Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

08-10-2021 | Año 3 | N°118

Boletín de Seguridad Cibernética

Semana del 01 al 07 de octubre de 2021

La semana en cifras

Hash

14

SHA

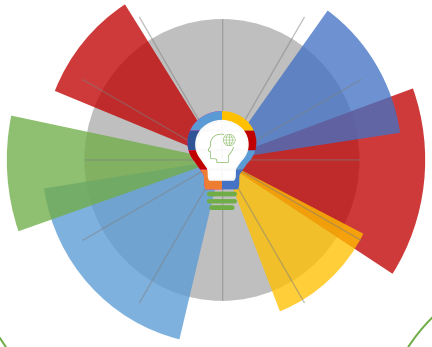
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

2

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

37

para vulnerabilidades

Las mitigaciones son útiles en productos de Cisco, Apache e IBM.

IP

1

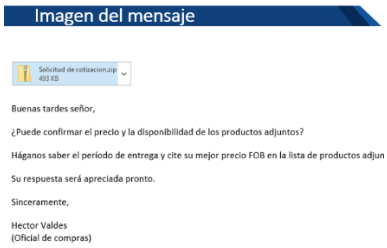
Informadas

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



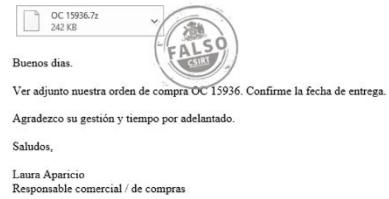
CSIRT alerta de campaña de phishing que difunde malware a través de falso documento	
Alerta de seguridad cibernética	2CMV21-00224-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de octubre de 2021
Última revisión	4 de octubre de 2021
Indicadores de compromiso	
SHA256	
6F4F6855FCDD160A4FBF8302D8E691D14C0EB042EBE3AF1136A6F32B630E0EC5 8B8286C8140567019C3A488098A614B54A627DEA794E71AB78AC73673E666702	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00224-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00224-01.pdf	

CSIRT alerta de campaña de phishing que difunde malware a través de falso documento	
Alerta de seguridad cibernética	2CMV21-00225-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de octubre de 2021
Última revisión	4 de octubre de 2021
Indicadores de compromiso	
SHA256	
62A74404A1015B4C005CE5DF182390C5023B69579B07966E007C17789DA50EA8 CE96FF74F859DEA118F58C971C56B6166FFE7960D668D0C35CE691961DE21097	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00225-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00225-01.pdf	

Imagen del mensaje

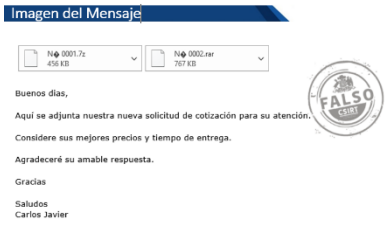
CSIRT alerta de campaña de phishing que difunde malware a través de falso documento	
Alerta de seguridad cibernética	2CMV21-00226-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de octubre de 2021
Última revisión	5 de octubre de 2021
Indicadores de compromiso	
SHA256	
7D2CF7D6F460E143C8E55CE0F4EA1F4F5C8D20374A7DB6BB25493FEE1C8DFF7A 7249D67D49A862E577120D3125E33566C61241969B4F48D701DE97A5FE0ABC04	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00226-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00226-01.pdf	

Imagen del mensaje



CSIRT alerta de campaña de phishing que difunde malware a través de falso documento	
Alerta de seguridad cibernética	2CMV21-00227-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de octubre de 2021
Última revisión	5 de octubre de 2021
Indicadores de compromiso	
SHA256	
:0B6BE9F616090F65BD7B198AFB262AD71D16A218A7119C28CB55025D33A70D30 7249D67D49A862E577120D3125E33566C61241969B4F48D701DE97A5FE0ABC04 450ABAA525D85E5E4349A9EBC13BC63724885D2EF403BCFE1A2245CF23937214	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00227-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00227-01.pdf	

