Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

04-06-2021 | Año 3 | N°100

Boletín de Seguridad Cibernética

Semana del 28 de mayo al 03 de junio de 2021

La semana en cifras

Hash

30

SHA

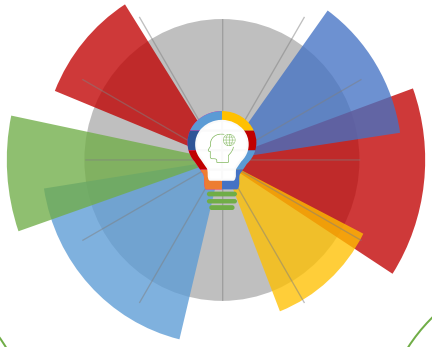
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

6

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

49

para vulnerabilidades

Las mitigaciones son útiles en productos de Mozilla, Google y Opera.

IP

44

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.

*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Malware

CSIRT advierte por campaña de phishing que suplanta al BBVA	
Alerta de seguridad cibernética	2CMV21-00187-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2021
Última revisión	31 de mayo de 2021
Indicadores de compromiso	
SHA256	
d6e727f3c218dcf962d1adcb709f689ee22d8c4f9f69ee2f4bfa39a3e763f376 bbc0947ca657f753eae1ed44b9cef04c730e8ef76d84c41901b243939dc25006	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00187-01/	
https://csirt.gob.cl/media/2021/05/2CMV21-00187-01.pdf	

CSIRT advierte nueva campaña de malware con falsa información de pago	
Alerta de seguridad cibernética	2CMV21-00189-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2021
Última revisión	3 de junio de 2021
Indicadores de compromiso	
SHA256	
2928734BB8B73D9B7C9DA9EE4BC8BE23C8F22D2FB8999A821AC23E0D716B543C 214400F77D9819CE9E81C88B9FFA42C2A6AC7FBBDF15F04E1D8D7EBAFA98289E	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00189-01/	
https://csirt.gob.cl/media/2021/06/2CMV21-00189-01.pdf	

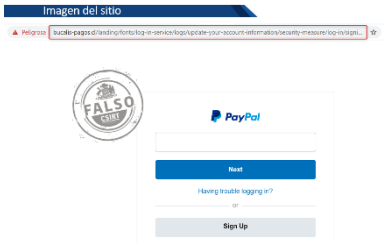
CSIRT alerta por campaña de phishing con malware a través de falsa factura	
Alerta de seguridad cibernética	2CMV21-00190-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2021
Última revisión	3 de junio de 2021
Indicadores de compromiso	
SHA256	
993403c2a403b7ac63751a627663cb897b88a1cc730e594437cbcacbbc20bf1f 790484C22FA0900159FCEA453DEDD48B9FD3CF53C72A2B538B55C0607D3E3A58	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00190-01/	
https://csirt.gob.cl/media/2021/06/2CMV21-00190-01.pdf	

IoC Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	Etiqueta de sistema autónomo	Documento web
185.143.223.26	Technology Advanced Investment Limited	4IIA21-00039-01
45.227.253.210	ru-informtech-1-mnt	4IIA21-00039-01
78.128.113.109	DirectWebH CORP	4IIA21-00039-01
185.24.233.143	Miti 2000 EOOD	4IIA21-00039-01
185.24.233.142	ServeByte VPS	4IIA21-00039-01
13.68.134.15	ServeByte VPS	4IIA21-00039-01
103.155.80.188	Microsoft Corporation	4IIA21-00039-01
91.191.209.234	VIET SPEED SERVICE COMPANY LIMITED	4IIA21-00039-01
103.155.81.125	L&L Investment Ltd.	4IIA21-00039-01
77.247.110.231	VIET SPEED SERVICE COMPANY LIMITED	4IIA21-00039-01

