



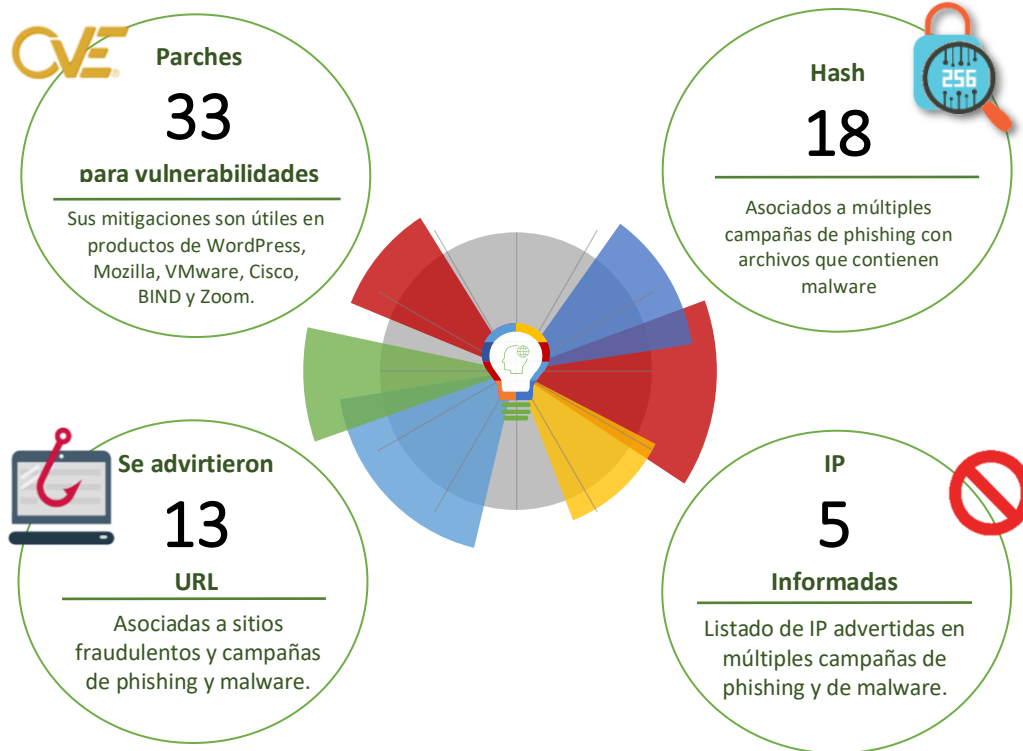
27-05-2022 | Año 4 | N°151

Boletín de Seguridad Cibernética

Semana del 20 al 26 de
mayo de 2022



La semana en cifras



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

Contenido

Malware.....	2
Sitios fraudulentos	4
Phishing	6
Vulnerabilidades	7
Actualidad.....	11
Muro de la Fama	14

Malware

Imagen del Mensaje



CSIRT advierte phishing con malware adjuntando falsa factura

Alerta de seguridad cibernética	2CMV21-00299-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de mayo de 2022
Última revisión	24 de mayo de 2022

Indicadores de compromiso

SHA256

```
30f6ded6df72c217f2022e927d38643ac2f472b149c3317c8f3407e3728b4755
af2f794adc6060e8c10fa32366d8be97bd3e4dd0a958978cb2315d035124f13e
49d34cf73009f109860f8f5a3857f205240ecfcc5b1dbffe04a054090b45575e
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
bb85e4530cc6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f
cb76672f7442b725e4c39db6edb7cc7259469cdd38b3d0f4f90226d981a380a9
845b03ca416bbc07b1193fb2a678f70e19d4b4698a30ac00aba8c635d71eb52
0a6af331a1d312b6b8563a5e4e8eaa83a5b933bd6f73f2b03168eb5e262b83d6
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
```

IoC URL

hXXp://ip-72-167-45-95.ip.secureserver[.]net/.contacto/?hash=
hXXps://facturadisponible.japanwest.cloudapp.azure[.]com/?hash=
hXXps://www.opvn[.]info/modules/mole.ija

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-0299-01/>
<https://www.csirt.gob.cl/media/2022/03/2CMV22-00299-01.pdf>

Imagen del mensaje



CSIRT advierte campaña de phishing con malware suplantando al Ministerio de Transportes

Alerta de seguridad cibernética	2CMV21-00300-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2022
Última revisión	26 de mayo de 2022

