Ministerio del Interior y Seguridad Pública

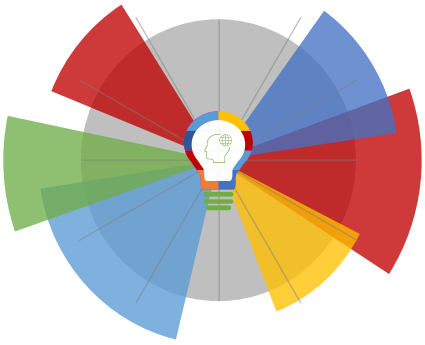
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

08-04-2022 | Año 4 | N°144

Boletín de Seguridad Cibernética

Semana del 1 al 7 de abril de 2022

La semana en cifras



Se advirtieron

10

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

70

para vulnerabilidades

Las mitigaciones son útiles en productos Apple, Android de Google, VMware, Palo Alto, Cisco y Spring.

IP

12

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

Sitios fraudulentos

Imagen del sitio

CSIRT informa sitio falso de One Drive	
Alerta de seguridad cibernética	8FFR22-01073-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de abril de 2022
Última revisión	7 de abril de 2022

Indicadores de compromiso
URL sitio falso
http://bigvantour[.]cl/wp-content/plugins/louowgvaem/blessing/onedriveoriginal11/index.php
IP
[190.153.219.252]
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/8ffr22-01073-01/
https://www.csirt.gob.cl/media/2022/04/8FFR22-01073-01.pdf

Phishing

Imagen del mensaje

CSIRT advierte phishing con falsos puntos del Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00503-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de abril de 2022
Última revisión	1 de abril de 2022
Indicadores de compromiso	
URL redirección	
http://ec2-34-238-41-18.compute-1.amazonaws[.]com/D0190238787912-3/?hash=bnVsbEBudWxsLmNs	
URL sitio falso	
https://itautarjeta[.]online/726a292db52f7f5/html/index.php	
IP	
[130.185.123.87]	
[130.185.123.46]	
[130.185.123.240]	
[185.235.41.84]	
[130.185.123.186]	
[130.185.123.125]	
[3.86.149.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00503-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00503-01.pdf	

Imagen del mensaje	CSIRT advierte phishing vía WhatsApp que suplanta a COPEC	
 http://empressauxiliary.top/copeccl/tb.php?hmdgcfqw1648996068508	Alerta de seguridad cibernética	8FPH22-00504-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	4 de abril de 2022
	Última revisión	4 de abril de 2022
	Indicadores de compromiso	
	URL sitio redirección	
	http://empressauxiliary[.]top/copeccl/tb.php?hmdgcfqw1648996068508	
	URL sitio falso	
	https://scrubdesk[.]top/Zk8tEV4f/copeccl/?_t=1649077409776#1649077411598	
	IP	
	[172.67.163.165]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00504-01/	
	https://www.csirt.gob.cl/media/2022/04/8FPH22-00504-01.pdf	

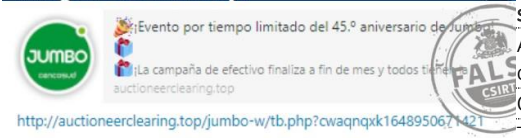
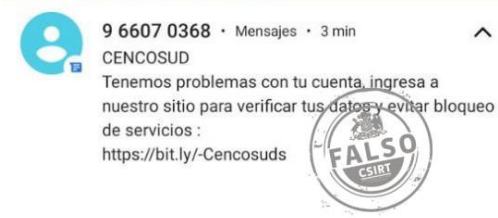
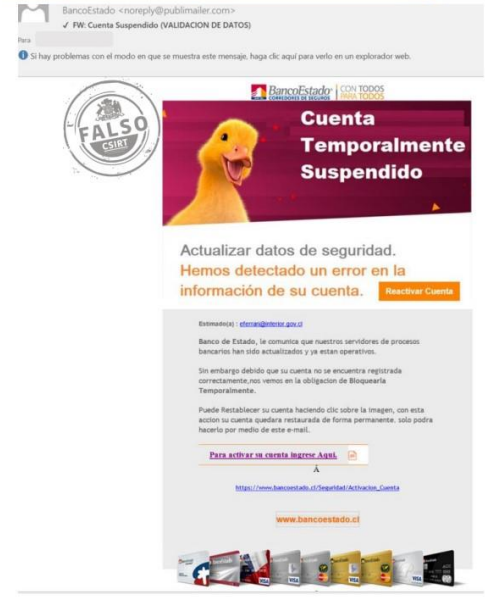
Imagen del mensaje	CSIRT informa phishing con falso concurso de aniversario del supermercado Jumbo	
 http://auctioneerclearing.top/jumbo-w/tb.php?cwaqnqxk1648950671421	Alerta de seguridad cibernética	8FPH22-00505-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	4 de abril de 2022
	Última revisión	4 de abril de 2022
	Indicadores de compromiso	
	URL sitio redirección	
	http://auctioneerclearing[.]top/jumbo-w/tb.php?cwaqnqxk1648950671421	
	URL sitio falso	
	https://75tqqbv[.]cn/Uvp64Fio/jumbo-w/?_t=1649080166301#1649080168531	
	IP	
	[104.21.18.208]	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00505-01/	
	https://www.csirt.gob.cl/media/2022/04/8FPH22-00505-01.pdf	