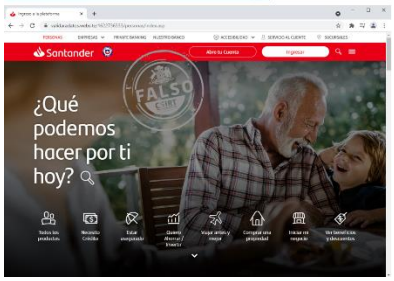
Sitios fraudulentos



CSIRT alerta por campaña de phishing que suplanta a PayPal	
Alerta de seguridad cibernética	8FFR21-00957-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de mayo de 2021
Última revisión	28 de mayo de 2021
Indicadores de compromiso	
URL sitio falso	
http://bucalis-pagos[.]cl/landing/fonts/log-in-service/logs/update-your-account-information/security-measure/log-in/signin?country.x=CL&locale.x=es_CL	
IP	
[162.241.60.178]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00957-01/	
https://www.csirt.gob.cl/media/2021/05/8FFR21-00957-01.pdf	

CSIRT alerta de página fraudulenta que suplanta a Linkedin	
Alerta de seguridad cibernética	8FFR21-00958-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2021
Última revisión	3 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://segurinorth[.]cl/linkedlin/linkedin_/login.php	
IP	
[186.64.118.120]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00958-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00958-01.pdf	

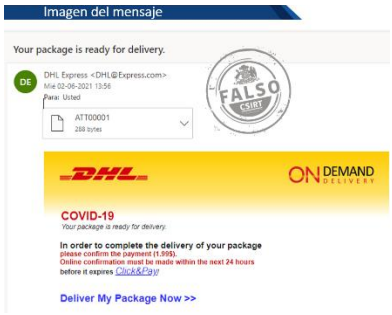
Imagen del sitio



CSIRT advierte de sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00959-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2021
Última revisión	3 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://validaradatos[.]website/1622736333/personas/index.asp	
IP	
[198.54.114.176]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00959-01/	
https://www.csirt.gob.cl/media/2021/06/8FFR21-00959-01.pdf	

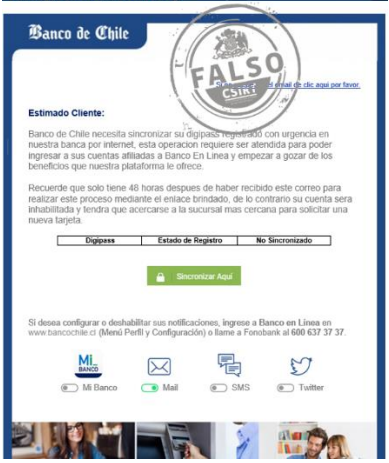
Phishing

CSIRT advierte de campaña de phishing del tipo «príncipe nigeriano»	
Alerta de seguridad cibernética	8FPH21-00403-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de mayo de 2021
Última revisión	28 de mayo de 2021
Indicadores de compromiso	
Servidor SMTP	
[209.85.222.66]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00403-01/	
https://www.csirt.gob.cl/media/2021/05/8FPH21-00403-01.pdf	



CSIRT alerta por campaña de phishing que suplanta a DHL	
Alerta de seguridad cibernética	8FPH21-00404-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2021
Última revisión	3 de junio de 2021
Indicadores de compromiso	
URL sitio falso	
https://baratinho[.]co/DHL/Shipment/Tracking/F004f19441/11644210b.php ?web=succes&local=_&id=1121856	
SMTP Host	
[111.67.23.103]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00404-01/	
https://www.csirt.gob.cl/media/2021/06/8FPH21-00404-01.pdf	

Imagen del mensaje



CSIRT alerta ante campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00405-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de junio de 2021
Última revisión	3 de junio de 2021
Indicadores de compromiso	
URL sitio redirección:	
http://shyamalaenterprises[.]com/5d3241e23d32d26cd7efdb671060f470	
URL sitio falso:	
https://bancochileportallogin.cl-bch[.]com/1622738784/persona/login	
SMTP Host	
[14876-25997.bacloud.info- 88.119.175.213]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00405-01/	
https://www.csirt.gob.cl/media/2021/06/8FPH21-00405-01.pdf	

Vulnerabilidades

CSIRT alerta por vulnerabilidades de alto riesgo en Mozilla Firefox	
Alerta de seguridad cibernética	9VSA21-00451-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de junio de 2021
Última revisión	1 de junio de 2021

