CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 207

semana del 16 al 22 de junio de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

14

IP advertidas en múltiples campañas de phishing y de malware.

URL ADVERTIDAS

23

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

8

Las mitigaciones son útiles en productos de VMware y Progress (MOVEit).

HASH REPORTADOS

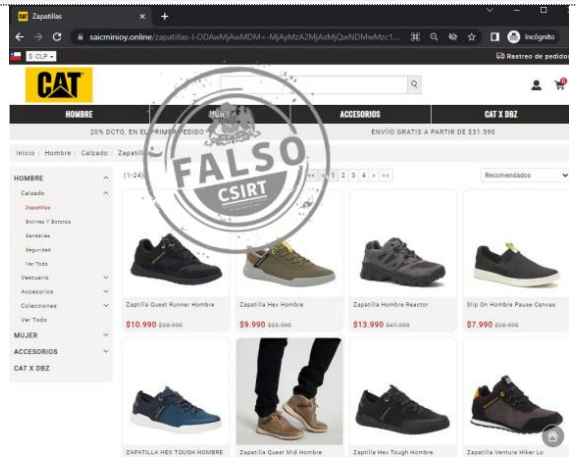
9

Hashes asociados a múltiples campañas de phishing con archivos que contienen malware

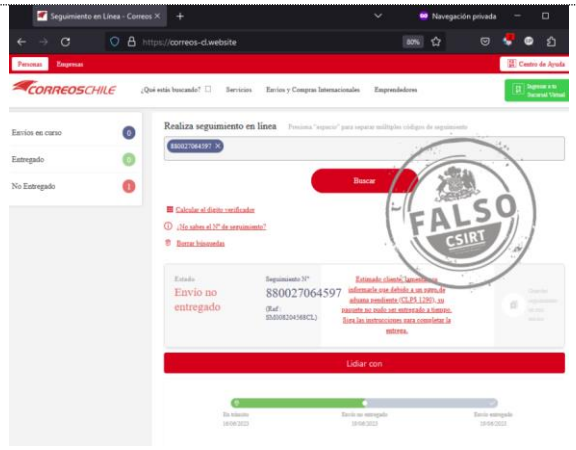
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

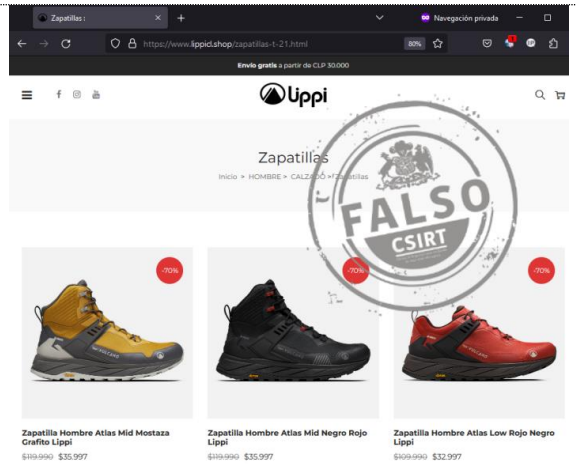
1. Sitios fraudulentos



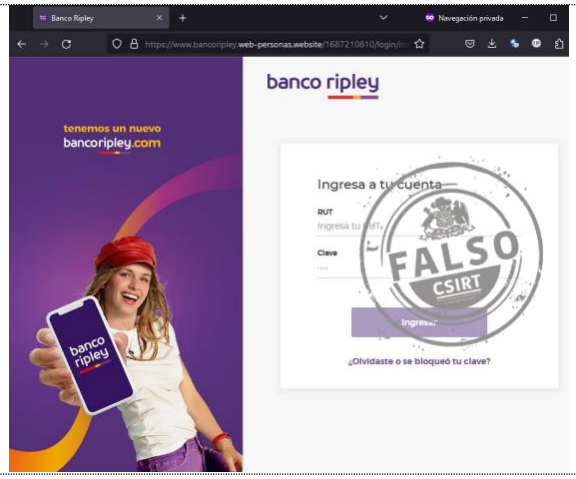
CSIRT alerta de nueva página fraudulenta que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01409-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de junio de 2023
Última revisión	19 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.saicminioy[.]online/	
Dirección IP	
[199.21.150.21]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01409-01	



