Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

19-08-2022 | Año 4 | N°163

Boletín de Seguridad Cibernética

Semana del 12 al 18 de agosto de 2022

La semana en cifras

Parches

21

para vulnerabilidades

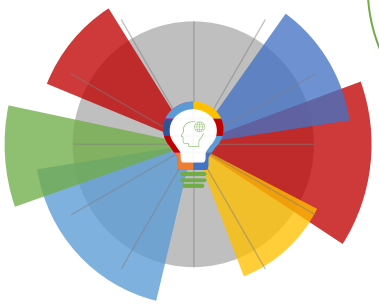
Las mitigaciones son útiles en productos de XX.

IP

4

Informadas

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



Se advirtieron

8

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

20

Asociadas a múltiples campañas de phishing con archivos que contienen malware

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

Contenido

Malware

Imagen del Mensaje

CSIRT advierte de phishing que menciona falsa conversación telefónica	
Alerta de seguridad cibernética	2CMV22-00317-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de agosto de 2021
Última revisión	11 de agosto de 2021
Indicadores de compromiso	
Asunto	
RFQ	
Correo de salida	
@haleon.com	
SHA256	
Nombre: RFQ.7z SHA256: 7d7912e50b323c06497a5a9d4a0b528a83acf29caab41a7e5a8fc2fa8688329b	
Nombre: RFQ.exe SHA256: 702a898f99fdcf56d29f5a9d4c54794c09880f7b000488a1f9f4c2259e520bee	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00317-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV22-00317-PH-01.pdf	

Imagen del Mensaje

CSIRT alerta ante campaña de phishing con malware Agent Tesla	
Alerta de seguridad cibernética	2CMV22-00318-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de agosto de 2021
Última revisión	12 de agosto de 2021
Indicadores de compromiso	
Asunto	
ORDEN DE COMPRA N°4290	
Correo de Salida	
@copreser.cl	
SHA256	
Nombre: OC4290.zip SHA256: b973f50e52f7c0b09b3570e42646b3318e6714a8befd18eafa7012d3d24e620f	

Nombre: UJkWKT0d2a2ImT9.exe SHA256: cdc5858474f99683bf2e098e9912837aa18502abaaca2a9827404abeb1ca3805	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00318-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV22-00318-PH-01.pdf	

Imagen del Mensaje

CSIRT alerta de phishing con malware que suplanta a YSA Mexicana	
Alerta de seguridad cibernética	2CMV21-00319-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de agosto de 2021
Última revisión	12 de agosto de 2021
Indicadores de compromiso	
Asunto	
RE: [EXTERNAL] RE: RE: Nuevo orden	
Correo de Salida	
@ysamexicana.com	
URL que se encuentran en la campaña	
slot999.site hagsahoy.com	familysafehidingplaces.com
howdyart.com	centericehockey.com
orders-marketplace.com	appleidd.info
ranaa.email	igctsansculottism.sbs
masterlink.guru	guiaestilosaude.online
archershut.com	happysscribe.com
weikumcommunications.com	tizzbizz.com
dphardmoney.com	qcorretor.com
shjyutie.com	baremaster.online
vivaberlin.net	liputanlima.com
mycto.today	ontherighttrack.systems
curvygirlugc.com	zzza002.xyz
otnmp.cfd	k-aashirwaad.com
alwrists.com	stillwatersagawork.com
propercandlecompany.com	skindoze.com
allindustry-bg.com	asdjmhfg.xyz
theyoungbizacademy.com	refaccionariafgnogales.com
expand658170.com	hunn.protlland.group
leslainesdumouchon.com	homebizen.com
suptisa.com	newszi.xyz
picnic-in-andong.com	nicetimecafe.net
wanligui.com	qdbs.cloud ebtl.wtf
cesarjunaro.com	dchasss.com
kuxita.xyz	kijangjantan.tech
simpkecpr.com	elegant-story.com
microsoftsecuritys.com	glimtmedia.com

responsefactor.com polyggroup.com talonxmfg.biz jam-nins.com picuar.com	1dot.online neatneighborncclean.com marionarzel.com app-arthrex.com xctech.world
SHA256	
Nombre: Se adjunta nueva lista de pedidos.zip SHA256: 2b0aba9b768f1f4449a65b2e85f0b94dde5c9ca639f3ddb38184eb65b6ed02d5 Nombre: Se adjunta nueva lista de pedidos.exe SHA256: e0c0c09b1e4bbdefaa39a956e232193ca2f5d672e0647da4a1cfc5c8b8f909e3	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00319-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV21-00319-PH-01.pdf	

