



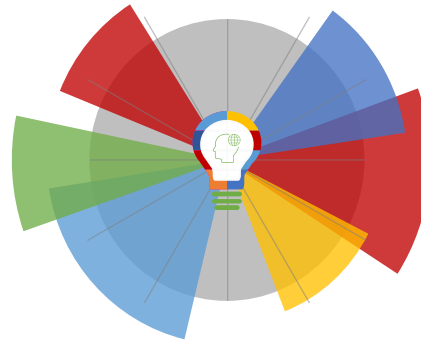
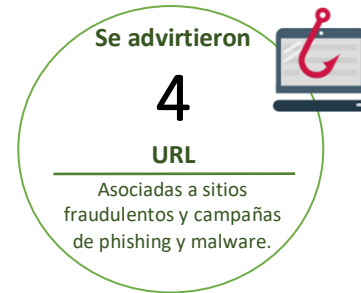
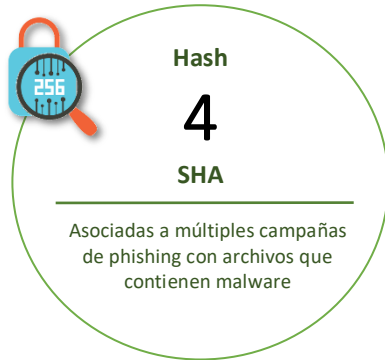
09-12-2021 | Año 3 | N°127

# Boletín de Seguridad Cibernética

Semana del 3 al 9 de  
diciembre de 2021



## 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
Vulnerabilidades .....	3
Actualidad.....	6
Recomendaciones y buenas prácticas .....	8
Muro de la Fama .....	9

## Malware

### Imagen del mensaje



### CSIRT informa campaña con malware Emotet

Alerta de seguridad cibernética	2CMV21-00255-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de diciembre de 2021
Última revisión	06 de diciembre de 2021
<b>Indicadores de compromiso</b>	
SHA256	
5D0311243534A50B4FFFA6BB32A952F86E51194D372741B30DBEA12C51EB4C443D46D69A3CB137E443329C73E8551DCFAA471BC271D891703850A0C931FAACD8	
<b>IoC red</b>	
<a href="http://www.duoyuhudong[.]cn/wp-content/we8xi/">http://www.duoyuhudong[.]cn/wp-content/we8xi/</a>	
<a href="http://sadabaha.com[.]np/wp-includes/pUMqITCt83a/">http://sadabaha.com[.]np/wp-includes/pUMqITCt83a/</a>	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/2cmv21-00255-01/">https://www.csirt.gob.cl/alertas/2cmv21-00255-01/</a>	
<a href="https://www.csirt.gob.cl/media/2021/12/2CMV21-00255-01-2.pdf">https://www.csirt.gob.cl/media/2021/12/2CMV21-00255-01-2.pdf</a>	

### Imagen del mensaje



### CSIRT advierte campaña de malware con Emotet

Alerta de seguridad cibernética	2CMV21-00256-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de diciembre de 2021
Última revisión	9 de diciembre de 2021
<b>Indicadores de compromiso</b>	
SHA256	
cb836996444ea64cbbc74d40ae7a98f45a0ba279176f9b453ab7bcf62a144ded67784b75c77762be449b4a271f9afa04520817197749c84a82ca8d1942867163	
<b>IoC Red</b>	
<a href="http://www.kjtaxpro[.]com/r0bh/">www.kjtaxpro[.]com/r0bh/</a>	
<a href="http://173.232.204.89/bnikg[.]exe">http://173.232.204.89/bnikg[.]exe</a>	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/2cmv21-00256-01/">https://www.csirt.gob.cl/alertas/2cmv21-00256-01/</a>	
<a href="https://www.csirt.gob.cl/media/2021/12/2CMV21-00256-01.pdf">https://www.csirt.gob.cl/media/2021/12/2CMV21-00256-01.pdf</a>	

## Vulnerabilidades



<b>CSIRT alerta de vulnerabilidades en IBM QRadar SIEM</b>	
Alerta de seguridad cibernética	9VSA21-00528-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de diciembre de 2021
Última revisión	6 de diciembre de 2021
<b>CVE</b>	
CVE-2017-15713	
CVE-2021-32399	
CVE-2021-29650	
CVE-2021-29154	
CVE-2021-22555	
CVE-2020-27777	
CVE-2021-3715	
CVE-2019-9924	
CVE-2018-18751	
CVE-2018-11768	
CVE-2020-7226	
CVE-2020-9492	
CVE-2018-8029	
CVE-2020-13954	
CVE-2021-22696	
CVE-2021-28163	
CVE-2021-28169	
CVE-2021-28165	
CVE-2021-29425	
CVE-2021-2161	
<b>Fabricante</b>	
IBM	
<b>Productos afectados</b>	
IBM Qradar SIEM: 7.3.0 a 7.4.3 Fix Pack 2, 7.4.3 GA.	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00528-01/">https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00528-01/</a>	
<a href="https://www.csirt.gob.cl/media/2021/12/9VSA21-00528-01.pdf">https://www.csirt.gob.cl/media/2021/12/9VSA21-00528-01.pdf</a>	



