



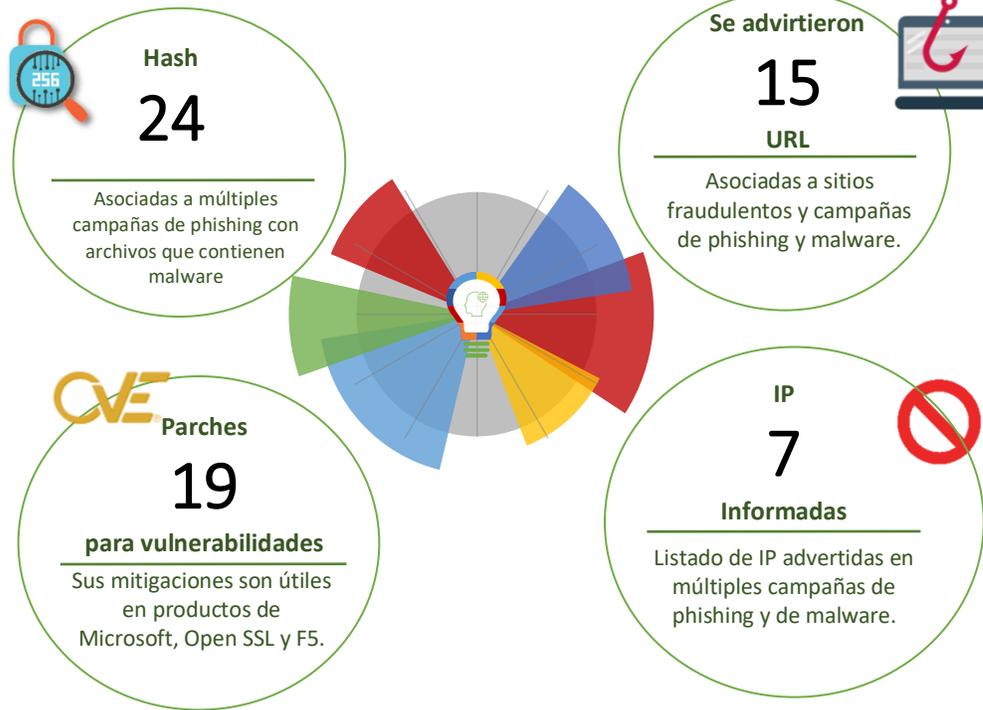
06-05-2022 | Año 4 | N°148

# Boletín de Seguridad Cibernética

Semana del 29 de abril  
al 5 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

Sitios fraudulentos .....	2
Phishing .....	3
Malware.....	5
Vulnerabilidades .....	7
Actualidad.....	9
Muro de la Fama .....	12

## Sitios fraudulentos

### Imagen del sitio



<b>CSIRT informa página web que suplanta al de Coopeuch</b>	
Alerta de seguridad cibernética	8FFR22-01080-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de abril de 2022
Última revisión	29 de abril de 2022
<b>Indicadores de compromiso</b>	
URL sitio falso	
hXXps://www.uniformesmussa[.]com/	
hXXps://ww3coopeuchc1.sportesweb[.]online/l/MTYzLjI0Ny43MC43MQ==/l/tef3/?#/	
IP	
[172.105.252.225]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8ffr22-01080-01/">https://www.csirt.gob.cl/alertas/8ffr22-01080-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/04/8FFR22-01080-01.pdf">https://www.csirt.gob.cl/media/2022/04/8FFR22-01080-01.pdf</a>	

## Phishing

### Imagen del mensaje



CSIRT informa phishing con falsa tarjeta bloqueada	
Alerta de seguridad cibernética	8FPH22-00517-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo de 2022
<b>Indicadores de compromiso</b>	
URL redirección	<a href="https://serviciservis[.]com/Centro_ayuda/cuenta-wabz/">https://serviciservis[.]com/Centro_ayuda/cuenta-wabz/</a>
URL sitio falso	<a href="https://sixthstartech[.]com/cmfmhil/pagina/imagenes/comun2008/banca-en-linea-personas.html">https://sixthstartech[.]com/cmfmhil/pagina/imagenes/comun2008/banca-en-linea-personas.html</a>
IP	[101.53.141.67]
<b>Enlaces para revisar el informe:</b>	
	<a href="https://www.csirt.gob.cl/alertas/8fph22-00517-01/">https://www.csirt.gob.cl/alertas/8fph22-00517-01/</a>
	<a href="https://www.csirt.gob.cl/media/2022/05/8FPH22-00517-01.pdf">https://www.csirt.gob.cl/media/2022/05/8FPH22-00517-01.pdf</a>