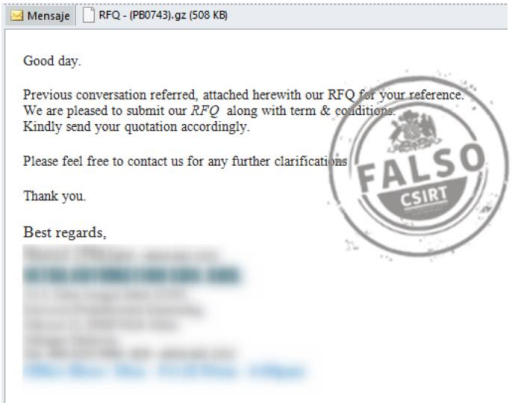
Imagen del Mensaje

CSIRT alerta por phishing con malware que suplanta a Aquarianinc	
Alerta de seguridad cibernética	2CMV22-00320-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2021
Última revisión	17 de agosto de 2021
Indicadores de compromiso	
Asunto	
Fw: RFQ_3247 A	
Correo de Salida	
@aquarianinc.net	
C2	
www.solutionwinners[.]com/p2e7/	
SHA256	
Nombre: RFQ_3247pdf A.zip SHA256: 8dc0123c60e7f240559994578b8c9f489b3d22f620d18e35214e275c9b983f87 Nombre: RFQ_3247 B.exe SHA256: 0ce551359d7ccdbc2a019cba29ce1491c8aa4bc48176e9e4cd69b948bb702526	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00320-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV22-00320-PH-01.pdf	

Imagen del mensaje

CSIRT alerta phishing con malware que suplanta a Cemex	
Alerta de seguridad cibernética	2CMV22-00321-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2021
Última revisión	17 de agosto de 2021
Indicadores de compromiso	
Asunto	
RE: RE: Pago del saldo	
Correo de Salida	
@cemexdominicana.com	
SHA256	
Nombre: Pago del saldo.zip SHA256: 1c9136738bbf4fc6d0065925255846c00bc0b6192c892b19cd8b38b226576ca9 Nombre: Pago del saldo.exe SHA256: d149d8bb179e47985f4615040059a21605141f84436cce4fe6795de5902c6112	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00321-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV22-00321-PH-01.pdf	

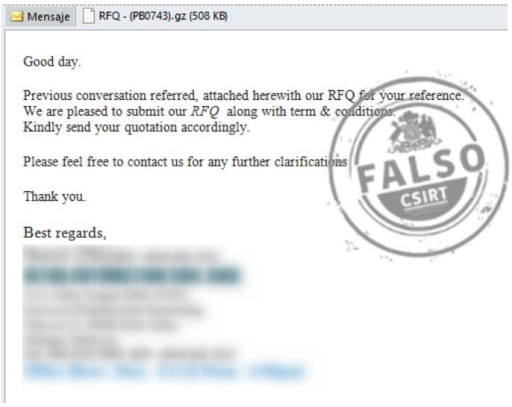
Imagen del mensaje



CSIRT alerta campaña de phishing con malware que suplanta a Kaktüs Çiçekçilik	
Alerta de seguridad cibernética	2CMV22-00322-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2021
Última revisión	17 de agosto de 2021
Indicadores de compromiso	
Asunto	
RFQ – (PB0743)	
Correo de Salida	
@kaktuscicekcilik.com	
SHA256	
Nombre: Pago del saldo.zip SHA256: 1c9136738bbf4fc6d0065925255846c00bc0b6192c892b19cd8b38b226576ca9	

Nombre: Pago del saldo.exe SHA256: d149d8bb179e47985f4615040059a21605141f84436cce4fe6795de5902c6112
Command and Control
http://66.29.145[.]162/?112233 http://kbfvzoboss[.]bid/alien/fre.php http://alphastand[.]trade/alien/fre.php http://alphastand[.]win/alien/fre.php http://alphastand[.]top/alien/fre.php
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00322-01/
https://www.csirt.gob.cl/media/2022/07/2CMV22-00322-PH-01.pdf