Indicadores de compromiso

SHA256

```
078e67fd81467f42d9ce1d65904e9dea2a84cab29975815ec7a03fdc2c740cc1
9830bd16aeddd4387da7bbe79c4e036b60b005df5d2964626c10be2d30257c35f
33d4ef958d813f13d0bc789726d7503200bf280caceb4667d99a144e634dbfd
bb85e4530cc6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
69bea5a467e532fbc06965b0d15f0bfbe5245c9f4f5009a3b4854762cb7454d4
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
5c8c5586ccb204e4c0826e2bfd883985c7c7c83c2bb4295d7bb4a69a1e57b8
c4fa0cda59435c48dd1ea003e9739a12a1c69c934d8ffcf1a522e16110e3d33c
```

IoC URL

famelic[.]com
csie.npu.edu[.]jtw

vanyapaperproducts[.]com
https://csie.npu.edu[.]tw/wp-content/languages/MTT002140001451.zip
https://www.vanyapaperproducts[.]com/common/img/next/R1ewB32bi97tH.duc

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00300-01/>
<https://www.csirt.gob.cl/media/2022/03/2CMV22-00300-01.pdf>

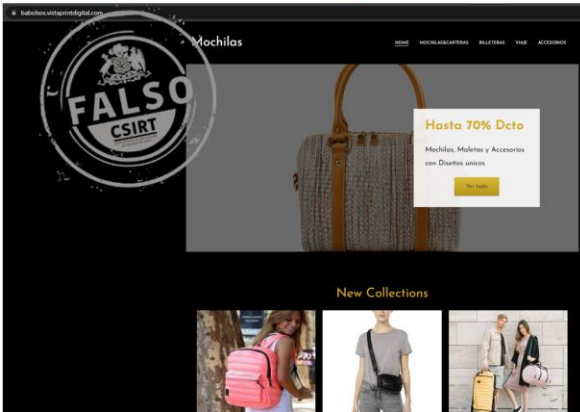
Sitios fraudulentos

Imagen del sitio



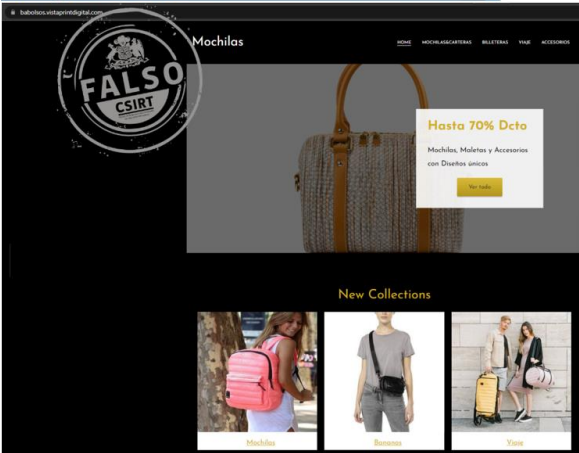
CSIRT informa sitio web falso de iCloud	
Alerta de seguridad cibernética	8FFR22-01083-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2022
Última revisión	20 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	https://rfsupplies[.]com/wp-content/update/info/83420a44cf9ca6419b80e89284c26fab/
IP	[160.153.50.7]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01083-01/
	https://www.csirt.gob.cl/media/2022/05/8FFR22-01083-01.pdf

Imagen del sitio



CSIRT informa sitio web que suplanta a tienda online	
Alerta de seguridad cibernética	8FFR22-01084-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de mayo de 2022
Última revisión	24 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	https://babolsos.vistaprintdigital[.]com/
IP	[198.55.28.6]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01084-01/
	https://www.csirt.gob.cl/media/2022/05/8FFR22-01084-01.pdf

Imagen del sitio



CSIRT informa activación de página falsa de tienda de mochilas	
Alerta de seguridad cibernética	8FFR22-01085-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2022
Última revisión	25 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	https://www.bagsafashions[.]shop/
IP	[104.17.198.73]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr22-01085-01/
	https://www.csirt.gob.cl/media/2022/05/8FFR22-01085-01.pdf

Phishing

Imagen del mensaje

Aviso importante: Cuenta suspendida.

