Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

27-08-2021 | Año 3 | N°112

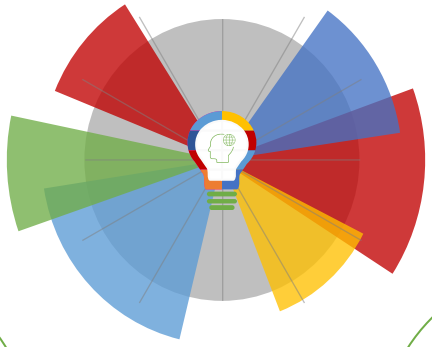
Boletín de Seguridad Cibernética

Semana del 20 al 26 de agosto 2021

La semana en cifras

Hash
26
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
8
para vulnerabilidades
Las mitigaciones son útiles en productos de Cisco y OpenSSL.

IP
18
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

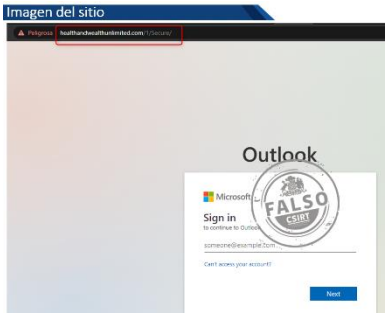
Malware

CSIRT alerta por campaña de phishing que suplanta a TNT	
Alerta de seguridad cibernética	2CMV21-00215-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de agosto de 2021
Última revisión	20 de agosto de 2021
Indicadores de compromiso	
SHA256	
2D23F05BA32B12E837AA34DD9CD41EABBEF0063579BD316A042EC79C82251F66 969FF1FB205201B293B0859D5955EFC6109549AAC06F5ED99566AB562FA1B39D	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00215-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00215-01.pdf	

CSIRT alerta ante campaña de malware con falsa cotización	
Alerta de seguridad cibernética	2CMV21-00216-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de agosto de 2021
Última revisión	26 de agosto de 2021
Indicadores de compromiso	
SHA256	
C4FF766D5EC46DC47A4EB9975953C7FBF653DA23217BBEB2C58C364FC193EF18 FBDD84D150F157C6106018A4FB1778056201DBFC806D01902AE6130E4E10DCF7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00216-01/	
https://csirt.gob.cl/media/2021/08/2CMV21-00216-01.pdf	

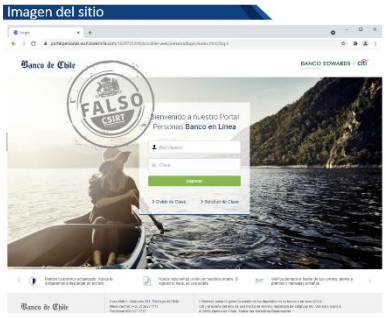
Sitios fraudulentos

Imagen del sitio



CSIRT alerta ante un sitio fraudulento que suplanta a Outlook	
Alerta de seguridad cibernética	8FFR21-01006-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de agosto de 2021
Última revisión	20 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
https://healthandwealthunlimited[.]com/1/Secure/	
IP	
[162.241.120.44]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01006-01/	
https://www.csirt.gob.cl/media/2021/08/8FFR21-01006-01.pdf	

Imagen del sitio



CSIRT alerta ante un sitio fraudulento que suplanta al BCI	
Alerta de seguridad cibernética	8FFR21-01007-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de agosto de 2021
Última revisión	23 de agosto de 2021
Indicadores de compromiso	
URL redirección	
https://bit.ly/loquin-bchile	
URL sitio falso	
http://139.99.233[.]26/16294647l0/personas	
IP	
[162.0.209.18]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01007-01/	
https://www.csirt.gob.cl/media/2021/08/8FFR21-01007-01.pdf	

Imagen del sitio

CSIRT alerta ante página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01008-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de agosto de 2021
Última revisión	23 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
http://basau[.]cl/1629731659/personas/index.asp	
IP	
[201.148.104.135]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01008-01/	
https://www.csirt.gob.cl/media/2021/08/8FFR21-01008-01.pdf	

