/default.asp	
URL de redirección	
N/A	
Dirección IP sitio falso	
[192.185.12.111]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01640-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01641-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 febrero, 2024
Última revisión	2 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://clou.entel[.]buzz/slot	
URL de redirección	
N/A	
Dirección IP sitio falso	
[162.62.53.33]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01641-01/	

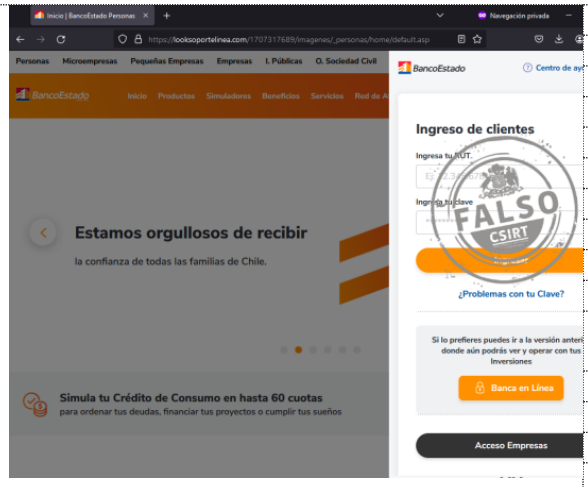


CSIRT alerta de nuevo sitio fraudulento que suplanta a Columbia	
Alerta de seguridad cibernética	8FFR23-01642-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 febrero, 2024
Última revisión	2 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://outdoorcolumbia[.]com	
URL de redirección	
N/A	
Dirección IP sitio falso	
[23.227.38.36]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01642-01/	



CSIRT alerta de nueva página fraudulenta que suplanta a Zimbra	
Alerta de seguridad cibernética	8FFR23-01643-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 febrero, 2024
Última revisión	6 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://eventosllacolen[.]cl/today/zimbra	
URL de redirección	
N/A	
Dirección IP sitio falso	
[190.107.176.64]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01643-01/	

2. Phishing



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH24-00926-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 febrero, 2024
Última revisión	7 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://looksoportelinea[.]com/1707317689/imagenes/_personas/home/default.asp	
URL de redirección	
https://underconcentral[.]com/activacion/cuenta-qdur/	
Dirección IP sitio falso	
[213.136.93.171]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00926-01/	

3. Malware

CSIRT alerta de nueva campaña de phishing con malware, en emails que suplantan a CGE	
Alerta de seguridad cibernética	2CMV24-00443-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 febrero, 2024
Última revisión	8 febrero, 2024
Indicadores de compromiso	
URL-Dominio	
https://garbasrealestate[.]com/cge/facteletricidad/?hash={mail} https://conveyancingteam[.]co.za/mymuword/factcgeeletricdad.zip?447307028	
SHA256	
c1e0f5185a2efc13b4e821ee1a2d445634e87fb380306315c482c05ae26fbd55 17a6f57be6897d2a7456ad9b0f5bc798b951c6c41b2511886706edee16c5c14c 36a9e7f1c95b82ffb99743e0c5c4ce95d83c9a430aac59f84ef3cbfab6145068 52f41817669af7ac55b1516894ee705245c3148f2997fa0e6617e9cc6353e41e b55333f085db8ef18ca3ba73a7b3984b3917d95c4f3fa57f939ebfe89c82a03c 0831dbcb3799c9e36ea586582e8ef907dcefeb2045351d6774c7ad0ef02a9af2	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/2cmv24-00443-01/	

4. Vulnerabilidades

CSIRT informa de vulnerabilidad crítica en Mastodon	
Alerta de seguridad cibernética	9VSA24-00971-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 febrero, 2024
Última revisión	5 febrero, 2024
CVE	
CVE-2024-23832	
Fabricante	
Mastodon	
Productos afectados	
Mastodon versiones anteriores 3.5.17, 4.0.x anteriores a 4.0.13, 4.1.x anteriores a 4.1.13, 7 4.2.x anteriores a 4.2.5.	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa24-00971-01/	

CSIRT comparte información de vulnerabilidades parchadas en actualización de seguridad de Android febrero 2024		
Alerta de seguridad cibernética	9VSA24-00972-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	6 febrero, 2024	
Última revisión	6 febrero, 2024	
CVE		
CVE-2024-0029	CVE-2023-5249	CVE-2023-43520
CVE-2024-0031	CVE-2023-5643	CVE-2023-43534
CVE-2024-0014	CVE-2024-20011	CVE-2023-33046
CVE-2024-0032	CVE-2024-20006	CVE-2023-33049
CVE-2024-0034	CVE-2024-20007	CVE-2023-33058
CVE-2024-0033	CVE-2024-20009	CVE-2023-33060
CVE-2024-0035	CVE-2024-20010	CVE-2023-33072
CVE-2024-0030	CVE-2023-32842	CVE-2023-33057
CVE-2024-0036	CVE-2023-32841	CVE-2023-33076
CVE-2024-0038	CVE-2023-32843	CVE-2023-43518
CVE-2024-0037	CVE-2024-20003	CVE-2023-43519
CVE-2024-0040	CVE-2023-49667	CVE-2023-43522
CVE-2023-40122	CVE-2023-49668	CVE-2023-43523
CVE.2023-40093	CVE-2023-43513	CVE-2023-43533
CVE-2023-5091	CVE-2023-43516	CVE-2023-43536
Fabricante		
Google		
Productos afectados		
Dispositivos con sistema operativo Android anteriores al 2024-02-01 security patch level.		
Enlaces para revisar el informe:		
https://csirt.gob.cl/vulnerabilidades/9vsa24-00972-01/		