BI Banco Itaú <facturacion@wowfactory.com.mx>



CSIRT advierte phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00531-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2022
Última revisión	20 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	https://bannco-Itau.cl.investoneuk[.]com/1653062530/wps/portal/newolb/web/login/ut/p/z1/SjPyk
IP	[217.79.245.244]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00531-01/
	https://www.csirt.gob.cl/media/2022/05/8FPH22-00532-01.pdf

Imagen del mensaje



CSIRT advierte phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00532-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2022
Última revisión	26 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	https://bamco-Itau.cl-zzvv[.]buzz/1653598918/bancochile-web/persona/login/index.html/login
IP	[172.67.155.66]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00532-01/
	https://www.csirt.gob.cl/media/2022/05/8FPH22-00532-01.pdf

Vulnerabilidades



INFORME DE Vulnerabilidad

9VSA21-00642-01
CSIRT comparte vulnerabilidades en dos plugin de Wordpress

PARA REGISTRAR | 1510
UN INCIDENTE | csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT alerta de dos vulnerabilidades en plugins de WordPress	
Alerta de seguridad cibernética	9VSA22-00642-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2022
Última revisión	19 de mayo de 2022
CVE	
CVE-2022-1654	
CVE-2021-25094	
Fabricante	
Jupiter y Tatsu	
Productos afectados	
Jupiter y Jupiter X Core. Tatsu Builder.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00642-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00642-01.pdf	



INFORME DE Vulnerabilidad

9VSA21-00643-01
CSIRT comparte vulnerabilidades en varios productos de Cisco

PARA REGISTRAR | 1510
UN INCIDENTE | csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT informa sobre vulnerabilidades en productos de Cisco		
Alerta de seguridad cibernética	9VSA22-00643-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	19 de mayo de 2022	
Última revisión	19 de mayo de 2022	
CVE		
CVE-2022-20797	CVE-2022-20765	CVE-2022-20721
CVE-2022-20806	CVE-2022-20759	CVE-2022-20722
CVE-2022-20807	CVE-2022-20681	CVE-2022-20723
CVE-2022-20809	CVE-2022-20677	CVE-2022-20724
CVE-2022-20802	CVE-2022-20718	CVE-2022-20725
CVE-2022-20666	CVE-2022-20719	CVE-2022-20726
CVE-2022-20667	CVE-2022-20720	CVE-2022-20727
CVE-2022-20668		
Fabricante		
Cisco		
Productos afectados		
Cisco Secure Network Analytics anteriores a 7.4.1.		
Cisco Expressway Series y Cisco TelePresence VCS 14.0 y anteriores.		
Cisco Enterprise Chat and Email (ECE) anteriores a 12.6(1) ES2.		
Cisco CSPC 2.10.0.2 y anteriores.		
Cisco ASA anteriores 9.12.4.38, 9.14.4, 9.15.1.21, 9.16.2.14 y 9.17.7.		

Cisco FMC y FTD software anteriores a 6.4.0.15, 6.6.5.2, 7.0.2 y 7.1.0.1.
800 Series Industrial Integrated Services Routers (Industrial ISRs)
800 Series Integrated Services Routers (ISRs)
1000 Series Connected Grid Router (CGR1000) Compute Modules
IC3000 Industrial Compute Gateways
Industrial Ethernet (IE) 4000 Series Switches
IOS XE-based devices configured with IOx
IR510 WPAN Industrial Routers

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00643-01/>

<https://www.csirt.gob.cl/media/2022/05/9VSA22-00643-01-1.pdf>



INFORME DE Vulnerabilidad

9VSA21-00644-01
CSIRT comparte vulnerabilidad en Cisco IOS XE

PARA REGISTRAR | 1510 UN INCIDENTE | [csirt.gob.cl](https://www.csirt.gob.cl)

CSIRT alerta de vulnerabilidad en Cisco IOS XR

Alerta de seguridad cibernética	9VSA22-00644-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2022
Última revisión	23 de mayo de 2022

CVE

CVE-2022-20821

Fabricante

Cisco

Productos afectados

Routers Cisco de la serie 8000 con software Cisco IOS XR 7.3.3.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00644-01/>

<https://www.csirt.gob.cl/media/2022/05/9VSA22-00644-01.pdf>



INFORME DE Vulnerabilidad

9VSA21-00645-01
CSIRT comparte vulnerabilidad en BIND

PARA REGISTRAR | 1510 UN INCIDENTE | [csirt.gob.cl](https://www.csirt.gob.cl)

CSIRT alerta de vulnerabilidades en productos VMware

Alerta de seguridad cibernética	9VSA22-00645-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2022
Última revisión	23 de mayo de 2022

CVE

CVE-2022-1183

Fabricante

ISC

Productos afectados

BIND 9.18.0 a 9.18.2, y versión 9.19.0 de BIND 9.19 development branch

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00645-01/>

<https://www.csirt.gob.cl/media/2022/05/9VSA22-00645-01.pdf>



INFORME DE Vulnerabilidad

9VSA21-00646-01
CSIRT comparte vulnerabilidades en Zoom

PARA REGISTRAR | 15 10 UN INCIDENTE | [csirt.gob.cl](https://www.csirt.gob.cl)