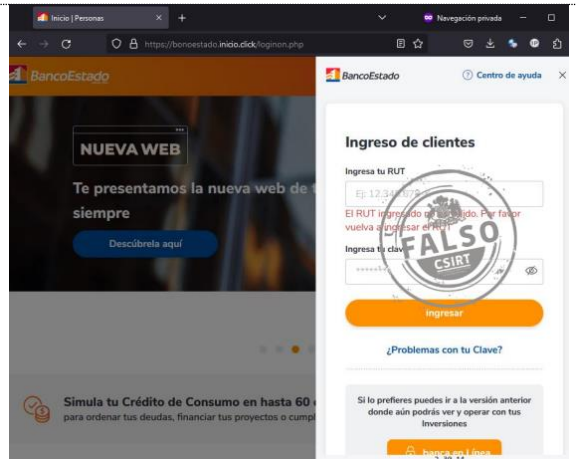
CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01410-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de junio de 2023
Última revisión	19 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://correos-cl[.]website/	
Dirección IP	
[38.60.196.88]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01410-01	



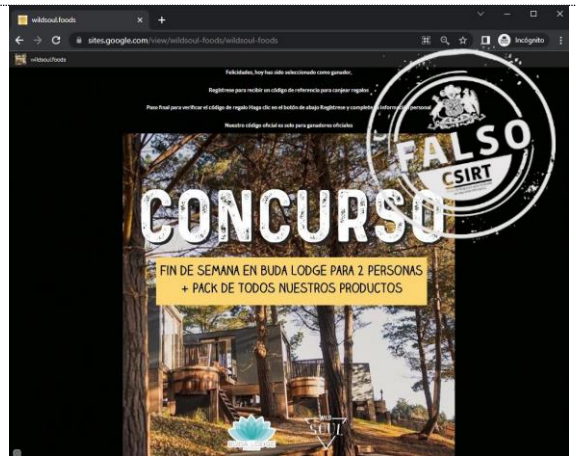
CSIRT alerta de nueva página fraudulenta que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01411-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de junio de 2023
Última revisión	19 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.lippicl[.]shop	
Dirección IP	
[172.67.179.240]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01411-01	



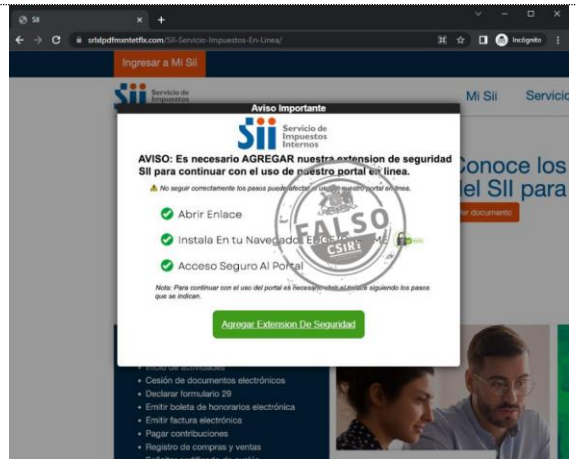
CSIRT alerta ante nueva página fraudulenta que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01412-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de junio de 2023
Última revisión	19 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.bancoripley.web-personas[.]website/1687210810/login/index.html	
Dirección IP	
[192.64.117.217]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01412-01	



CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01413-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2023
Última revisión	20 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://bonoestado.inicio[.]click/loginon.php	
Dirección IP	
[104.21.78.226]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01413-01	

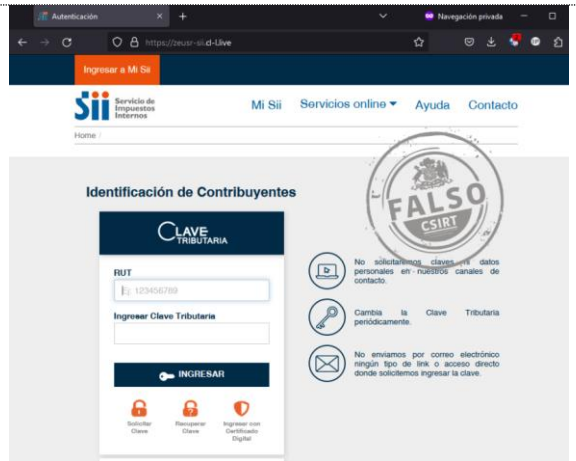


CSIRT alerta ante nuevo sitio fraudulento que suplanta a Wild Foods	
Alerta de seguridad cibernética	8FFR23-01414-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2023
Última revisión	20 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://sites.google[.]com/view/wildsoul-foods/wildsoul-foods	
Dirección IP	
[74.125.126.139]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01414-01	