CVE

CVE-2021-29964	CVE-2021-29965	CVE-2021-29963
CVE-2021-29967	CVE-2021-29960	CVE-2021-29959
CVE-2021-29966	CVE-2021-29961	CVE-2021-29962

Fabricante

Mozilla Firefox

Productos afectados

Mozilla Firefox, versiones 60.0 a 88.0.1.
Mozilla Firefox ESR, versiones 60.0 a 78.10.1.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00451-01
https://www.csirt.gob.cl/media/2021/06/9VSA21-00451-01.pdf

CSIRT alerta de vulnerabilidades en Arch Linux para Google Chrome, Chromium, Opera y Firefox	
Alerta de seguridad cibernética	9VSA21-00452-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de junio de 2021
Última revisión	2 de junio de 2021

CVE

CVE-2021-29959	CVE-2021-30515	CVE-2021-30528
CVE-2021-29960	CVE-2021-30516	CVE-2021-30529
CVE-2021-29961	CVE-2021-30517	CVE-2021-30530
CVE-2021-29966	CVE-2021-30518	CVE-2021-30531
CVE-2021-29967	CVE-2021-30519	CVE-2021-30532
CVE-2021-30506	CVE-2021-30520	CVE-2021-30533
CVE-2021-30507	CVE-2021-30521	CVE-2021-30534
CVE-2021-30508	CVE-2021-30522	CVE-2021-30535
CVE-2021-30509	CVE-2021-30523	CVE-2021-30536
CVE-2021-30510	CVE-2021-30524	CVE-2021-30537
CVE-2021-30511	CVE-2021-30525	CVE-2021-30538
CVE-2021-30512	CVE-2021-30526	CVE-2021-30539
CVE-2021-30513	CVE-2021-30527	CVE-2021-30540
CVE-2021-30514		

Fabricante

Arch Linux

Productos afectados
Arch Linux, todas las versiones.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00452-01
https://www.csirt.gob.cl/media/2021/06/9VSA21-00452-01.pdf

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.

CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash	Tipo Malware	Documento web
63befc6bb3786e74dee73c9587ca84dd8a58c9286e0cf8fe3d8cb3d57d5dac09	HTML/MsPhishing.4231!tr	2CMV21-00188-01
5b52135e0a170eafb2b9479fecbe0591cc14fc3d7cbe6e10d69ab4dd15637dfb	Malware_Generic.P0	2CMV21-00188-01
eb1d58d1abb7cfd2ebff24f51f0f29f8de57c2db6e7dd4ccbfda995d3c79eca2	MSIL/Kryptik.ABFE!tr	2CMV21-00188-01
637013751874069a4a4760441983256373b17562c2e495b065a02a1946ea242f	MSIL/Kryptik.ABFE!tr	2CMV21-00188-01
9e6994570cedbc6d1bc2b077bda2bdf38c26ab2f2d09ea3797c45d786fd1b2d9	MSIL/Kryptik.ABFE!tr	2CMV21-00188-01
9f5e5e193854fb9895b76cd77311d035898e962cad0d1b2b29b47d6c6a7bb762	MSIL/Kryptik.ABFE!tr	2CMV21-00188-01
6e362240f8c0314c8c10319312b7abe77fd4821f5ace2b8e2837e07c86f3ab75	MSIL/Kryptik.ABFE!tr	2CMV21-00188-01
6268b4d14af382d2e100b4d2c1b7b52b328378c3af21ad4760a68effebba109f	MSOffice/CVE_2017_11882.DMP!exploit	2CMV21-00188-01
6973dab1da8d0bcb8185df7aa63b8474bc9491f16f7642a347b529789f19d6da	MSIL/Kryptik.ZXG!tr	2CMV21-00188-01
f65487da822d73ed1e256fe7f2cd899fc9ccd960e3bebf4d6dd97970fe593355	MSExcel/Agent.IW!tr.dldr	2CMV21-00188-01
d0e42c37adcec6fa1a50c21d69203a5b28d22e2966cfeadbd93cadbf55275adc	MSExcel/Agent.IW!tr.dldr	2CMV21-00188-01
6896a20592c845f700ff938f1f56a9e16c875ad443ee3af1bb2cda6b058939b8	MSExcel/Agent.IW!tr.dldr	2CMV21-00188-01
eb9c42d04b0b717b5deaffe35d5ba4d5903bfc9560bfc44b99466882b00737a8	NSIS/Ninjector.J!tr	2CMV21-00188-01
5b9d8a84ee305113d9915edb5c6adf6182894fefa40e046b536971083064b5fd	MSIL/Kryptik.ZXG!tr	2CMV21-00188-01
fd80bdd9cb1cb0f140ce78a39a8c73087f27c85322ca17ed66a39026ac09c151	MSIL/Kryptik.ZXG!tr	2CMV21-00188-01
bc7b55dc8b895ede4c466b79554e95d636e4ce4c63d424424fa129b5b1a9f115	MSIL/Kryptik.ABFE!tr	2CMV21-00188-01
c0ef7eed28bd3e549da41468485c00a42101941e46d4c07a6d0e6098e62f86a9	MSIL/GenKryptik.FGBF!tr	2CMV21-00188-01
b22e70ef1e6ff0036fd8a54bd5d279ae5ddd18a719ef27de57afb5a8c6e77217	MSIL/Kryptik.ABFE!tr	2CMV21-00188-01
b1f983e596b7a482b5efd382e231495ef7589c4051362c15cb5013bfd4002a28	MSIL/Kryptik.ABFE!tr	2CMV21-00188-01