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT alerta vulnerabilidades en Zoom	
Alerta de seguridad cibernética	9VSA22-00646-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2022
Última revisión	25 de mayo de 2022
CVE	
CVE-2022-22784	CVE-2022-22786
CVE-2022-22785	CVE-2022-22787
Fabricante	
Zoom	
Productos afectados	
Zoom Client for Meetings (para Android, iOS, Linux, macOS, y Windows), versiones anteriores a la 5.10.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00646-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00646-01.pdf	



INFORME DE Vulnerabilidad

9VSA21-00647-01
CSIRT comparte vulnerabilidad en Spring de VMware

PARA REGISTRAR | 15 10 UN INCIDENTE | [csirt.gob.cl](https://www.csirt.gob.cl)

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT alerta de vulnerabilidad en Spring de VMware	
Alerta de seguridad cibernética	9VSA22-00647-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2022
Última revisión	26 de mayo de 2022
CVE	
CVE-2022-22978	
Fabricante	
VMware	
Productos afectados	
Spring Security versiones 5.5.6 y 5.6.3 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00647-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00647-01.pdf	



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA21-00648-01
CSIRT comparte vulnerabilidades día cero en Firefox y Thunderbird

PARA REGISTRAR | 1510
UN INCIDENTE | [csirt.gob.cl](https://www.csirt.gob.cl)



CSIRT alerta de vulnerabilidades día cero en Mozilla Firefox y Thunderbird	
Alerta de seguridad cibernética	9VSA22-00648-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2022
Última revisión	26 de mayo de 2022
CVE	
CVE-2022-1802	
CVE-2022-1529	
Fabricante	
Mozilla	
Productos afectados	
Firefox anteriores a 100.0.2	
Firefox for Android anteriores a 100.3.0	
Firefox anteriores a ESR 91.9.1	
Thunderbird anteriores a 91.9.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00648-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00648-01.pdf	

Actualidad

Ciberconsejos: Vulnerabilidades informáticas

Un paso clave hacia una mayor ciberseguridad es mantener nuestros equipos y su software siempre actualizados. Esto, porque entre las millones de líneas de código de los actuales programas informáticos es imposible evitar que se cuelen vulnerabilidades, errores que pueden facilitar el accionar de los ciberdelincuentes y que muchas veces cuesta muchísimo descubrir.

La forma en que los desarrolladores de software arreglan estas fallas es publicando actualizaciones a medida de que las vulnerabilidades son descubiertas, lo que puede suceder incluso años después de lanzado el programa.

Es por todo esto que decidimos dedicar esta semana de Ciberconsejos a aprender más de las vulnerabilidades informáticas, qué son y cómo protegernos de sus efectos:

<https://www.csirt.gob.cl/recomendaciones/ciberconsejos-vulnerabilidades/>.



The image displays five informational cards from CSIRT regarding software vulnerabilities. Each card features the CSIRT logo and the title 'Qué son y cómo protegernos Vulnerabilidades informáticas'.
1. **Card 1:** Explains that vulnerabilities are flaws in programs, often called 'weak points' that allow unauthorized access. It notes that intruders can exploit these to access data, take control of devices, or encrypt files for ransom. An illustration of a broken chain link is shown.
2. **Card 2:** Discusses vulnerabilities in the Internet of Things (IoT) and industrial applications, which can be exploited to allow unauthorized manipulation of physical objects. It mentions that CSIRT regularly publishes important new vulnerabilities at [csirt.gob.cl/vulnerabilidades](https://www.csirt.gob.cl/vulnerabilidades). An illustration of a robotic arm is shown.
3. **Card 3:** Lists various types of vulnerabilities that can be exploited, such as accessing/modifying system memory, installing malicious software (malware), destroying or altering confidential data, and damaging or destroying machines or domestic appliances connected to the internet. A skull and crossbones icon is used.
4. **Card 4:** Focuses on the importance of 'patches'. It states that software companies regularly release updates to fix new vulnerabilities, known as 'patches'. It emphasizes the need to keep software up-to-date and legal to access these patches. An illustration of a bandage is shown.
5. **Card 5:** Provides protection tips: keep applications and systems updated, download only legitimate programs, and check specialized portals for new vulnerabilities like [csirt.gob.cl/vulnerabilidades](https://www.csirt.gob.cl/vulnerabilidades). It also lists roles for cybersecurity: performing vulnerability scans for detection and correction, and conducting penetration tests. An illustration of a shield is shown.