Imagen del mensaje



CSIRT advierte phishing que suplanta a Cencosud	
Alerta de seguridad cibernética	8FPH22-00506-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de abril de 2022
Última revisión	7 de abril de 2022
Indicadores de compromiso	
URL sitio falso	
https://bit.ly/-Cencosuds	
IP	
[172.67.186.46]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00506-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00506-01.pdf	

Imagen del mensaje



CSIRT alerta phishing con falsa cuenta suspendida del Banco Estado	
Alerta de seguridad cibernética	8FPH22-00507-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de abril de 2022
Última revisión	7 de abril de 2022
Indicadores de compromiso	
URL redirección	
http://smartlineprofiles[.]am/activacion/cuenta-nuge/	
URL sitio falso	
http://uthh.edu[.]mx/content/public/Support/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[45.236.130.175]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00507-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00507-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidad en Spring Framework	
Alerta de seguridad cibernética	9VSA22-00605-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de abril de 2022
Última revisión	4 de abril de 2022
CVE	
CVE-2022-22965	
Fabricante	
Spring	
Productos afectados	
Pivotal Spring Framework: versiones 5.0.0 – 6.0.0-M3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00605-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00605-01.pdf	

CSIRT comparte vulnerabilidades en Apple	
Alerta de seguridad cibernética	9VSA22-00606-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Bajo
TLP	Blanco
Fecha de lanzamiento original	4 de abril de 2022
Última revisión	4 de abril de 2022
CVE	
CVE-2022-22674 CVE-2022-22675	
Fabricante	
Apple	
Productos afectados	
CVE-2022-22674: macOS Monterey 12.3.1 CVE-2022-22675: iOS 15.4.1 iPadOS 15.4.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00606-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00606-01.pdf	

CSIRT comparte vulnerabilidad crítica de Trend Micro	
Alerta de seguridad cibernética	9VSA22-00607-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de abril de 2022
Última revisión	4 de abril de 2022
CVE	
CVE-2022-26871	
Fabricante	
Trend Micro	
Productos afectados	
Trend Micro Apex Central 2019 Hotfix b5874 a 2019 R3 b3752, tanto on premise como SaaS.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00607-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00607-01.pdf	

CSIRT alerta de nuevas vulnerabilidades críticas en productos VMware	
Alerta de seguridad cibernética	9VSA22-00608-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2022
Última revisión	5 de abril de 2022
CVE	
CVE-2022-22965 - CVE-2022-22948 - CVE-2022-22943 CVE-2022-22951 - CVE-2022-22952 - CVE-2022-22943 CVE-2022-22944 - CVE-2022-22945	
Fabricante	
VMware	
Productos afectados	
CVE-2022-22965 Tanzu Application Service: https://network.pivotal.io/products/elastic-runtime/ Tanzu Operations Manager: https://network.tanzu.vmware.com/products/ops-manager VMware TKGI: https://network.pivotal.io/products/pivotal-container-service/ CVE-2022-22948 VMware vCenter Server (vCenter Server) VMware Cloud Foundation (Cloud Foundation) CVE-2022-22951 y CVE-2022-22952 VMware Carbon Black App Control (AppC)	