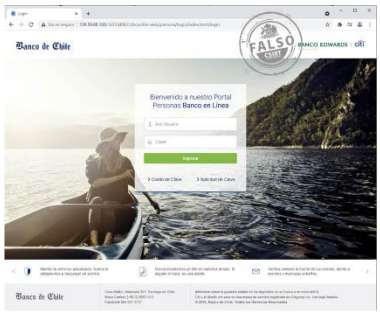
CSIRT alerta de campaña de phishing que difunde malware a través de falso documento	
Alerta de seguridad cibernética	2CMV21-00228-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de octubre de 2021
Última revisión	5 de octubre de 2021
Indicadores de compromiso	
SHA256	
5eeaa8b81eedd5136b3b945de9bf07a5840b22710b3361a0629fb85bb0f37032	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00228-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00228-01.pdf	



CSIRT alerta de campaña de phishing que difunde malware a través de falso documento	
Alerta de seguridad cibernética	2CMV21-00229-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de octubre de 2021
Última revisión	5 de octubre de 2021
Indicadores de compromiso	
SHA256	
D51EC30DA8DE0B7487119F9501A6710EA582C5B7A21E023A37F1E356BE77CEEB 44DC661DCA92EFFF41CC571F43370D5BA77280EF8D4386B6DD902334C864F2F6 :8BD2DEBCDB3C6E54B4042D937478B1CABD8AA00824687F35B1DE14990FCF0B43 184F46651603FCCCCBBA6AB8283A1551C8B41213E1B2522493E4B309E5FFCF56	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00229-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00229-01.pdf	

Phishing

Imagen del Sitio



CSIRT alerta de campaña de smishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00437-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de octubre de 2021
Última revisión	5 de octubre de 2021
Indicadores de compromiso	
URL de SMS	
https://bitly[.]com/3trinkD	
URL sitio falso	
http://139.59.88[.]100/1633348621/bcochile-web/persona/login/index.html/login	
IP	
[139.59.88.100]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00437-01/	
https://www.csirt.gob.cl/media/2021/10/8FPH21-00437-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidad crítica en IBM QRadar	
Alerta de seguridad cibernética	9VSA21-00501-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de octubre de 2021
Última revisión	4 de octubre de 2021
CVE	
CVE-2021-37967	
Fabricante	
IBM	
Productos afectados	
IBM QRadar Azure marketplace images 7.3.0 a 7.3.3 Patch 9 IBM QRadar Azure marketplace images 7.4.0 a 7.4.3 Patch 2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00501-01	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00501-01.pdf	

CSIRT advierte de vulnerabilidad de riesgo alto en Apache HTTP Server 2.4.49	
Alerta de seguridad cibernética	9VSA21-00502-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de octubre de 2021
Última revisión	6 de octubre de 2021
CVE	
CVE-2021-41773	
Fabricante	
Apache	
Productos afectados	
Apache HTTP Server 2.4.49	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00502-01	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00502-01.pdf	

CSIRT alerta de nuevas vulnerabilidades graves en productos de Cisco	
Alerta de seguridad cibernética	9VSA21-00503-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de octubre de 2021
Última revisión	7 de octubre de 2021

CVE

CVE-2021-34710	CVE-2021-34758	CVE-2020-24587
CVE-2021-34735	CVE-2021-34766	CVE-2020-24588
CVE-2021-34698	CVE-2021-34744	CVE-2020-26139
CVE-2021-34748	CVE-2021-34757	CVE-2020-26140
CVE-2021-34775	CVE-2021-34706	CVE-2020-26141
CVE-2021-34776	CVE-2021-34702	CVE-2020-26142
CVE-2021-34777	CVE-2021-34711	CVE-2020-26143
CVE-2021-34778	CVE-2021-1534	CVE-2020-26144
CVE-2021-34779	CVE-2021-34782	CVE-2020-26145
CVE-2021-34780	CVE-2021-34742	CVE-2020-26146
CVE-2021-1594	CVE-2021-34772	CVE-2020-26147
CVE-2021-34788	CVE-2020-24586	