a8e061e48643e10db29180deb2ff64f3ad29d b963ab8e5e873e502393e000204	MSIL/Kryptik.ZXG!tr	2CMV21-00188-01
438e019ba7340139fd86e01963afadc594ee3 311335393cddf62c0f4b70a25b4	MSExcel/CVE_2017_11882!exploit	2CMV21-00188-01
7bc8e9198c499b6c48d39e99734d3c9081d0 eae625f5ac9a2ca4f571946a1501	MSIL/GenKryptik.FGBF!tr	2CMV21-00188-01
0f058ccb8be8dd3f2deee0431840c3216df44 e4359d4e642d8182d5cb83e1401	MSIL/GenKryptik.FGBF!tr	2CMV21-00188-01
b702c2e7c50f5f52c52bad18ca760178e235fe 158d152d0785604671361ba9a1	HTML/Phish.HHH!tr	2CMV21-00188-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso: Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

IP	Etiqueta de sistema autónomo	Documento web
31.24.230.65	Uk-2 limited	2CMV21-00188-01
180.214.238.19	Vietnam posts and telecommunications group	2CMV21-00188-01
103.125.189.175	Vietnam posts and telecommunications group	2CMV21-00188-01
104.243.41.239	Reliablesite	2CMV21-00188-01
45.137.22.42	Rootlayer web services ltd.	2CMV21-00188-01
45.15.143.151	Dedipath-llc	2CMV21-00188-01
155.94.136.153	Asn-quadranet-global	2CMV21-00188-01
67.225.226.156	Liquidweb	2CMV21-00188-01
162.241.241.32	Unifiedlayer-as-1	2CMV21-00188-01
54.240.48.3	Amazon-aes	2CMV21-00188-01
50.21.190.90	1&1 ionos se	2CMV21-00188-01
103.155.80.187	Vietnam posts and telecommunications group	2CMV21-00188-01
185.222.57.171	Rootlayer web services ltd.	2CMV21-00188-01
185.222.57.209	Rootlayer web services ltd.	2CMV21-00188-01
176.9.108.27	Hetzner online gmbh	2CMV21-00188-01
185.121.120.179	Delis llc	2CMV21-00188-01
185.222.58.149	Rootlayer web services ltd.	2CMV21-00188-01
104.47.56.41	Microsoft-corp-msn-as-block	2CMV21-00188-01

Actualidad

Presidente Piñera anuncia proyecto de ley que crea la Agencia Nacional de Ciberseguridad

El Presidente Piñera anunció, durante su Cuenta Pública 2021, la ampliación de la agenda de Seguridad Pública del Gobierno al mundo digital, con la creación de la Agencia Nacional de Ciberseguridad, proyecto desarrollado en conjunto con el CSIRT de Gobierno, dependiente de la Subsecretaría del Interior.