CVE-2022-22943 VMware Tools for Windows CVE-2022-22944 VMware Workspace ONE Boxer CVE-2022-22945 VMware NSX Data Center for vSphere. VMware Cloud Foundation (Cloud Foundation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00608-01/
https://www.csirt.gob.cl/media/2022/04/9VSA22-00608-01.pdf

CSIRT comparte información de Cisco sobre vulnerabilidad Spring4Shell	
Alerta de seguridad cibernética	9VSA22-00609-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2022
Última revisión	5 de abril de 2022
CVE	
CVE-2022-22965	
Fabricante	
Cisco	
Productos afectados	
Productos confirmados por Cisco como afectados hasta el momento de la redacción de este documento: Cisco Crosswork Optimization Engine Cisco Crosswork Zero Touch Provisioning (ZTP) Cisco Edge Intelligence Productos en investigación por Cisco (la empresa irá actualizando a continuación a medida que confirma o descarta que los siguientes productos estén afectados por Spring4Shell): Cisco Application-Oriented Networking Healthcare Services Extensions Cisco Continuous Deployment and Automation Framework Cisco Ultra Cloud Core – Network Respository Function Cisco Ultra Cloud Core – User Plane Function Cisco CX Cloud Agent Software Cisco Extensible Network Controller (XNC) Cisco Network Insights for Data Center Cisco Nexus Dashboard Data Broker, formerly Cisco Nexus Data Broker Cisco Nexus Insights Cisco Wide Area Application Services (WAAS) Cisco Adaptive Security Appliance (ASA) Cisco Firepower Management Center (FMC)	

Cisco Firepower System Software
Cisco Security Manager
Cisco Automated Subsea Tuning
Cisco CloudCenter Action Orchestrator
Cisco CloudCenter Workload Manager
Cisco Collaboration Audit and Assessments
Cisco Common Services Platform Collector (CSPC)
Cisco Connected Mobile Experiences
Cisco Connected Pharma
Cisco Crosswork Change Automation
Cisco Crosswork Data Gateway
Cisco Crosswork Network Automation
Cisco Crosswork Network Controller
Cisco Crosswork Situation Manager
Cisco DNA Assurance
Cisco Data Center Network Manager (DCNM)
Cisco Evolved Programmable Network Manager
Cisco Intelligent Node (iNode) Manager
Cisco IoT Field Network Director
Cisco Network Change and Configuration Management
Cisco Nexus Dashboard, formerly Cisco Application Services Engine
Cisco Optical Network Planner
Cisco Shelf Virtualization Orchestrator (SVO)
Cisco Smart PHY
Cisco Smart Software Manager
Cisco Virtual Topology System – Virtual Topology Controller (VTC) VM
Cisco WAN Automation Engine (WAE)
Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)
Cisco DNA Center
Cisco IOx Fog Director
Cisco Mobility Unified Reporting and Analytics System
Cisco Network Assurance Engine
Cisco Network Convergence System 2000 Series
Cisco ONS 15454 Series Multiservice Provisioning Platforms
Cisco Optical Network Controller
Cisco SD-WAN Cloud OnRamp for Co-Location
Cisco SD-WAN vManage
Cisco Ultra Cloud Core – Access and Mobility Management Function
Cisco Ultra Cloud Core – Policy Control FunctionCisco Ultra Cloud Core – Session Management Function
Cisco Ultra Services Platform
Cisco Business Dashboard
Cisco HyperFlex HX Data Platform
Cisco BroadCloud for Carriers
Cisco BroadWorks
Cisco Cloud Connect
Cisco Emergency Responder
Cisco Enterprise Chat and Email