Fabricante

Cisco

Productos afectados

Cisco ATA 190 Series Analog Telephone Adapter Software.
Cisco AsyncOS for Cisco Web Security Appliance (WSA).
Cisco Intersight Virtual Appliance.
Cisco Small Business 220 Series Smart Switches.
Cisco Identity Services Engine (ISE).
Cisco TelePresence Collaboration Endpoint (CE) Software y Cisco RoomOS Software.
Cisco Smart Software Manager On-Prem (SSM On-Prem).
Cisco Business 220 Series Smart Switches.
Cisco Identity Services Engine (ISE).
Cisco IP Phone software.
Cisco AsyncOS Software for Cisco Email Security Appliance (ESA).
Cisco DNA Center.
Cisco Vision Dynamic Signage Director.
Cisco Orbital.
Aironet 1532 APs, AP803 Integrated AP on IR829 Industrial Integrated Services Routers.
Aironet 1542 APs, Aironet 1810 APs, Aironet 1815 APs, Aironet 1832 APs, Aironet 1842 APs, Aironet 1852 APs, Aironet 1800i Aps.
Aironet 1552 APs, Aironet 1552H APs, Aironet 1572 APs, Aironet 1702 APs, Aironet 2702 APs, Aironet 3702 APs, IW 3702 Aps.
Aironet 1560 Series APs, Aironet 2800 Series APs, Aironet Series 3800 APs, Aironet Series 4800 APs, Catalyst IW 6300 APs, 6300 Series Embedded Services APs (ESW6300).
Catalyst 9105 APs, Catalyst 9115 APs, Catalyst 9120 APs, Integrated AP on 1100 Integrated Services Routers.
Catalyst 9117 AP.

Catalyst 9124 AP, Catalyst 9130 AP. Meraki GR10, GR60, MR20, MR30H, MR33, MR36, MR42, MR42E, MR44, MR45, MR46, MR46E, MR52, MR53, MR53E, MR55, MR56, MR70, MR74, MR76, MR84, MR86. Meraki MR12, MR18, MR26, MR32, MR34, MR62, MR66, MR72. Meraki MX64W, MX65W, MX67W, MX67CW, MX68W, MX68CW, Z3, Z3C. IP Phone 8861, IP Phone 8865 y IP Conference Phone 8832. IP Phone 6861 y IP Phone 8861 Running Third-Party Call Control (3PCC) Software. Wireless IP Phone 8821. Webex Desk Series y Webex Room Series. Webex Board Series. Webex Wireless Phone 840 y 860.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00503-01
https://www.csirt.gob.cl/media/2021/10/9VSA21-00503-01.pdf

Actualidad

CSIRT de Gobierno lanza campaña de consejos por el Mes de la Ciberseguridad en conjunto con miembros de CSIRTAmericas, nacida bajo el alero de la OEA

Con motivo del Mes de la Ciberseguridad, que se celebra cada octubre, 12 CSIRT del continente —organizados en CSIRTAmericas— y el Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA) se han unido para desarrollar una nueva campaña de concientización. Esta presentará tres veces a la semana, durante todo el mes, distintos consejos ilustrados y orientados a diferentes públicos. La primera semana fue realizada con miras al público general. Luego seguirán niños, niñas y adolescentes, pymes y adultos mayores.

La idea, presentada por el CSIRT del Gobierno de Chile a CSIRTAmericas y adoptada rápidamente, ha sido plasmada en imágenes en nuestro país recopilando consejos enviados por cada uno de los CSIRT partícipes: Buenos Aires y Neuquén en Argentina, Chile, Colombia, Costa Rica, Ecuador, Estados Unidos, Jamaica, Panamá, Paraguay, República Dominicana y Uruguay. Las publicaciones son hechas en inglés y castellano y podrán verlas aparecer durante todo el mes en https://twitter.com/CSIRTGOB.