Imagen del mensaje



CSIRT advierte phishing con malware con dirección de correo de Indonesia	
Alerta de seguridad cibernética	2CMV22-00323-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2021
Última revisión	17 de agosto de 2021
Indicadores de compromiso	
Asunto	
? FACTURA – Notificacion Giro Folio 012210001 del 15/08/2022 – SII – – (895863965798)	
Correo de Salida	
@server.tapinkab.go.id	
SHA256	
Nombre: 00F722I0513E5S6006.zip SHA256: d64ad4f5d6562d586393ca4846a9cd74cd122d00b47cedff3155487c053d351b Nombre: 00F722I0513E5S6006.msi SHA256: aab9f684d7629871f11665e4c195e04e77ac15714c2112e86f39c46d7bbbc2c7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00323-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV22-00323-PH-01.pdf	

Imagen del Mensaje

CSIRT informa campaña de phishing con malware que suplanta a Intelideck	
Alerta de seguridad cibernética	2CMV22-00324-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2021
Última revisión	17 de agosto de 2021
Indicadores de compromiso	
Asunto	
Estado de Saldos Vencidos de Junio 2022 y Julio 2022 (SOA)	
Correo de Salida	
@intelideck.com	
SHA256	
Nombre: 008_facturas y datos bancarios.xlsx SHA256: 7ef97e0b7a5de9da7c45613fbee89aefd46c2217ec16f965a5d843715a45be7d	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00324-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV22-00324-PH-01.pdf	

Imagen del Mensaje

CSIRT alerta de campaña de phishing con malware Agent Tesla	
Alerta de seguridad cibernética	2CMV22-00325-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de agosto de 2021
Última revisión	18 de agosto de 2021
Indicadores de compromiso	
Asunto	
Standard Quote Request Acknowledgement.	
Correo de Salida	
@helioserralharia.com	
SHA256	
Nombre: Quotation.zip SHA256: 7ef97e0b7a5de9da7c45613fbee89aefd46c2217ec16f965a5d843715a45be7d Nombre: 1XF06zRaiW1O4z5.exe SHA256: 9e3b838c5f8a0e399b16d7120d2f23b0ddd90439f60e79d0657fb8da32d3340c	

Nombre: YiPd.exe SHA256: 9e3b838c5f8a0e399b16d7120d2f23b0ddd90439f60e79d0657fb8da32d3340c
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00325-01/
https://www.csirt.gob.cl/media/2022/07/2CMV22-00325-PH-01.pdf

Imagen del Mensaje

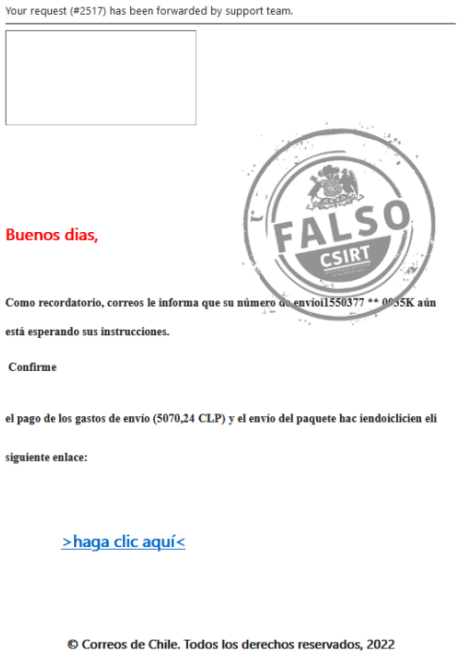
CSIRT alerta de phishing con malware que conecta el equipo a una botnet	
Alerta de seguridad cibernética	2CMV22-00326-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2021
Última revisión	17 de agosto de 2021
Indicadores de compromiso	
Asunto	
Product Inquiry	
Correo de Salida	
@soyuz-sa.com.ar	
SHA256	
Nombre: 10000102122.pdf.rar SHA256: b53c44252fda5b2043f90987b3f3098bf8a9e11c436c9cb90cc74de7def4c6a0 Nombre: 10000102122.pdf.exe SHA256: 5c0ca937fc859373ad8f8fe4741fdf6fde4afba1980de7b62130c387a9dd3107 Nombre: Uagr.exe SHA256: 456c364944232346054ed197e3d56d48b50a83baa7997f78dbf8ba3ed7c6f5ef	
Command and Control	
95.111.251.64:1405	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00326-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV22-00326-PH-01.pdf	