Cisco Unified Customer Voice Portal Cisco Unified Intelligence Center Cisco Unity Connection Cisco Virtualized Voice Browser Cisco Webex Board, formerly Cisco Spark Board Cisco Meeting Server Cisco Video Surveillance Operations Manager Cisco Vision Dynamic Signage Director Cisco Cloud Hosted Services Cisco BroadCloud Cisco Cloud Application Policy Infrastructure Controller (Cloud APIC) Cisco Cloud Email Security Cisco Cognitive Intelligence Cisco DNA Center Cloud Cisco Intersight Cisco IoT Control Center Cisco Managed Services Accelerator (MSX) Cisco Registered Envelope Service Cisco Smart Collector – Lifecycle Management Cisco Umbrella Cisco Webex Centers – Meeting Center, Training Center, Event Center, Support Center Cisco Webex Events Cisco Webex Meeting Server – Multimedia Platform Cisco Webex Meetings
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00609-01/
https://www.csirt.gob.cl/media/2022/04/9VSA22-00609-01.pdf

CSIRT advierte de vulnerabilidad crítica en GitHub	
Alerta de seguridad cibernética	9VSA22-00610-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de abril de 2022
Última revisión	4 de abril de 2022
CVE	
CVE-2022-1162	
Fabricante	
GitHub	
Productos afectados	
GitLab Community Edition y Enterprise Edition, versiones anteriores a 14.7.7, 14.8.5 y 14.9.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00607-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00607-01.pdf	

CSIRT advierte de nuevas vulnerabilidades en Android	
Alerta de seguridad cibernética	9VSA22-00610-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de abril de 2022
Última revisión	4 de abril de 2022
CVE	
CVE-2021-0694 - CVE-2021-39794 - CVE-2021-39795 - CVE-2021-39796 CVE-2021-39797 - CVE-2021-39798 - CVE-2021-39799 - CVE-2021-39803 CVE-2021-39804 - CVE-2021-39808 - CVE-2021-39805 - CVE-2021-39809 CVE-2021-39795 - CVE-2021-39803 - CVE-2021-39807 - CVE-2021-0707 CVE-2021-39801 - CVE-2021-39802 - CVE-2021-39800 - CVE-2022-20081 - CVE-2021-25477 - CVE-2021-35081 - CVE-2021-35112 - CVE-2021-35123 CVE-2021-30334 - CVE-2021-35091 - CVE-2021-35095 - CVE-2021-35130 - CVE-2021-30339 - CVE-2021-30341 - CVE-2021-30342 - CVE-2021-30343 CVE-2021-30347 - CVE-2021-35104 - CVE-2021-30281 - CVE-2021-30338 CVE-2021-30340 - CVE-2021-30344 - CVE-2021-30345 - CVE-2021-30346 CVE-2021-30349 - CVE-2021-30350 - CVE-2021-35070 - CVE-2021-35100	
Fabricante	
Google	
Productos afectados	
Android, versión 12L y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00611-01/	

https://www.csirt.gob.cl/media/2022/04/9VSA22-00611-01.pdf

CSIRT informa de vulnerabilidad en productos de Palo Alto	
Alerta de seguridad cibernética	9VSA22-00612-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de abril de 2022
Última revisión	7 de abril de 2022
CVE	
CVE-2022-0778	
Fabricante	
Palo Alto	
Productos afectados	
PAN-OS 8.1 y posteriores GlobalProtect, todas las versiones Cortex XDR agent, todas las versiones.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00612-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00612-01.pdf	

CSIRT comparte nuevas vulnerabilidades críticas en productos VMware	
Alerta de seguridad cibernética	9VSA22-00613-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de abril de 2022
Última revisión	7 de abril de 2022
CVE	
CVE-2022-22954 - CVE-2022-22955 - CVE-2022-22956 CVE-2022-22957 - CVE-2022-22958 - CVE-2022-22959 CVE-2022-22960 - CVE-2022-22961	
Fabricante	
VMware	
Productos afectados	
VMware Workspace ONE Access VMware Identity Manager (vIDM) vRealize Lifecycle Manager vRealize Automation VMware Cloud Foundation	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00613-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00613-01.pdf	

Noticias

Listado de vulnerabilidades que requieren parchado urgente según la CISA de EE.UU. (Abril 2022)

La Agencia de Ciberseguridad e Infraestructura (CISA) del Gobierno Federal de los Estados Unidos mantiene y actualiza frecuentemente una lista de las vulnerabilidades más importantes que están siendo explotadas en el ciberespacio de dicho país.