Phishing

CSIRT alerta ante campaña de smishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH21-00429-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de agosto de 2021
Última revisión	23 de agosto de 2021
Indicadores de compromiso	
URL de SMS	
https://santander.alertascl[.]app	
URL sitio falso	
https://santander.personascl[.]website/1629731027/personas/index.asp	
IP	
[162.0.217.22]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00429-01/	
https://www.csirt.gob.cl/media/2021/08/8FPH21-00429-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidades graves en OpenSSL	
Alerta de seguridad cibernética	9VSA21-00483-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de agosto de 2021
Última revisión	25 de agosto de 2021
CVE	
CVE-2021-3711 CVE-2021-3712	
Fabricante	
OpenSSL	
Productos afectados	
OpenSSL de 1.0.2 a 1.1.1k	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00483-01	
https://www.csirt.gob.cl/media/2021/08/9VSA21-00483-01.pdf	

CSIRT alerta ante vulnerabilidades graves en productos de Cisco	
Alerta de seguridad cibernética	9VSA21-00484-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de agosto de 2021
Última revisión	26 de agosto de 2021
CVE	
CVE-2021-1577 CVE-2021-1586 CVE-2021-1523 CVE-2021-1583 CVE-2021-1584 CVE-2021-1591	
Fabricante	
Cisco	
Productos afectados	
Cisco APIC Cisco Cloud APIC Cisco Nexus 9000 Series Fabric Switches en modo ACI Cisco Nexus 9500 Series Switches	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00484-01	
https://www.csirt.gob.cl/media/2021/08/9VSA21-00484-01.pdf	

IoC Malware

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

Recomendamos 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 de archivos maliciosos	Tipo de malware	Documento web
0062a862d8ddf459bc7856c5508210b5dcd2556bca253d5e3a944da6072a11fd	MSIL/Kryptik.ACNW!tr	2CMV21-00217-01
0737d41e822019478beb9b93fed27d068b445fe4b5b43e1df783ec4b8060e825	MSIL/Kryptik.ACMW!tr	2CMV21-00217-01
20ce4ad3d1dba6ed154ef7c636999e7e7d9f1cc222fa30f55b4bf0f1970b8edb	MSIL/Kryptik.ACNW!tr	2CMV21-00217-01
23a45145326f58846289d244b9ceb1b00be99ea5e34bc401fb607ae95d388472	MSIL/Kryptik.ACNW!tr	2CMV21-00217-01
278f267f77ff83df744828fa889e70d8fa1a43ac7f72867bbe36fd15b1aa18da	MSOffice/CVE_2017_11882.C!exploit	2CMV21-00217-01
404ca6fc3bc9ad699a8ae48c4218950a975a99cc89ce7cb54aaaa3994328a871	MSIL/Kryptik.ACNW!tr	2CMV21-00217-01
41da4a11a15f11f40805f3b0297c3865fcf0555de8676eec82540016f93031ef	MSIL/Kryptik.ACMW!tr	2CMV21-00217-01
565e856482246139a5f07be019a334bbe9b8e5174f46d233b174d97eb0e7bd82	MSIL/Kryptik.ACNW!tr	2CMV21-00217-01
6a42e8f82ce75d8bd12c272c13147a60d3b8db60cf4ffd102e069a0e7ea2d1c1	MSIL/Kryptik.ACMJ!tr	2CMV21-00217-01
7d651771e88d52df36c36062179de3fb0da569bf47ddc7077454f8d79f6f91fe	MSIL/Kryptik.ACMW!tr	2CMV21-00217-01
816dea5b9076362a0ce99c77a9e800fd0b18fe3263ee659b02f232fd16a1380f	HTML/Phishing.AWP!tr	2CMV21-00217-01
8201428f0603b9fdf45a83e20cae201a1745125aed2e6da64e116c33646be43f	MSIL/Kryptik.ACNW!tr	2CMV21-00217-01
8b47e2ca0ef3079502eaa8304526f0efc23e0ba03601db1ba69495219faecd52	MSIL/Kryptik.ACNW!tr	2CMV21-00217-01
a7defcf41d31defbb13e2ee1d671df93c87c6cc5a92ed53f24d15cf3efa67f14	MSIL/Kryptik.ACMW!tr	2CMV21-00217-01
b48de45bf0990f193349d61287bb54f9a1c022752710a30b7bd5c491f004a7ef	MSOffice/CVE_2018_0798!tr	2CMV21-00217-01
bdbf7ed8832d6c75c941bd9283b964e0d4d4d8028d80abcba8656200d13e72f7	W32/GenKryptik.FJLP!tr	2CMV21-00217-01
c248f3ca02c8576b7682a9a26b35b27b9ef56c4a349b0880c370a5f401f63fac	MSIL/GenKryptik.FJEE!tr	2CMV21-00217-01