### Imagen del mensaje



CSIRT alerta phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00518-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo de 2022
<b>Indicadores de compromiso</b>	
URL redirección	<a href="hXXps://gestionvalpa[.]net/activacion/cuenta-afsn/">hXXps://gestionvalpa[.]net/activacion/cuenta-afsn/</a>
URL sitio falso	<a href="hXXps://kendranew[.]com/pagina/imagenes/comun2008/banca-en-linea-personas.html">hXXps://kendranew[.]com/pagina/imagenes/comun2008/banca-en-linea-personas.html</a>
IP	[190.114.253.236] [138.128.170.234]
<b>Enlaces para revisar el informe:</b>	
	<a href="https://www.csirt.gob.cl/alertas/8fph22-00518-01-2/">https://www.csirt.gob.cl/alertas/8fph22-00518-01-2/</a>
	<a href="https://www.csirt.gob.cl/media/2022/05/8FPH22-00518-01.pdf">https://www.csirt.gob.cl/media/2022/05/8FPH22-00518-01.pdf</a>

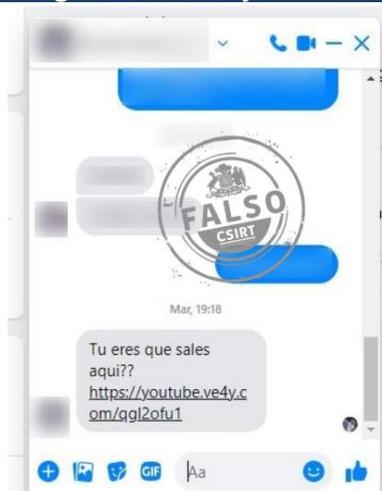
## Imagen del mensaje



### CSIRT advierte phishing con falsa cuenta suspendida

Alerta de seguridad cibernética	8FPH22-00519-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo de 2022
<b>Indicadores de compromiso</b>	
URL redirección	<a href="https://kaukaparaiso[.]com/ganador/cuenta-ozli/">https://kaukaparaiso[.]com/ganador/cuenta-ozli/</a>
URL sitio falso	<a href="https://nsp.kendranew[.]com/1651501451/Login">https://nsp.kendranew[.]com/1651501451/Login</a>
IP	[168.232.165.180] [138.128.170.234]
<b>Enlaces para revisar el informe:</b>	
	<a href="https://www.csirt.gob.cl/alertas/8fph22-00519-01/">https://www.csirt.gob.cl/alertas/8fph22-00519-01/</a>
	<a href="https://www.csirt.gob.cl/media/2022/05/8FPH22-00519-01.pdf">https://www.csirt.gob.cl/media/2022/05/8FPH22-00519-01.pdf</a>

## Imagen del mensaje



### CSIRT advierte phishing a través de Facebook Messenger

Alerta de seguridad cibernética	8FPH22-00520-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2022
Última revisión	4 de mayo de 2022
<b>Indicadores de compromiso</b>	
URL redirección	<a href="https://youtube.ve4y[.]com/qgl2ofu1">hXXps://youtube.ve4y[.]com/qgl2ofu1</a>
URL sitio falso	<a href="https://ranzer-gost.format[.]com/">hXXps://ranzer-gost.format[.]com/</a>
IP	[104.18.134.62]
<b>Enlaces para revisar el informe:</b>	
	<a href="https://www.csirt.gob.cl/alertas/8fph22-00520-01/">https://www.csirt.gob.cl/alertas/8fph22-00520-01/</a>
	<a href="https://www.csirt.gob.cl/media/2022/05/8FPH22-00520-01.pdf">https://www.csirt.gob.cl/media/2022/05/8FPH22-00520-01.pdf</a>

## Malware

### Imagen del mensaje

Estimado(A)

**Tesorería General de la República (TGR)** informa que existen obligaciones, producto de una liquidación tributaria que se encuentra impaga. Una liquidación tributaria corresponde a la determinación de diferencias de impuesto detectadas por el SII.