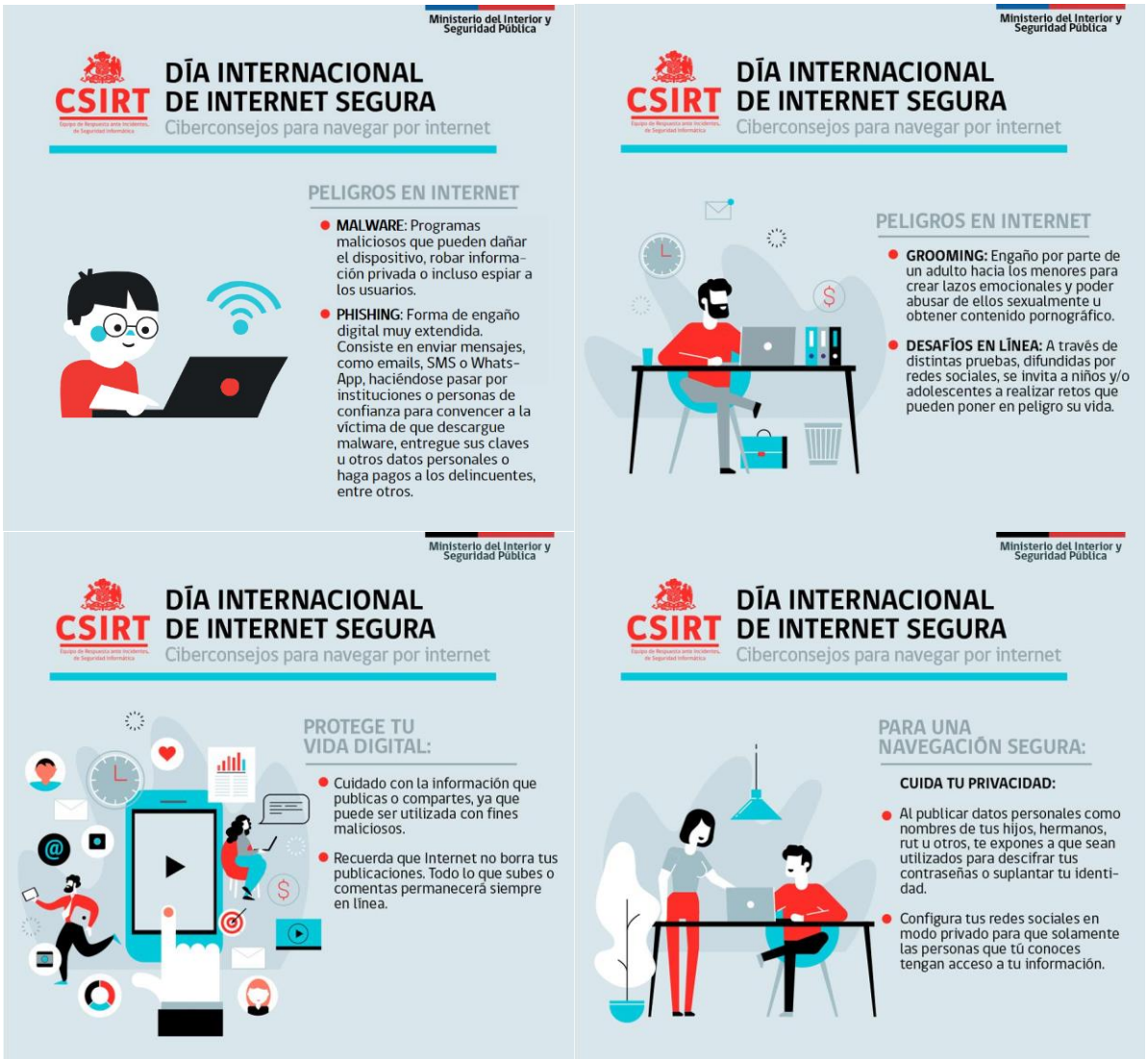
CSIRT comparte información de vulnerabilidades críticas en Cisco Expressway Series	
Alerta de seguridad cibernética	9VSA24-00973-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 febrero, 2024
Última revisión	8 febrero, 2024
CVE	
CVE-2024-20252 CVE-2024-20254 CVE-2024-20255	
Fabricante	
WatchGuard	
Productos afectados	
Cisco Expressway Series	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa24-00973-01/	