d4953c66a37f9278bc31caa24482b89a23715d8773d410a6e9320a7e1f4cbe6e	MSOffice/CVE_2017_11882.C!exploit	2CMV21-00217-01
e255f15f5259558788630152afacc7dc83c6c3967c14ee3e41319c9c9816aed9	MSIL/Kryptik.ACNW!tr	2CMV21-00217-01
e9b80d27e528c322f1c5dc32bd741c04b4df8cee6e82c019f00981a0953f291a	JS/Phish.AB38!tr	2CMV21-00217-01
eae874ad4727a1ada90f46d6ccc209364ef76bb1d31c3477622a1b31e3161f31	MSIL/Kryptik.ACMW!tr	2CMV21-00217-01
f3063315d75d9df54da2b73570e1ee4f06118e73d593346c02372d6f653a4e60	MSOffice/CVE_2017_11882.DMP!exploit	2CMV21-00217-01

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
143.244.129.103	DigitalOcean LLC	2CMV21-00217-01
40.92.51.98	Microsoft Corporation	2CMV21-00217-01
45.137.22.41	RootLayer Web Services Ltd.	2CMV21-00217-01
104.168.173.77	Hostwinds LLC.	2CMV21-00217-01
45.137.22.91	RootLayer Web Services Ltd.	2CMV21-00217-01
38.103.244.230	PSINet Inc.	2CMV21-00217-01
107.173.52.104	ColoCrossing	2CMV21-00217-01
84.38.132.116	DATACLUB-MNT	2CMV21-00217-01
103.147.184.27	NXKY Vietnam Company Limited	2CMV21-00217-01
185.222.58.110	bd-rootlayer-1-mnt	2CMV21-00217-01
185.222.57.217	bd-rootlayer-1-mnt	2CMV21-00217-01
103.156.91.208	Representative office No. 2 VietServer Services technology Ltd.	2CMV21-00217-01
103.155.82.143	VIETSPEED SERVICE COMPANY LIMITED	2CMV21-00217-01
27.102.51.187	DAOU TECHNOLOGY	2CMV21-00217-01

Nombres de archivos con malware:

N°	Archivo Malware
1	PAYMENT RECEIPT.html
2	Executed PSA Released.shtml
3	Container ETAbest offer 8796___pdf.lzh
4	Our New Order.zip

5	BANK DETAILS.zip
6	TRANSFER SLIP.zip
7	Nuevo Orden de Agosto.zip
8	Download All Attachments [NEW ORDER].zip
9	D190a.pdf.iso
10	REMITTANCE.lzh
11	PO#4500491796.r15
12	00971-210426-0001 PROFORMA INVOICE.gz
13	Imp_362 xls.zip
14	TEXGEEK SCAN AND SOFT COPY. xlsx.iso
15	Export CheckList-EXP0198121-28-25-AUG-2021_12_31_PM.xlsx
16	PRODUCTS234567.xlsx
17	PORe-Conform.zip
18	MT103-24-08-2021 756K.xlsx
19	Proforma PL BL08242021_pdf.gz

Actualidad

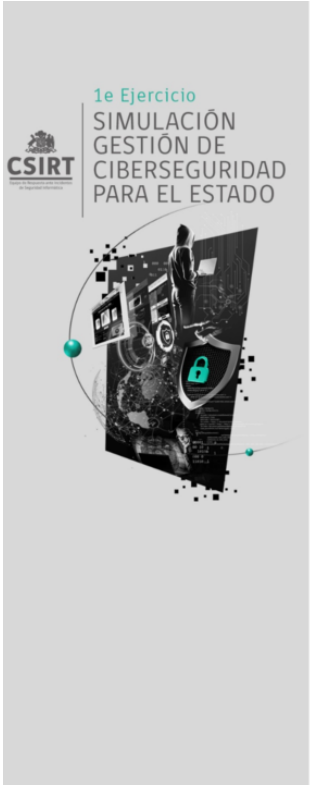
CSIRT de Gobierno realiza exitoso Primer Ejercicio de Simulación en Gestión de Ciberseguridad para funcionarios públicos

Esta semana tuvo lugar el primer ejercicio de Simulación en Gestión de Ciberseguridad para el Estado, desarrollado en conjunto por el CSIRT de Gobierno, dependiente de la Subsecretaría del Interior, y la firma de ciberseguridad Kaspersky. La instancia reunió a 250 encargados de ciberseguridad de distintas reparticiones de la Administración Pública y de empresas que tienen convenios con el CSIRT de Gobierno.