Phishing

Imagen del mensaje

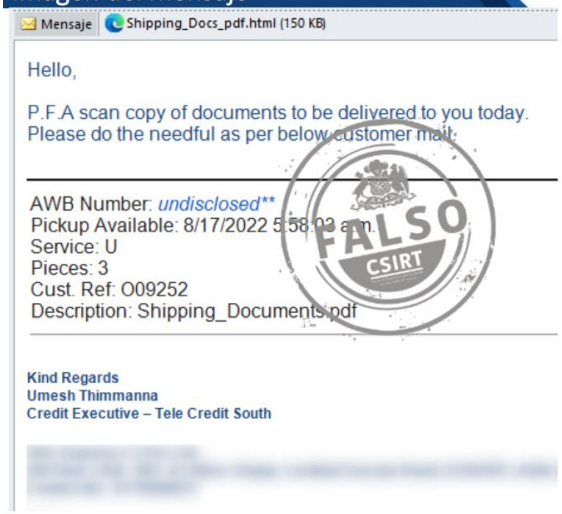
CSIRT alerta de campaña de phishing que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FPH22-00575-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de agosto de 2022
Última revisión	10 de agosto de 2022
Indicadores de compromiso	
URL sitio redirección	
https://s3rvicu4ck.com/activacion/cuenta-lwnr/	
URL sitio falso	
http://simpeg.unhi.ac.id/1660079023/Login	
IP	
[172.104.45.98]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00575-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00575-01.pdf	

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH22-00576-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de agosto de 2022
Última revisión	12 de agosto de 2022
Indicadores de compromiso	
URL sitio redirección	
https://cutt[.]ly/DXrrCb8	
URL sitio falso	
https://milton-exhibits[.]com/chilipost/content/	
IP	
[61.244.88.136]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00576-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00576-01.pdf	

Imagen del mensaje



CSIRT alerta campaña de phishing que suplanta a OneDrive de Microsoft	
Alerta de seguridad cibernética	8FPH22-00577-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2022
Última revisión	17 de agosto de 2022
Indicadores de compromiso	
URL sitio redirección	
file://C:/Users/%USUARIO%/Downloads/Shipping_Docs_pdf.html	
URL sitio falso	
https://imbibetechnologies[.]co.in/realestcvxsff/1d_.php	
IP	
[192.185.107.168]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00577-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00577-01.pdf	

Imagen del mensaje

CSIRT alerta de phishing que busca robar datos personales	
Alerta de seguridad cibernética	8FPH22-00578-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2022
Última revisión	17 de agosto de 2022
Indicadores de compromiso	
URL sitio redirección	
File://C:\Users\IEUser\Desktop\scandoc23675.PDF.xml	
URL sitio falso	
http://f0708738.xsph.ru/dxln.php	
IP	
[141.8.193.236]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00578-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00578-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades en Zimbra	
Alerta de seguridad cibernética	9VSA22-00690-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de agosto de 2022
Última revisión	12 de agosto de 2022
CVE	
CVE-2022-2068 CVE-2022-37044 CVE-2022-37042 CVE-2022-37041	CVE-2022-24407 CVE-2022-37043 CVE-2022-27924 CVE-2022-27925
Fabricantes	
Zimbra	
Productos afectados	
Zimbra Collaboration Suite, versiones anteriores a Zimbra 8.8.15 patch 33 o Zimbra 9.0.0 patch 26.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00690-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00690-01.pdf	

CSIRT alerta de vulnerabilidades en Android	
Alerta de seguridad cibernética	9VSA22-00691-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de agosto de 2022
Última revisión	18 de agosto de 2022
CVE	
CVE-2022-32894 CVE-2022-32893	
Fabricantes	
Apple	
Productos afectados	
Macs que usen macOS Monterey iPhone 6s y posteriores iPad Pro (todos los modelos), iPad Air 2 y posteriores, iPad quinta generación y posteriores, iPad mini 4 y posteriores y los iPod touch de séptima generación.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00691-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00691-01.pdf	