5. Noticias y concientización

Ciberconsejos para el Día de la Internet Segura 2024

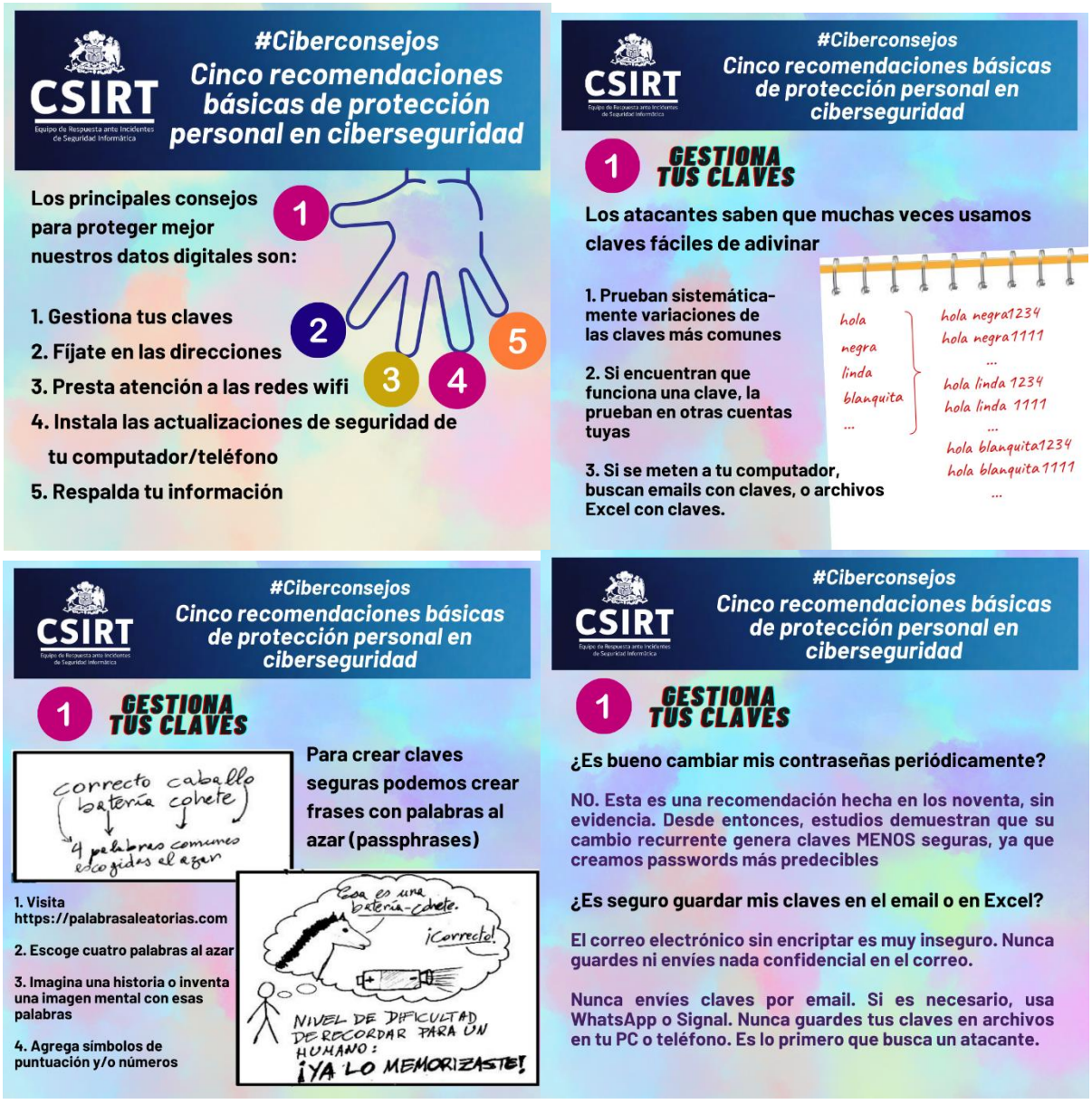
Este martes 6 de febrero se promovió en gran parte del mundo el Día Internacional de la Internet Segura, y para celebrarlo también en Chile publicamos las siguientes definiciones de peligros en línea, junto con algunas recomendaciones para navegar más seguros.

Encuéntralos en formato PDF aquí: https://csirt.gob.cl/recomendaciones/ciberconsejos-dia-internet-segura-2024/



Ciberconsejos | Cinco recomendaciones básicas de protección personal en ciberseguridad

Esta semana decidimos hacer un recordatorio sobre cómo gestionar nuestras claves de forma más segura, la primera parte de las "Cinco recomendaciones básicas de protección personal en #ciberseguridad", charlas que publicamos en video y PDF aquí: https://csirt.gob.cl/noticias/ultimas-charlas-mes-de-la-ciberseguridad-2023/



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.

- Andrés Barrientos Cisternas
- Marcelo Fabio
- Andrés Peñailillo
- Eduardo Riveros
- Wesly Rodrigo Vega Pizarro
- Ignacio Acebedo Burgos
- Felipe Cortes
- Horacio Gabriel Galleguillos Vega

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.02.09 16:46:50 -03'00'