CSIRTAmericas Network
Ciberconsejos para el
MES DE LA CIBERSEGURIDAD
NAVEGACIÓN SEGURA
Mantente seguro en Internet, y sigue estos consejos:
EVITA abrir archivos de origen desconocido y TEN CUIDADO con solicitudes de datos personales y contraseñas a través de correos electrónicos.
ACTIVA siempre el doble factor de autenticación para tus aplicaciones (2FA).
CSIRTAmericas Network
Ciberconsejos para el
MES DE LA CIBERSEGURIDAD
NAVEGACIÓN SEGURA
UTILIZA contraseñas robustas distintas para tus cuentas. Para esto:
INCLUYE diferentes caracteres y símbolos.
EVITA utilizar información personal (nombre, fecha de nacimiento, etc.).
CSIRTAmericas Network
Ciberconsejos para el
MES DE LA CIBERSEGURIDAD
NAVEGACIÓN SEGURA
Para navegar seguro en internet, sigue estos consejos:
BORRA el caché y cookies del navegador para limitar el rastreo por terceros de lo que visitas en internet.
UTILIZA el modo incógnito o de navegación privada para impedir que algunos sitios web rastreen tus búsquedas y navegación.
EVITA conectarte a wifi públicos, especialmente para realizar pagos o compartir datos personales o financieros
CSIRTAmericas Network
Cybertips for a new
CYBERSECURITY AWARENESS MONTH
SAFE INTERNET BROWSING
Para navegar seguro en internet, sigue estos consejos:
CLEAR your browser's cache and cookies to limit third-party tracking of what you visit on the Internet
USE incognito mode or private browsing to prevent some websites from tracking your searches and browsing
AVOID connecting to public wifi, especially to make payments or share personal or financial data
CSIRTAmericas Network
Ciberconsejos para el
MES DE LA CIBERSEGURIDAD
NAVEGACIÓN SEGURA
EVITA acceder a enlaces sospechosos, unos de los medios más utilizados para redirigir a las víctimas a sitios maliciosos son enlaces o hipervínculos
CIERRA la sesión cuando finalices una actividad en una página web a la que hayas accedido con tus credenciales (usuario y contraseña)
NUNCA realice descargas de aplicaciones desde páginas que no sean oficiales
CSIRTAmericas Network
Cybertips for a new
CYBERSECURITY AWARENESS MONTH
SAFE INTERNET BROWSING
AVOID accessing suspicious links, one of the most used means to redirect victims to malicious sites are links or hyperlinks
CLOSE the session when you finish an activity on a web page to which you have logged in with your credentials (user and password)
NEVER download applications from unofficial websites

Ciberconsejos | Recomendaciones para aprovechar este CyberMonday con seguridad

Cada nueva edición de los CyberDay y CyberMonday de la Cámara de Comercio de Santiago (CCS) exhibe nuevos récords de participantes y ventas, y debido a esta creciente popularidad es que queremos recordarles las principales recomendaciones de seguridad que es necesario seguir en internet, para evitar hacer clic en sitios maliciosos o caer en estafas digitales.

Para colaborar con la ciberseguridad de todos, también es posible revisar y compartir todos los consejos aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-cybermonday2021/.