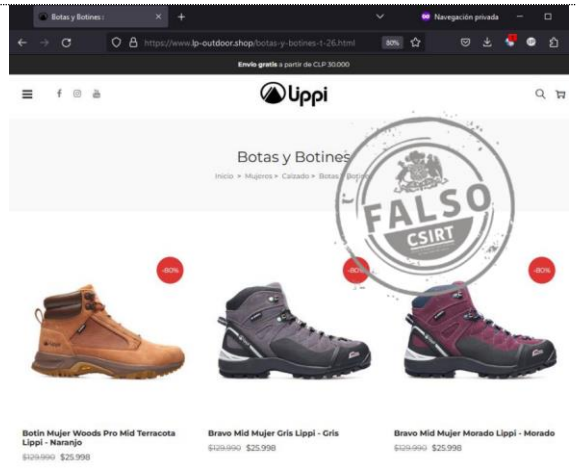


CSIRT alerta de nueva página fraudulenta que suplanta al Servicio de Impuestos Internos	
Alerta de seguridad cibernética	8FFR23-01415-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2023
Última revisión	22 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://srlxlpdfmxntetflx[.]com/SII-Servicio-Impuestos-En-Linea/	
Dirección IP	
[172.67.214.30]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01415-01	

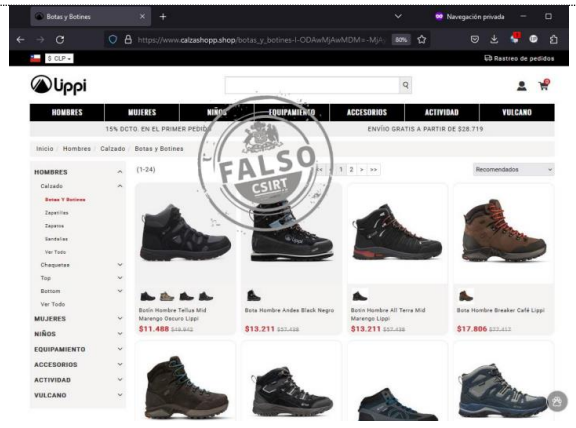
CSIRT alerta de nuevo sitio fraudulento que suplanta al SII	
Alerta de seguridad cibernética	8FFR23-01416-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2023
Última revisión	22 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
http://170.39.230[.]80/inicio.html	
Dirección IP	
[170.39.230.80]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01416-01	



CSIRT alerta ante nuevo sitio falso que suplanta al Servicio de Impuestos Internos	
Alerta de seguridad cibernética	8FFR23-01417-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2023
Última revisión	22 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://zeusr-sii.cl-l[.]live/	
Dirección IP	
[172.67.223.228]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01417-01	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01418-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2023
Última revisión	22 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.lp-outdoor[.]shop/	
Dirección IP	
[104.21.2.127]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01418-01	



CSIRT alerta de nueva página fraudulenta que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01419-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2023
Última revisión	22 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.calzashopp[.]shop/	
Dirección IP	
[199.21.150.9]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01419-01	

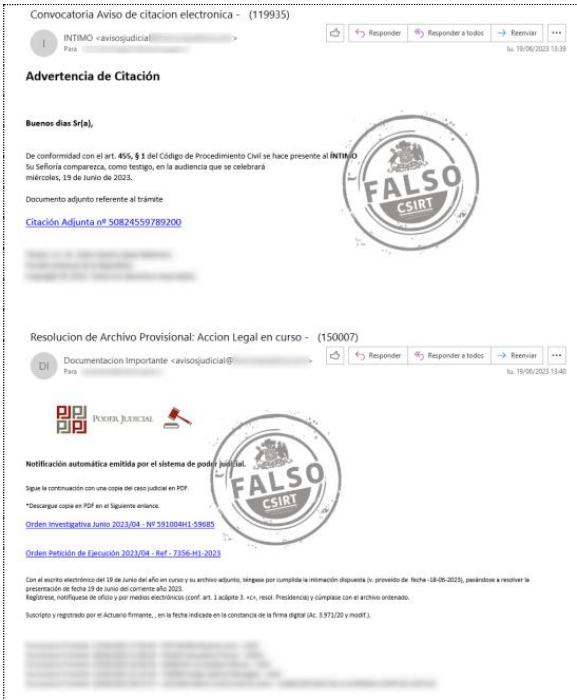
2. Phishing

CSIRT alerta de una nueva página fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00836-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2023
Última revisión	20 de junio de 2023
URL redirección	
https://trylocall[.]com/wp-content/activacion/cuenta-kyhu/	
URL sitio falso	
https://homefogastadp[.]info/1686775823/imagenes/_personas/home/default.asp	
Dirección IP	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8FPH23-00836-01/	

CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00837-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2023
Última revisión	20 de junio de 2023
Indicadores de compromiso	
URL redirección	
https://reachercontact[.]com/activacion/cuenta-zksc/	
URL sitio falso	
https://comunistable[.]com/1687268783/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[98.142.101.90]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8FPH23-00837-01/	

CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00838-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2023
Última revisión	22 de junio de 2023
Indicadores de compromiso	
URL redirección	
https://www.hopgia[.]vn/upload/news/activacion/cuenta-kzy	
URL sitio falso	
https://homefogastadp[.]info/1687449138/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8FPH23-00838-01/	

3. Malware



CSIRT alerta de nueva campaña de phishing con malware, que suplanta al Poder Judicial	
Alerta de seguridad cibernética	2CMV23-00419-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2023
Última revisión	20 de junio de 2023
Indicadores de compromiso	
URL-Dominio	
https://jccrivelliabogadospublicidad.brazilsouth.cloudapp[.]azure.com/ http://20.206.121[.]188/ https://www.dropbox[.]com/s/dl/wdw1uk4rc4iihly/ https://www.dropbox[.]com/s/dl/0thjroopb2nae4x/ https://www.dropbox[.]com/s/dl/zl93ykl0jlz7dcr/ http://ip-api[.]com/json	
SHA256	
58cfa0e09bc0acc1bc993045633ea70e3cd3797ff55d86045168fee3db2562e1 49123043ba4257cb61d00a931ea273f724a9cda06ec8eb107ddeab4d664ac88306 04388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15 865f12dd2959457978155d2eb83833ea00d0afc06f3aa820866f6a55476ad3e4 84d73fd51c09a001c449100862d48062eee947bc2d632264f820cdf3393789ef 0604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15 816266195405aa5c6d9564f0db7fc58dca1c064558f7c96c47f7cbfc3bf68d7d 5ccb8f4becf4f5c5440d62ebb9c21abf84d5c564eb72ec9d12f27fc824307998 0604388f107d1ed9abbb13912e5cdc2f9a2da8d0e528fbb4546c23b2f08c6f15	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00418-01/	

4. Vulnerabilidades

CSIRT comparte información de vulnerabilidades críticas en MOVEit, al menos una ya se encuentra siendo explotada	
Alerta de seguridad cibernética	9VSA23-00850-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de junio de 2023
Última revisión	16 de junio de 2023
CVE	
CVE-2023-34362 CVE-2023-35036	
Fabricantes	
Progress	
Productos afectados	
MOVEit Transfer 2023.0.0 MOVEit Transfer 2022.1.x MOVEit Transfer 2022.0.x MOVEit Transfer 2021.1.x MOVEit Transfer 2021.0.x	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00850-01/	

CSIRT comparte información de nueva vulnerabilidad en MOVEit Transfer	
Alerta de seguridad cibernética	9VSA23-00851-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de junio de 2023
Última revisión	20 de junio de 2023
CVE	
CVE-2023-35708	
Fabricante	
MOVEit Transfer 2023.0.x (15.0.x) MOVEit Transfer 2022.1.x (14.1.x) MOVEit Transfer 2022.0.x (14.0.x) MOVEit Transfer 2021.1.x (13.1.x) MOVEit Transfer 2021.0.x (13.0.x) MOVEit Transfer 2020.1.x (12.1) MOVEit Transfer 2020.0.x (12.0) o anterior MOVEit Cloud	
Productos afectados	
Progress	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00851-01/	

CSIRT comparte información de nuevas vulnerabilidades en vCenter Server de VMware	
Alerta de seguridad cibernética	9VSA23-00852-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2023
Última revisión	22 de junio de 2023
CVE	
CVE-2023-20892 CVE-2023-20893 CVE-2023-20894 CVE-2023-20895 CVE-2023-20896	
Fabricantes	
VMware	
Productos afectados	
VCenter Server 7.0, 8.0. Cloud Foundation (vCenter Server) 5.x, 4.x	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00852-01/	