Con el objetivo de fortalecer el rol de los encargados de ciberseguridad es que los invitamos a participar de una simulación de la respuesta ante un ciberataque, realizada de una manera lúdica, entretenida y didáctica. Así, este juego de simulación pone en práctica los conocimientos de gestión y la toma de decisiones, para poder afrontar y responder de manera efectiva y eficiente ante un ciberataque en el ámbito de la administración pública, vinculando la ciberseguridad a la reputación en la gestión de las tecnologías de información dentro del Estado.

Los tres encargados de ciberseguridad que obtuvieron los mayores puntajes fueron Andrés Camacho, de la Dirección de Presupuesto, Ítalo Foppiano, de la Universidad de Concepción y Jorge Montiel, de Metro de Santiago.

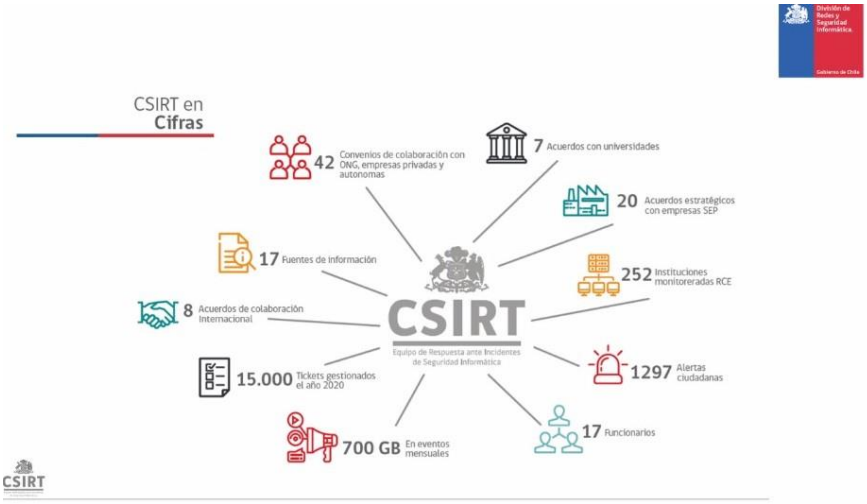
Tras el fin del ejercicio, tuvimos la alegría de constatar excelentes puntajes entre los participantes, estando así los 30 participantes con mejores resultados dentro de los 10 valores más altos, existiendo numerosos empates. Más orgullo aún nos causa el que el ranking fuera en su mayoría liderado por funcionarios de órganos del Estado y empresas públicas.

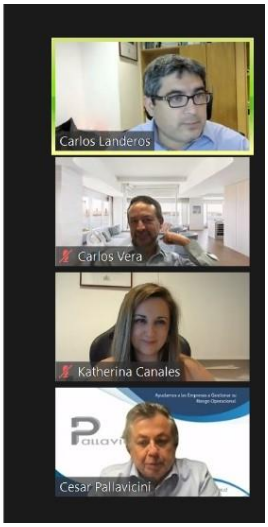


1°	Andrés Camacho	Dirección de Presupuesto
2°	Ítalo Foppiano	Universidad de Concepción
3°	Jorge Montiel	Metro de Santiago
4°	Abraham Almarza	Ministerio de Bienes Nacionales
4°	Hugo Moreno	Tesorería General de la República
5°	Cristián Mella	Fiscalía Nacional Económica
5°	Marcelo Rojo	Fiscalía Nacional Económica
5°	Diego Cancino	SB Pay
5°	Daniel Muñoz	Subsecretaría de Desarrollo Regional
6°	Fernando Jofré	Servicio de Evaluación Ambiental
6°	Cristián Silva	Oficina de Estudios y Políticas Agrarias
6°	Nicol Jeria	Agencia Nacional de Educación
7°	Fabián Acevedo	Subsecretaría de Energía
7°	Ariel Urrea	Junta Nacional de Auxilio Escolar y Becas
7°	Patricio Núñez	Superintendencia de Casinos de Juego
7°	Alejandro Figueroa	Dipreca
7°	Guillermo Meneses	Superintendencia de Seguridad Social
7°	Carlos Morales	Comisión para el Mercado Financiero
7°	Alejandro Figueroa	Dirección de Previsión de Carabineros
7°	Johan Palma Burrows	Econssa Chile
7°	Viterba Ordóñez	Servicio Médico Legal
7°	Tania Estrada	Instituto de Seguridad Laboral
7°	Roberto Siña	Estado Mayor Conjunto
8°	Francisco Barrera	Instituto de Salud Pública
8°	Rodrigo Ramírez	Consejo Nacional de Educación
8°	Marcelo Cancino	Servicio de Salud Ñuble
8°	Alexis Ubilla Salinas	Ministerio de Obras Públicas
8°	Rodrigo Cerda	Servicio de Evaluación Ambiental
8°	Victor Masjuan	Sixbell
8°	Alba Sepulveda	ODEPA