Le invitamos a regularizar esta situación a través de nuestro sitio web, en el menú **Recaudación / Pagos Impuestos Fiscales**, a la brevedad posible, a fin evitar las molestias de un cobro judicial, el cual entre otras acciones, puede implicar el embargo de bienes u otras medidas de apremio.

Puede descargar el informe generador por el TGR en el **Botón** de información.

#### Adjuntos de información

Atención: Informe contraseña para ver su PDF. **¡FALSO!** No clicas en tu contraseña a nadie, contraseña : 020105

02/05/2022 12:51:40



### CSIRT advierte campaña con malware que suplanta a la TGR

Alerta de seguridad cibernética	2CMV21-00296-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2022
Última revisión	2 de mayo de 2022

#### Indicadores de compromiso

##### SHA256

```
03840e262fc8208312074c8c0cc5790c586516c1d36536425f52a0768d69021e
9181e3ecde1ea8f60d4eb0c16f760c51a3f099766bcc1eb9ad19136894a5ada
bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f
cb7f180d74dd744fe32260026cc12d051af0c5f6e1ef31adc387773a1b44f967
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
754aad3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f
16add40397c045ed4c393f83443a10cb583171e2fe1f95782e06276db474adb
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
880a365b8d47729b16359bd90136ecbc176e3191eba9a7f18f6285a0cf624620
ea972fdc38c685ace5c5a23b849ac673825e7e4d257bb5b06312ec43c1645400
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
610ce9c0087f8b7a87cb839efe47338121d5681d4a4bd8f248acf6c29969c47
```

##### IoC URL

```
https://physionormandie[.]com/wp-content/languages/-
/https://www.tgr.cl
https://www.tri-
techmechanical[.]com/components/com_config/dad/HD812U1NDS71Y[.]
zip
```

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/2cmv22-00296-01/>

<https://www.csirt.gob.cl/media/2022/05/2CMV22-00296.pdf>

## Imagen del mensaje

Asunto: Tesorería General de la República (TGR) informa que existen obligaciones pendientes.



Estimado(A)

Tesorería General de la República (TGR) informa que existen obligaciones, producto de una liquidación tributaria que se encuentra impaga. Una liquidación tributaria corresponde a la determinación de diferencias de impuesto detectadas por el SII.

Le invitamos a regularizar esta situación a través de nuestro sitio web, en el menú **Recaudación / Pagos / Impuestos Fiscales**, o la brevedad posible, a fin evitar las molestias de un cobro judicial, el cual entre otras acciones, puede implicar el embargo de bienes u otras medidas de apremio.

Puede descargar el informe generador por el TGR en el Adjuntos de información.

### Adjuntos de información

Atención: Informe contraseñ@ para ver su PDF. Nunca le des tu contraseñ@ a nadie.  
contraseñ@ :020205

## CSIRT advierte phishing con malware suplantando a TGR

Alerta de seguridad cibernética	2CMV21-00297-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2022
Última revisión	4 de mayo de 2022

### Indicadores de compromiso

#### SHA256

```
4a2d4e8907797a94e5cd032cc67c7a1116f9f640c6aaed531afc60578385adf5
20eb84bc76f6da4eff41a66dfcc0b4c5372233d1568f73d701b9f9f8e8c98da1
2182ac079032bc9e21f20646ff5be6f9a8536a70ce2824b1c2783178e8f2f723
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
cb7f180d74dd744fe32260026cc12d051af0c5f6e1ef31adc387773a1b44f967
bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f
754aad3aa19e07f2ba20217ddb0412d90e686e9965100ec7dc16475dea2077f
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
8941f7cc75ae085f5b45c94b831ecc0f8a2aeba792d75b98292660feda2b8775
fd99e83a1161f3cf6bc07f5f973d0272e42e7f1aa9fa7ae22c9c9b1378b3d6c5
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
5ee419a1bda6b3d9ed3c5ffcaa2b4763bd7e7c57d40caa4f89ceebcd689ac840
```