5. Concientización

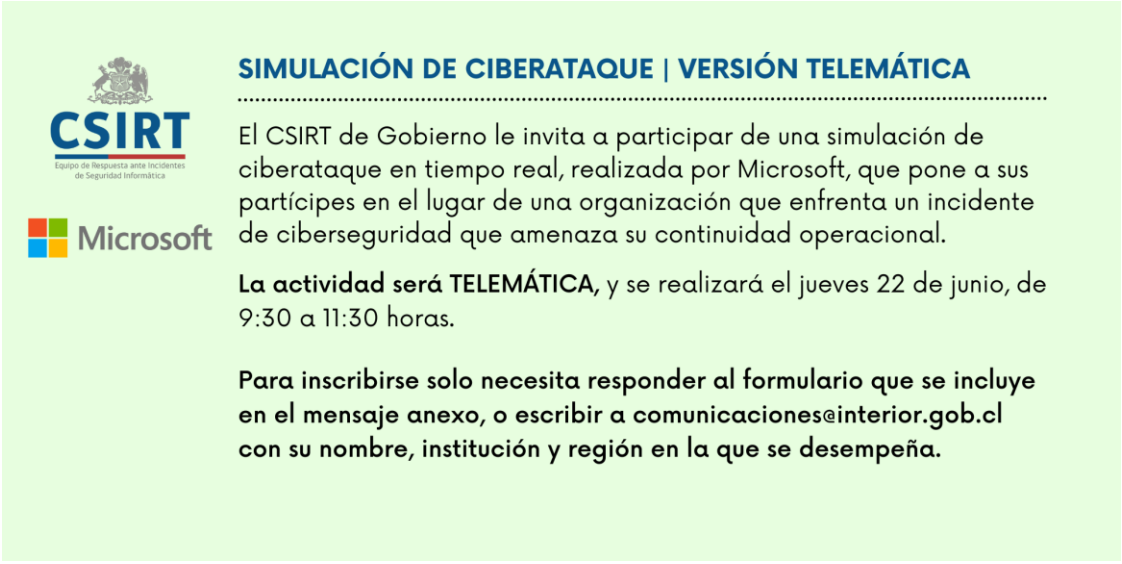
Ciberconsejos para evitar realizar falsas inversiones | CMF y CSIRT

En conjunto con la Comisión para el Mercado Financiero, en el CSIRT preparamos estos consejos para que no caigas en falsas inversiones, estafas que se promocionan con peligrosa facilidad en las redes sociales. Evita estafas y aumenta la seguridad de tus amigos y familiares compartiendo nuestros Ciberconsejos: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-cmf-y-csirt/

Exitosa cuarta versión de la simulación de ciberataque para funcionarios públicos, presentada por el CSIRT y Microsoft.

Más de 130 funcionarios públicos de todas las regiones del país participaron de la primera instancia telemática de las simulaciones de ciberataque que cada mes entrega el CSIRT de la mano de Microsoft, sesiones que comenzaron en marzo.

Como en las presentaciones anteriores, los funcionarios participantes pudieron presenciar un video que simula las distintas situaciones a las que se enfrentan las diferentes funciones dentro de una organización que sufre un ciberataque, y las decisiones que deben ir tomando, enfatizando la importancia que tiene el rol que debe temer la ciberseguridad en una empresa o entidad pública, y la necesidad de crear planes de contingencia y recuperación conocidos a todo nivel de la organización.



Ciberdiccionario Volumen 39

Nuevas definiciones se suman al Ciberdiccionario del CSIRT esta semana, la primera del invierno. Añadimos los significados, en el contexto de la ciberseguridad, de entropía, virus de macros, STEM y CIO. Esperamos que les resulten útiles. Todos los volúmenes del ciberdiccionario, junto al resto de nuestras recomendaciones están contenidas siempre en: http://csirt.gob.cl/recomendaciones.

6. 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 que los sitios web a los que se ingrese sean los oficiales.

7. 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.

- Juan Pablo Berríos
- Luis Miguel Bravo Ramírez
- David Soto
- Enrique Moraga
- Andrés Rodríguez
- Pamela Lillo Fabres
- Andrea de los Ángeles Salas Piraino
- Sergio Sanguinetti
- Manuel Alfredo Carvajal Castillo
- Rodrigo Andrés Silva Maldonado
- Rafael

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.23 15:16:08 -04'00'