Consideramos que este listado (disponible en cisa.gov/known-exploited-vulnerabilities-catalog) supone un material útil para difundir también en Chile, ya que muchos de los sistemas que se usan en nuestro país son los mismos afectados por las vulnerabilidades destacadas por la CISA

Actualmente, el listado está compuesto de las siguientes 609 vulnerabilidades, que recomendamos parchar cuanto antes, usando las actualizaciones dispuestas por los respectivos proveedores en sus sitios web.

Pueden revisar el listado completo aquí: https://www.csirt.gob.cl/noticias/listado-vulnerabilidades-cisa/

Información sobre proveedores afectados por "Spring4Shell"

A fines de marzo se dio conocer la existencia de una vulnerabilidad crítica que afecta a Spring, un framework de Java ampliamente utilizado (algunas estimaciones señalan que es la más popular del mundo). La vulnerabilidad, apodada "Spring4Shell" fue identificada como CVE-2022-22965 y publicada en su momento por el CSIRT de Gobierno. Sus detalles pueden verse aquí:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00605-01/

Varias empresas que usan Spring para desarrollar algunos de sus productos han identificado aquellos que estarían afectados por la vulnerabilidad, y entregado parches para corregirla. Algunos de las principales son VMware, Cisco, Red Hat, SolarWinds y SAP, cuyos detalles y enlaces respectivos se detallan en el presente documento.

Es muy importante que las organizaciones identifiquen si sus sistemas cuentan con programas vulnerables a esta amenaza, la que se teme que pueda ser ampliamente por ciberdelincuentes. Tanto es así que ya la empresa de ciberseguridad Check Point asegura que alrededor de un sexto de las empresas con software vulnerable ya han sido atacadas[1].

Proveedor: VMware

Productos afectados
VMware Tanzu Application Service for VMs
VMware Tanzu Operations Manager
VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)

Proveedor: Cisco

Productos confirmados por Cisco como afectados hasta el momento de la redacción de este documento:
Cisco Crosswork Optimization Engine
Cisco Crosswork Zero Touch Provisioning (ZTP)
Cisco Edge Intelligence

Proveedor: Red Hat

Productos afectados:
Red Hat Descision Manager 7
Red Hat JBoss A-MQ 6

Red Hat JBoss Fuse 6

Red Hat JBoss Fuse 7
Red Hat Process Automation 7
Red Hat JBoss A-MQ 7
Red Hat Virtualization 4

Proveedor: SolarWinds

Productos en investigación (no confirmados ni descartados como afectados):
Security Event Manager (SEM)
Database Performance Analyzer (DPA)
Web Help Desk (WHD)

Proveedor: SAP

Productos afectados:
SAP NetWeaver Application Server for Java todas las versiones.

Puedes encontrar más información aquí: https://www.csirt.gob.cl/noticias/proveedores-spring4shell/

Actualidad

Ciberconsejos para una Operación Renta 2022 más segura

Aprovechando que la Operación Renta se realiza masivamente por internet, los ciberdelincuentes despliegan cada año diversas formas de engañar a las personas para robar su dinero, aumentando además con el tiempo su sofisticación.

Por eso, cada abril publicamos un recordatorio de las principales recomendaciones para estar atentos, fijarnos bien en los emails o mensajes de texto que podemos recibir, y detectar aquellos que son estafas o programas maliciosos. ¡Revisa estos consejos y compártelos con tus amigos y familiares!

Encuentra los ciberconsejos aquí: csirt.gob.cl/recomendaciones/operacion-renta-2022/

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 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.

- Maurizio Mattoli
- Luis Valdebenito Cereceda
- Gonzalo Araya Rivero
- David Soto
- Eder Patricio Morán Heredias
- Carlos Humberto de la Fuente Castro
- Carlos Montoya
- Óscar Felipe Cuadra Navarro
- Eduardo Retamales Morales
- Bárbara Palacios Cabezas
- Maickol Alexander Reyes Vidal
- Mario Contreras Mora
- Luciano Miguel Tobaria
- Christian Abarca
- Marcelo Eduardo Azola Martínez
- Ricardo González
- Cristián Acuña
- Juan Alfonso Muñoz Castañeda
- Reynaldo Augusto Araya Villalón
- Fabián Soto
- Hanz Sandoval