#### IoC URL

```
hXXps://phisionormandie[.]com/wp-content/languages/-
/https://www.tgr.cl/?cliente=
hXXps://www.stt.eesc.usp[.]br/wp-content/languages/SII63301220.zip
hXXps://www.hardam[.]biz/stats/awsindex/TD821YEJSDM813UJR.zip
```

#### Enlaces para revisar el informe:

```
https://www.csirt.gob.cl/alertas/2cmv22-00297-01/
https://www.csirt.gob.cl/media/2022/05/2CMV22-00297.pdf
```

## Vulnerabilidades



<b>CSIRT alerta de vulnerabilidad crítica en Microsoft Edge</b>	
Alerta de seguridad cibernética	9VSA22-00627-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de mayo de 2022
Última revisión	3 de mayo de 2022
<b>CVE</b>	
CVE-2022-1314 - CVE-2022-1313 - CVE-2022-1312 CVE-2022-1310 - CVE-2022-1308 - CVE-2022-1307 CVE-2022-1306 - CVE-2022-1305 - CVE-2022-1364 CVE-2022-1309	
<b>Fabricante</b>	
Microsoft	
<b>Productos afectados</b>	
Microsoft Edge (Chromium-based): 79.0.309.71 – 100.0.1185.39.	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00627-01/">https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00627-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/05/9VSA22-00627-01.pdf">https://www.csirt.gob.cl/media/2022/05/9VSA22-00627-01.pdf</a>	



<b>CSIRT alerta de vulnerabilidades en OpenSSL</b>	
Alerta de seguridad cibernética	9VSA22-00628-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2022
Última revisión	4 de mayo de 2022
<b>CVE</b>	
CVE-2022-1292 - CVE-2022-1343 - CVE-2022-1434 CVE-2022-1473	
<b>Impacto</b>	
CVE-2022-1292: Moderado CVE-2022-1343: Moderado CVE-2022-1434: Bajo CVE-2022-1473: Bajo	
<b>Fabricante</b>	
OpenSSL	
<b>Productos afectados</b>	
OpenSSL versiones 1.0.2, 1.1.1 y 3.0.	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00628-01/">https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00628-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/05/9VSA22-00628-01.pdf">https://www.csirt.gob.cl/media/2022/05/9VSA22-00628-01.pdf</a>	



<b>CSIRT alerta de vulnerabilidad crítica en BIG-IP de F5</b>	
Alerta de seguridad cibernética	9VSA22-00629-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de mayo de 2022
Última revisión	5 de mayo de 2022
<b>CVE</b>	
CVE-2022-1388	
<b>Fabricante</b>	
F5	
<b>Productos afectados</b>	
BIG-IP, versiones:	
16.1.0 a 16.1.2	
15.1.0 a 15.1.5	
14.1.0 a 14.1.4	
13.1.0 a 13.1.4	
12.1.0 a 12.1.6 (no serán parchados)	
11.6.1 a 11.6.5 (no serán parchados)	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00622-01/">https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00622-01/</a>	
<a href="https://www.csirt.gob.cl/media/2022/04/9VSA22-00622-01.pdf">https://www.csirt.gob.cl/media/2022/04/9VSA22-00622-01.pdf</a>	