<b>CSIRT alerta de vulnerabilidades en Google Chrome</b>	
Alerta de seguridad cibernética	9VSA21-00529-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de diciembre de 2021
Última revisión	7 de diciembre de 2021
<b>CVE</b>	
CVE-2021-4062	
CVE-2021-4068	
CVE-2021-4067	
CVE-2021-4066	
CVE-2021-4065	
CVE-2021-4064	
CVE-2021-4063	
CVE-2021-4061	
CVE-2021-4052	
CVE-2021-4059	
CVE-2021-4058	
CVE-2021-4057	
CVE-2021-4056	
CVE-2021-4055	
CVE-2021-4054	
CVE-2021-4053	
<b>Fabricante</b>	
Google	
<b>Productos afectados</b>	
Google Chrome, versiones 70.0.3538.67 a 96.0.4664.45.	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00529-01/">https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00529-01/</a>	
<a href="https://www.csirt.gob.cl/media/2021/12/9VSA21-00529-01.pdf">https://www.csirt.gob.cl/media/2021/12/9VSA21-00529-01.pdf</a>	



<b>CSIRT alerta de vulnerabilidades críticas en VPN de SonicWall</b>	
Alerta de seguridad cibernética	9VSA21-00530-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de diciembre de 2021
Última revisión	9 de diciembre de 2021
<b>CVE</b>	
CVE-2021-20038	
CVE-2021-20045	
CVE-2021-20043	
CVE-2021-20040	
CVE-2021-20039	
CVE-2021-20041	
CVE-2021-20042	
CVE-2021-20044	
CVE-2021-20045	
<b>Fabricante</b>	
SonicWall	
<b>Productos afectados</b>	
SonicWall SMA 100, SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v.	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00530-01/">https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00530-01/</a>	
<a href="https://www.csirt.gob.cl/media/2021/12/9VSA21-00530-01.pdf">https://www.csirt.gob.cl/media/2021/12/9VSA21-00530-01.pdf</a>	

## Actualidad

### El Control de la Semana | No. 19 Acuerdos de Nivel de Servicio

En su número 19, el Control de la Semana explica de qué se trata un Acuerdo de Nivel de Servicio (SLA), y cómo una institución debe definirlo para obtener las mejores prestaciones de sus proveedores.

Todo lo encontrarán en el siguiente documento descargable:

<https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-19/>



## Ciberconsejos para un escaneo más seguro de los códigos QR

Los códigos QR son esas cajas que parecen «pixeladas» y que han proliferado en Chile especialmente desde el inicio de la actual pandemia, ya que permiten abrir rápidamente información en los teléfonos de clientes y usuarios en lugar de, por ejemplo, usar cartas físicas en los restaurantes.

Pero, no sería Ciberconsejos si no fuéramos a recomendarles tener precaución con esta tecnología. Porque así como un QR puede contener información valiosa y segura, también puede ser aprovechado por inescrupulosos para que descarguemos, sin querer, programas maliciosos, o entremos en sitios falsos. Para evitarlo, debemos ser cuidadosos y seguir estos Ciberconsejos: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-qr/>.



**CIBERCONSEJOS PARA UN ESCANEO SEGURO DE CÓDIGOS QR**

• **¿Qué es un código QR?**

Son códigos de barras mejorados que almacenan mucha más información y son más fáciles de leer, por lo que fueron denominados en inglés códigos "quick response", o sea, de respuesta rápida.

Su forma es cuadrada y hoy pueden ser leídos por la mayoría de los smartphones. Son, funcionalmente, enlaces a contenido en internet.



**CIBERCONSEJOS PARA UN ESCANEO SEGURO DE CÓDIGOS QR**

• Los códigos QR son una forma simple de enlazar el mundo físico con la web. Algunos fines con que se utilizan:

- Descargar aplicaciones
- Acceder al menú de un restaurante
- Compartir tarjetas de presentación
- Promocionar artículos y ofertas en la web o en las calles.
- Implementar el pasaporte Covid-19 y pases de movilidad.



**CIBERCONSEJOS PARA UN ESCANEO SEGURO DE CÓDIGOS QR**

• Riesgos de un código QR

- **QRishing:** Ataque tipo phishing. El usuario escanea el código QR y es dirigido a un sitio web falso, donde se solicitan sus credenciales e información sensible.
- **Descarga de malware:** Al escanear el código QR, la persona es dirigida a una web de descarga de malware, pudiendo robar información, activar cámaras o micrófono y suscribir al usuario servicios premium, entre otros.



**CIBERCONSEJOS PARA UN ESCANEO SEGURO DE CÓDIGOS QR**

• Riesgos de un código QR

- **QRlacking o secuestro de sesión:** Consiste en robar la cuenta de un servicio que inicie sesión con código QR, por ejemplo WhatsApp. La víctima escanea un código malicioso que suplanta al original y el delincuente accede a su cuenta.
- **Rastreo:** Con estos códigos es posible saber por dónde navega el usuario en internet y conocer su geolocalización.



**CIBERCONSEJOS PARA UN ESCANEO SEGURO DE CÓDIGOS QR**

• ¿Cómo evitar estos riesgos?

- Deshabilitar la opción de abrir de forma automática los enlaces al escanear un código QR.
- Evitar escanear códigos QR de dudosa procedencia.
- Antes de ingresar al enlace ofrecido por el QR, revisar que su URL es confiable y coincide con la carta del restaurante, tríptico, anuncio o publicación web.



**CIBERCONSEJOS PARA UN ESCANEO SEGURO DE CÓDIGOS QR**

• ¿Cómo evitar estos riesgos?

- Nunca ingresar al sitio ni escribir sus contraseñas si la URL no coincide con las que el sitio que quiere usar debería tener.
- Comprobar, en caso de administrar un negocio, que los códigos QR que usa o promociona no han sido alterados.



## 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.

- Diego Garcés
- Víctor Cofré
- Soledad Pacheco