La noticia, también aquí: https://www.csirt.gob.cl/noticias/csirt-de-gobierno-realiza-exitoso-primer-ejercicio-de-simulacion-en-gestion-de-ciberseguridad-para-funcionarios-publicos/.

Director del CSIRT expone sobre colaboración público-privada ante Comunidad de Profesionales de Gestión de Riesgo Operacional





En un conversatorio dirigido a la Comunidad de Profesionales de Gestión de Riesgo Operacional (GRO), el Director Nacional del CSIRT de Gobierno, Carlos Landeros, realizó una presentación explicando el rol y funciones de esta esta institución de la Subsecretaría del Interior, poniendo especial énfasis en las formas en que realiza su labor de colaboración público-privada.

En el evento, la Comunidad de Profesionales de Gestión de Riesgo Operacional fue representada por sus directores, Carlos Vera y César Pallaviccini. Esta comunidad fue fundada en 2011, originalmente para reunir a varios profesionales de la seguridad de la información y luego ampliándose a áreas como la auditoría, la gestión de calidad, el riesgo tecnológico y el derecho informático.

La noticia también la pueden leer en el siguiente enlace: https://www.csirt.gob.cl/noticias/director-del-csirt-de-gobierno-expone-sobre-colaboracion-publico-privada-ante-la-comunidad-de-profesionales-de-gestion-de-riesgo-operacional/.

Ciberconsejos | Cómo prevenir el secuestro de WhatsApp

A través del secuestro de WhatsApp, delincuentes pueden tomar control total de una cuenta en esta app. ¿Cómo evitarlo? Léalo aquí: csirt.gob.cl/recomendaciones/ciberconsejos-como-prevenir-el-secuestro-de-whatsapp/.

El Comando de la Semana | No. 14 OScanner

En la sección El Comando de la Semana esta vez compartimos OScanner, un escáner de vulnerabilidades en bases de datos Oracle.

El objetivo de estos comandos que compartimos semanalmente no es reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por el CSIRT de Gobierno.

Descarga el comando de esta semana aquí:: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-14/.

El Control de la Semana | No. 8 Perímetro de Seguridad Física

En esta Ficha de Control Normativo tratamos los principales conceptos asociados a la definición del perímetro de seguridad física de la organización, parte esencial de llevar a la práctica su Política General de Seguridad de la Información, ya que los centros de procesamientos de datos pueden verse afectados por elementos físicos como incendios, humedad, accidentes, robo, destrucción y vandalismo.

En el documento descargable a continuación, encontrarán restos consejos y otras consideraciones, parte de nuestra serie de fichas de control normativo.

Pueden descargar esta quinta ficha semanal, aquí: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-8/.

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.

- Andrés Aldana F.
- Eliezer Hernán Aguilera Mella
- Óscar Alejandro Huerta Olivares
- Jorge Antonio Fuenzalida Astudillo
- Ana María González Tobar
- Tomás Eduardo Gaete Fischer
- Patricio Ayala Zúñiga
- Carlos Eduardo Tapia Carreras
- Raúl Rodrigo Palma Orellana
- Lorena Valentina Bustamante Núñez
- Felipe Latapiatt Fuentes
- Jair Palma
- Catalina Beatriz Novoa Muñoz
- Joseph Escobar
- Marco Antonio
- Carlos Reboredo
- Victor Cofré
- C4t(.)py_01
- Rolin Soto Soto
- Dixon Andrés
- Romel Rivas
- José Ignacio Ávila Silva
- Daniel Ignacio Brown Madariaga
- Rodrigo Letsan Chiong Rayo
- Paula Alcaíno

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.08.27 17:28:12 -04'00'