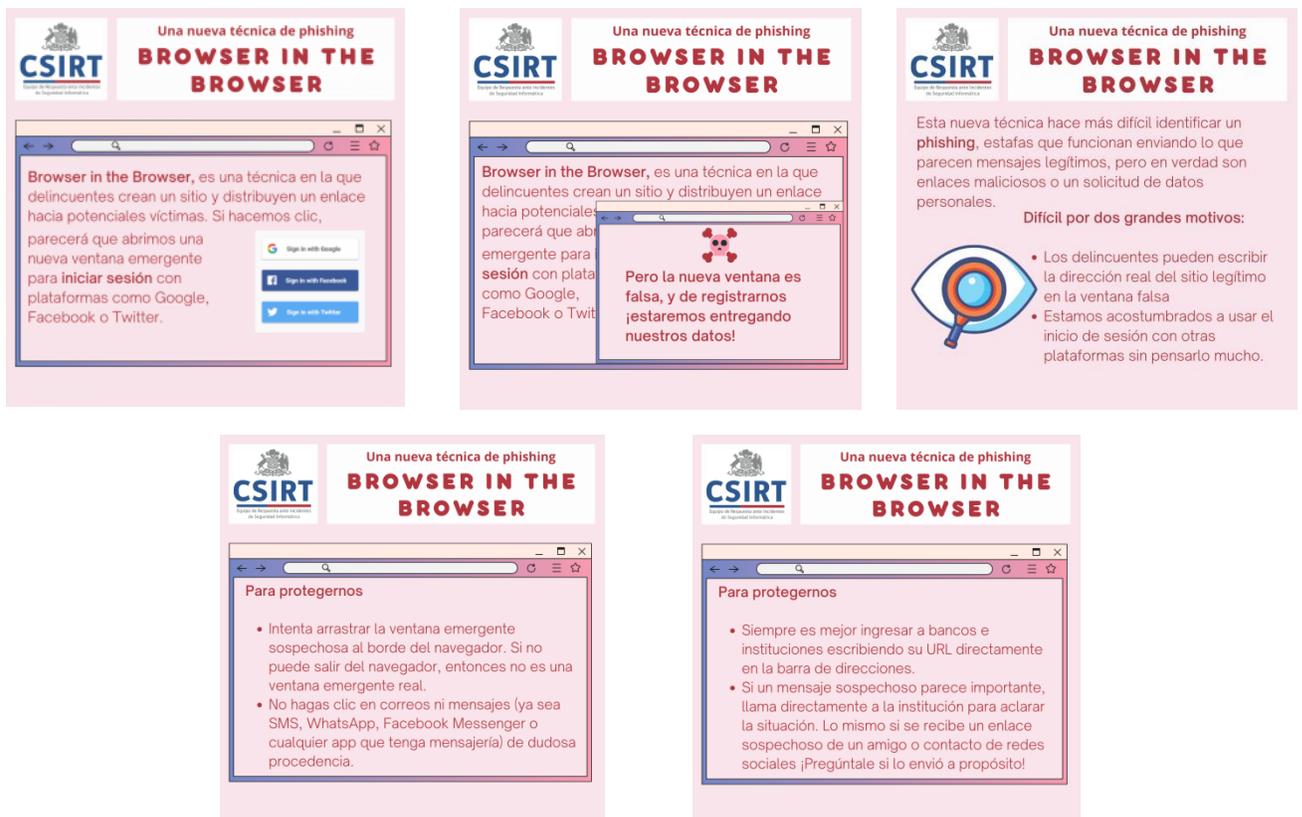
## Actualidad

### Ciberconsejos | Browser In The Browser (BITB), la nueva técnica que dificulta identificar un phishing

Una de las técnicas más utilizadas por los ciberdelincuentes es el phishing, la que busca engañar a sus víctimas con correos o páginas web falsas, con el objetivo de inyectar programas maliciosos u obtener los datos personales de los usuarios, como claves bancarias o de redes sociales y así robarles dinero o suplantarlos en internet, entre otros delitos.

Y así como los sistemas de ciberseguridad han ido mejorando, las técnicas de phishing también han evolucionado. Un ejemplo de esto es la técnica conocida como Browser in the Browser (BITB).

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



The infographic is divided into five panels, each with the CSIRT logo and the title "Una nueva técnica de phishing BROWSER IN THE BROWSER".