Subsecretaría del Interior y Cámara de Comercio de Santiago coordinan medidas de seguridad para primer CyberDay de 2022

Como ya es tradición, entre el lunes 30 de mayo y el miércoles 1 de junio tendrá lugar una nueva versión del CyberDay, instancia organizada por la Cámara de Comercio de Santiago (CCS) y que, en esta ocasión, contará con la participación de 751 tiendas online de empresas y 44 fundaciones.

Al igual que en años anteriores, las autoridades se encuentran tomando las precauciones necesarias para evitar estafas, suplantaciones u otro tipo de fraudes durante el evento de compras on line.

Al respecto, el subsecretario del Interior, Manuel Monsalve, explicó que “para el Gobierno la seguridad de las personas es fundamental y eso incluye su vida digital, por tal motivo hemos tomado diferentes medidas para resguardarlos”.

Los consejos también los encuentran en: csirt.gob.cl/recomendaciones/consejos-cyberday-2022/.



The image displays a grid of six posters titled "CIBERCONSEJOS PARA UN CYBERDAY SEGURO" with the hashtag #Cyberd. Each poster provides specific advice:

- Poster 1 (Top Left):**
 - SI BUSCAS:** una buena oferta, hazlo directamente en los sitios web oficiales de las tiendas comerciales.
 - SI RECIBES UN CORREO:** inesperado con enlaces o archivos adjuntos sobre una oferta especial, descártalo, podría tratarse de una estafa de phishing.
 - STATS:** CYBERDAY: 795 comercios serán parte del evento. Verifica todas las webs oficiales en www.ccs.cl
- Poster 2 (Top Middle):**
 - LOS ATACANTES CREAN:** aplicaciones falsas que lucen idénticas a las originales. Si realizas tus compras desde tu tablet o smartphone, asegúrate de utilizar aplicaciones confiables.
 - ANTES DE COMPRAR:** actualiza las aplicaciones y la seguridad de tus dispositivos.
 - STATS:** CYBERDAY: 640 millones de dólares en transacciones dejó Cyber Day en 2021. Verifica todas las webs oficiales en www.cyber.cl
- Poster 3 (Top Right):**
 - NO GUARDES:** los datos de la forma de pago en tus dispositivos. Si logras a perderlos, te expones al robo de tus credenciales y posibles estafas.
 - ANTES DE COMPRAR:** analiza los pagos permitidos en el sitio web. Utiliza canales de pago formales y conocidos.
 - STATS:** CYBERDAY: 150 millones de visitas dejó el Cyber Day en Chile en 2021. Verifica todas las webs oficiales en www.cyber.cl
- Poster 4 (Bottom Left):**
 - NUNCA:** compartas la información de tus tarjetas de crédito, claves dinámicas o cuentas bancarias.
 - PON ATENCIÓN:** al sitio en el que navegas. Fíjate en detalles como la dirección web y la presencia del candado "https" ya que podría tratarse de un sitio falso.
 - STATS:** CYBERDAY: Precios claramente identificables y en moneda local. Verifica todas las webs oficiales en www.cyber.cl
- Poster 5 (Bottom Middle):**
 - PLANIFICA:** bien tus compras. A veces todo lo que se requiere para ser víctima de una estafa es un clic en el enlace incorrecto.
 - REVISAR:** periódicamente tus cuentas y saldos de tarjetas. Si encuentras transacciones que no coinciden con tus compras, contacta rápidamente a tu banco.
 - STATS:** CYBERDAY: resolución en línea. Hazte la contratación como consumidor y comerciante. Verifica todas las webs oficiales en www.cyber.cl
- Poster 6 (Bottom Right):**
 - Si adviertes ofertas vía email o sitios falsos,** contacta con el Equipo de Respuesta ante Incidentes de Seguridad Informática **CSIRT DE GOBIERNO** en CSIRT.GOB.CL o al teléfono **1510**.
 - Y si eres víctima de una estafa,** contacte con la Brigada de Cibercrimen de la Policía de Investigaciones de Chile **227080658**.

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.

- Sonia Inostroza Adasme
- Bárbara Palacios Cabezas
- María Gabriela Fernández
- Rodrigo Parada Queupumil
- Mario Cuadra
- Humberto Antonio Morales Gutiérrez
- Andrés Aldana F.
- Richard
- Carlos David Escalona Peraza
- Chemy Reyes González
- Claudio González
- Cristián Acuña
- Elizabeth
- Karina Hidalgo Albuerno
- Mathias Roco Fernández