CSIRT alerta de vulnerabilidades en Google Chrome	
Alerta de seguridad cibernética	9VSA22-00692-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de agosto de 2022
Última revisión	18 de agosto de 2022
CVE	
CVE-2022-2856 CVE-2022-2852 CVE-2022-2854 CVE-2022-2855 CVE-2022-2857 CVE-2022-2858	CVE-2022-2853 CVE-2022-2856 CVE-2022-2859 CVE-2022-2860 CVE-2022-2861
Fabricantes	
Google	
Productos afectados	
Google Chrome anteriores a 104.0.5112.101.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00692-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00692-01.pdf	

Actualidad

Exitoso comienzo del Diplomado en Seguridad de la Información y Ciberseguridad realizado por Capacitación Usach en colaboración con el CSIRT de Gobierno

Este martes 16 de agosto inició el primer diplomado en Seguridad de la Información y Ciberseguridad para el sector público, iniciativa conjunta del programa de Capacitación de la Usach y el CSIRT de Gobierno. La instancia es gratuita para encargados de ciberseguridad y de seguridad de la información del aparato estatal y cuenta con casi 350 inscritos.

Esta nota también en:
https://www.csirt.gob.cl/noticias/diplomadousach2022/

Como parte de la jornada inaugural de este nuevo Diplomado, la Jefa de la División Redes y Seguridad Informática del Ministerio del Interior y Seguridad Pública, Ingrid Inda Camino, junto con el Encargado del CSIRT de Gobierno, Carlos Silva Caffi, y Carlos Lobos, Director de los Programas de Ciberseguridad de Capacitación de la Universidad de Santiago de Chile (Usach), dieron una bienvenida a los nuevos estudiantes y explicaron de que se trata esta iniciativa conjunta entre ambas instituciones.

Ingrid Inda, agradeció a la Usach por este aporte al desarrollo de las capacidades de ciberseguridad en nuestro país y destacó que "como Gobierno, queremos que los chilenos vivan tranquilos y seguros, y por eso tenemos como meta lograr más avances en materia de ciberseguridad en sus distintas aristas", razón por la cual nace esta iniciativa, que "permitirá avanzar en concientización, formación, educación e incentivos para el desarrollo de capacidades en ciberseguridad".

Por su parte, Silva recalcó que "la colaboración en ciberseguridad es fundamental. Por eso, para el CSIRT de Gobierno es tan importante el encargado de ciberseguridad, el subrogante y el equipo de ciberseguridad, ya que todos podemos lograr que los datos y la seguridad de los chilenos estén protegidos". El objetivo del diplomado es desarrollar competencias en los estándares de ciberseguridad aplicables en el sector público, diseñar e implementar de un sistema de gestión de seguridad de la información bajo el estándar ISO 27001, diseñar e implementar controles de seguridad de la información alineados con el estándar ISO 27002 e implementar de un Centro de Monitoreo de Ciberseguridad (SOC) usando herramientas open source.

Ciberguía familiar | Hábitos para navegar Internet

Llevar una vida digital segura y sana es tarea de todos, y los padres y cuidadores tienen un rol fundamental. Desde el momento en que los niños, niñas y adolescentes tienen acceso a un teléfono inteligente o juegan conectados, deben estar informados y conscientes de que en el mundo online, así como en la vida física.

Para apoyar esta importante misión que tienen los padres y cuidadores en el mundo actual, el CSIRT de Gobierno elaboró esta guía familiar para que tanto adultos como adolescentes, niños y niñas puedan navegar de forma segura y sana: https://www.csirt.gob.cl/recomendaciones/ciberguia-familiar-habitos-para-navegar-internet/

Ciberdiccionario Volumen 14

Continuamos en el Mes del Niño y Niña y por eso la edición del ciberdiccionario de esta semana explica algunos términos que utilizan los jóvenes para comunicarse en redes sociales, como challenge, followers, stalker y streamer.

También puedes descargar esta nueva edición del ciberdiccionario aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-14/

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 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 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.

- Francisco Villablanca Paredes
- Marco Antonio Escobar E.
- Felipe Andrés Patricio Herrera Carrasco
- Adrián Muñoz
- Jerson Andrés Valenzuela Campusano
- Cristián Eing Latorre
- Felipe Saraleguir