- Panel 1:** Explains that attackers create a site and distribute a link to potential victims. When clicked, it appears as if a new window is opening for login on platforms like Google, Facebook, or Twitter.
- Panel 2:** States that attackers create a site and distribute a link to potential victims. It appears as if a new window is opening for login on platforms like Google, Facebook, or Twitter. However, the new window is fake, and they will steal our data!
- Panel 3:** Explains that this new technique makes it more difficult to identify phishing, as they use legitimate-looking messages, but in reality, they are malicious links or requests for personal data. It is difficult for two main reasons:
  - Attackers can write the real URL of the legitimate site in the fake window.
  - We are accustomed to using login platforms without thinking much.
- Panel 4:** Titled "Para protegernos" (To protect ourselves), it lists:
  - Try to drag the suspicious pop-up window from the edge of the browser. If you cannot move it, it is not a real pop-up window.
  - Do not click on emails or messages (whether via SMS, WhatsApp, Facebook Messenger, or any messaging app) of dubious origin.
- Panel 5:** Titled "Para protegernos", it lists:
  - It is always better to enter banks and institutions by writing the URL directly in the address bar.
  - If a suspicious message seems important, call the institution directly to clarify the situation. Even if you receive a link from a friend or contact on social media, ask them if they sent it to you!

## Ciberconsejos | Decálogo de Ciberseguridad

Como CSIRT de Gobierno, sabemos bien que la ciberseguridad depende de todos. Por eso, es esencial que tengamos siempre presentes algunas reglas básicas para estar más seguros en línea.

Es con ese objetivo que diseñamos el siguiente Decálogo de Ciberseguridad, diez consejos que todos debemos conocer, indispensables para tener una vida digital más segura.

Enlace: <https://www.csirt.gob.cl/recomendaciones/decalogo-de-ciberseguridad/>.



**DECÁLOGO DE CIBERSEGURIDAD**

DIEZ RECOMENDACIONES QUE TODOS DEBEMOS CONOCER

1. No hagas clic en enlaces que lleguen por email, mensajes de texto o WhatsApp no solicitados.

Pueden descargar programas maliciosos (malware) o pedir información confidencial, como datos bancarios, haciéndose pasar por mensajes legítimos (técnica conocida como phishing).



**DECÁLOGO DE CIBERSEGURIDAD**

2. Activa autenticación de dos pasos o doble factor de autenticación en cuentas y apps. Así no basta con tu clave para robar tu perfil, exige un segundo paso, como una clave temporal enviada a tu celular.

3. Crea contraseñas robustas y diferentes en cada sitio. Nunca uses fechas o números con significado para ti. Ideal es elegir dos o tres palabras inconexas y usar mayúsculas, números y otros signos (como puntuación y exclamación).



**DECÁLOGO DE CIBERSEGURIDAD**

4. No entres a sitios sospechosos, como los de pornografía y torrents, especialmente si no cuentas con un buen antivirus, ya que suelen ser usados para distribuir malware.

5. Solo descarga programas autorizados, originales y de las tiendas oficiales (de los mismos proveedores, la App Store o Google Play) y tenlos actualizados, así suman soluciones a nuevas programas maliciosos que los puedan afectar.



**DECÁLOGO DE CIBERSEGURIDAD**

6. Realiza respaldos periódicos de los datos más importantes que manejes. Estos deben mantenerse desconectados, para evitar que sean infectados si los dispositivos que respaldan reciben el ataque de un malware.

7. No publiques información confidencial en redes sociales, como datos personales y que permitan individualizarte, a tus familiares o dónde vives o vacaciones. Menos aún tu RUT o fotos del carnet de identidad.



**DECÁLOGO DE CIBERSEGURIDAD**

9. Nunca entregues a nadie tus claves bancarias, de redes sociales u otras cuentas importantes, por mucho que diga trabajar en el banco o empresa en cuestión.

8. Si vas a teletrabajar, solicita una VPN para tu conexión a la red del trabajo.



**DECÁLOGO DE CIBERSEGURIDAD**

10. Solo conecta a tu equipo unidades USB (como pendrives o discos duros externos) si es estrictamente necesario y proviene de una persona de confianza. Pueden ser vectores de malware.

Síguenos en nuestras redes sociales  
Informa sobre tus actividades y mantenlas actualizadas

CSIRT  
Teléfono: 92 200 6 0000  
Correo: [www.csirt.gob.cl](mailto:www.csirt.gob.cl)

Twitter, LinkedIn, Instagram

## 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.

- Nicolás Moreno
- César López
- David Soto
- Juan Alfonso Muñoz