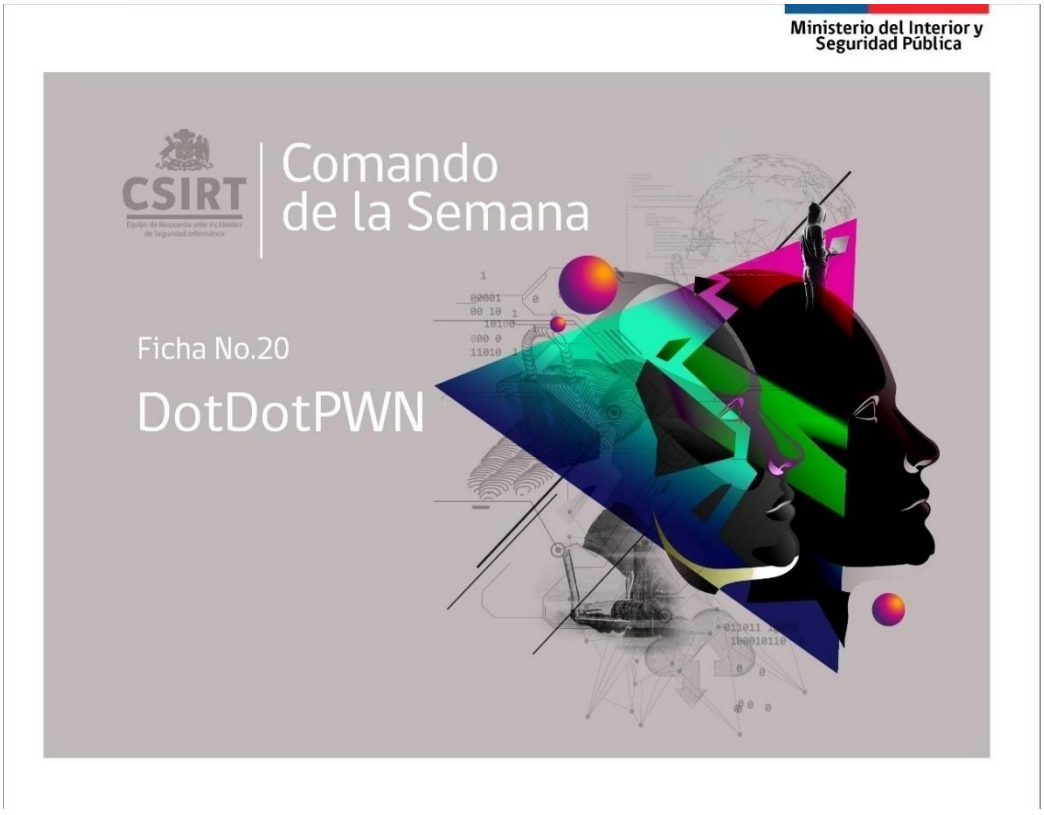

Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS PARA UN CYBERMONDAY SEGURO #Cybercl
9. PLANIFICA bien tus compras. A veces todo lo que se requiere para ser víctima de una estafa es un clic en el enlace incorrecto.
10. REVISA periódicamente tus cuentas y saldos de tarjetas. Si encuentras transacciones que no coinciden con tus compras, contacta rápidamente a tu banco.
CYBERDATO: La tasa de reclamos alcanzó 0.016% de las ventas en el último CyberMonday, según Sernac
Verifica todas las webs oficiales en www.cyber.cl
CÁMARA DE COMERCIO DE SANTIAGO
Ministerio del Interior y Seguridad Pública
CSIRT
CIBERCONSEJOS PARA UN CYBERMONDAY SEGURO #Cybercl
1. Si adviertes ofertas vías email o sitios falsos, contacta con Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT
224863850
2. Y si eres víctima de una estafa, contáctate con Brigada de Cibercrimen de la PDI
227080658
CÁMARA DE COMERCIO DE SANTIAGO

El Comando de la Semana | No. 20 DotDotPWN

El Comando de la Semana revisa en esta ocasión a DotDotPWN, un fuzzer inteligente muy flexible para descubrir vulnerabilidades de directorio transversal en software como servidores HTTP/FTP/TFTP, plataformas web como CMS, ERP, blogs, etc. Además, tiene un módulo independiente del protocolo para enviar la carga útil deseada al host y al puerto especificado. Por otro lado, también se podría utilizar en forma de scripting utilizando el módulo STDOUT.

Con los comandos que compartimos semanalmente no pretendemos 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.

Encuentra el comando de esta semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-20/.



El Control de la Semana | No. 14 Sincronización de Relojes

En esta ocasión, nuestra Ficha de Control Normativo trata sobre como establecer mecanismos de Sincronización de Relojes de todas las partes de una red, algo clave para conseguir eficiencia en los servicios, evitar complicaciones y facilitar los análisis temporales de los diferentes registros que incorporan el sello de tiempo.

En el documento descargable a continuación encontrarán todos los detalles del control de esta semana: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-14/.

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.

- Francisco Javier Gutiérrez
- Valeria Cañas
- Hanz Sandoval
- Andrés Aldana F.
- Patricio Pérez Cárcamo
- Tyr Mehamed Ravanal Rivas
- Ricardo Rojas Zurita
- Joseph de Freitas
- Jorge Rodrigo Muñoz Ubilla
- Erwin
- Fernando Enrique González Rojas
- Carina Lobel
- Esteban Vásquez Moraga

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.15 11:00:58 -03'00'