El proyecto de ley que establece una Agencia Nacional de Ciberseguridad, "para prevenir y combatir los delitos informáticos", en palabras del Primer Mandatario, se suma los proyectos para la creación del Ministerio de Seguridad Pública y el que define una nueva carrera funcionaria para Carabineros, prometidos también ayer como parte de la nueva agenda legislativa enfocada en mejorar la seguridad de todos los chilenos.

"Esta agencia será el órgano que entregue seguridad a los chilenos en el ciberespacio, que proteja los bienes y activos de la sociedad digital, y que se coordine con el sector privado de manera permanente para garantizar la seguridad de los ciudadanos en el ciberespacio", indica el Subsecretario del Interior, Juan Francisco Galli, "ya que no podemos olvidar que en los sectores productivos privados se concentran la mayor cantidad de las iniciativas digitales, que constituyen las nuevas infraestructuras críticas informáticas de la cuarta revolución industrial", agrega.

Galli explica que esta nueva agencia ayudará a prevenir los ciberdelitos y proteger la infraestructura crítica de la información, "reflejando claramente el modelo que en estos tres años se ha trabajado, implementado y probado con el sector público y privado, por parte del CSIRT de Gobierno con bastante éxito", señala.

Como resultado de la experiencia del trabajo del CSIRT de Gobierno desde 2018, se instauran dentro de las responsabilidades de la nueva Agencia de Ciberseguridad el estar a cargo de las instancias de comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, tanto del sector público como privado, nacionales e internacionales. Lo anterior, con el propósito además de fortalecer la confianza entre organismos y entregar una respuesta común a los riesgos del ciberespacio, previniendo las amenazas sistémicas sectoriales y evitando la expansión de los efectos perjudiciales de un incidente.

El proyecto de ley se encuentra en las revisiones finales y se espera sea presentado al Congreso en el mes de julio, siendo un proyecto innovador dentro del marco internacional, no solo porque se convierte en una de las primeras iniciativas en Latinoamérica en la materia, sino porque concentra por un lado la gobernanza en la materia y por otro la protección de la infraestructura critica de la información.

El detalle, en el sitio del CSIRT, aquí: https://www.csirt.gob.cl/noticias/presidente-pinera-anuncia-proyecto-de-ley-que-crea-la-agencia-nacional-de-ciberseguridad/.

La nota publicada por La Tercera sobre el proyecto de ley de Agencia Nacional de Ciberseguridad: https://www.latercera.com/earlyaccess/noticia/infraestructura-critica-digital-y-coordinacion-con-privados-en-que-consiste-el-proyecto-que-anuncio-pinera-sobre-una-agencia-nacional-de-ciberseguridad/MXLOYTLOK5HLDMEVXKG5QPWRPM/.

Ciberconsejos | Qué es el SIM swapping y qué hacer si se es víctima

Una modalidad de ataque cibernético de muy alto impacto es la clonación o "swapping" de la tarjeta SIM de nuestros celulares. Para estar más conscientes de este peligro y saber qué hacer si se es víctima, le dedicamos los ciberconsejos de esta semana: https://www.csirt.gob.cl/

Recomendaciones y buenas prácticas

Recomendaciones generales de seguridad

- 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 los sitios web que se ingresen sean los oficiales.

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 problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Rosa Andrea Candia Rojas
- Jonathan Fletcher Castro
- Sebastián Ignacio Maldonado Caroca
- Madelein Cristin Valdés Lobos
- Eduardo Cristóbal Escanilla Alemán
- Mariana Alexandra Ursini Pallante
- Tomás Carrasco Argomedo
- María Paz Castex
- Erika Saavedra Morales
- Claudia Negri
- Agustín Mouzo
- José Luis Heriberto Tapia Olmedo
- René Manuel Miranda
- Monserrat Canales Oportus
- Juan Pablo Contreras Lara
- Ramón Gálvez Humeres
- Alejandra Pizarro González
- Tomás Eduardo Gaete Fischer
- Valentina Fernanda Rubilar Navarro
- Deborah Gormaz
- Elías
- Victor Gregorio Gatica Núñez
- Laura Antonella Ageno Baraqui

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.04 12:31:11 -04'00'