



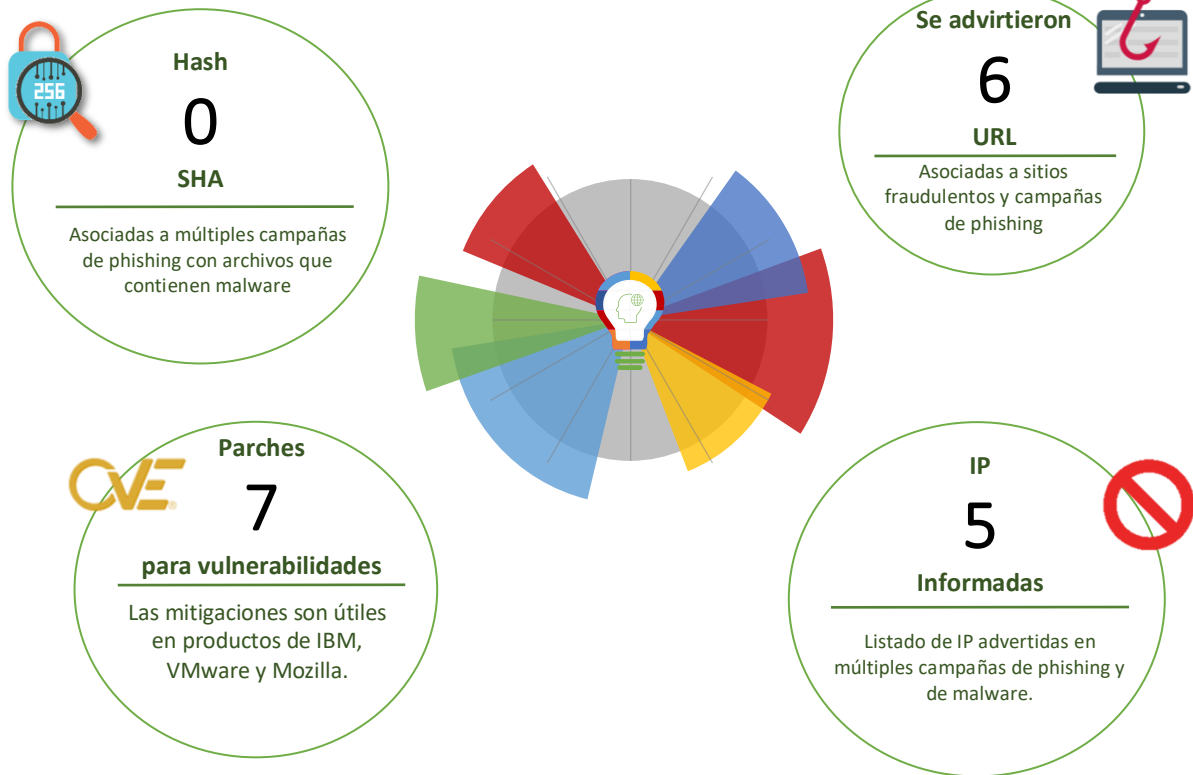
06-08-2021 | Año 3 | N°109

Boletín de Seguridad Cibernética

Semana del 30 de julio a 05
de agosto 2021



La semana en cifras

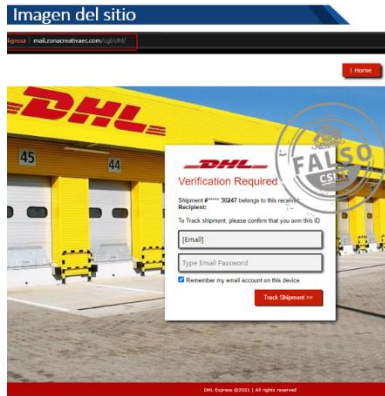


*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web <https://www.csirt.gob.cl>

Contenido

Sitios fraudulentos	2
Phishing	4
Vulnerabilidades	5
Actualidad.....	7
Recomendaciones y buenas prácticas	11
Muro de la Fama	12

Sitios fraudulentos

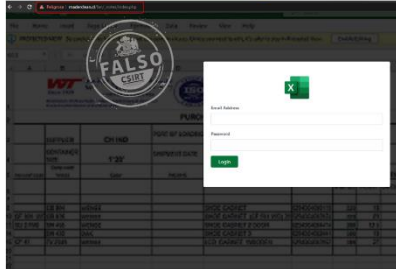


CSIRT alerta de página fraudulenta que suplanta a DHL	
Alerta de seguridad cibernética	8FFR21-00998-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de julio de 2021
Última revisión	29 de julio de 2021
Indicadores de compromiso	
URL sitio falso	https://mail.zonacreativaec[.]com/cgl/clhl/
IP	[192.232.251.15]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr21-00998-01/
	https://www.csirt.gob.cl/media/2021/07/8FFR21-00998-01.pdf



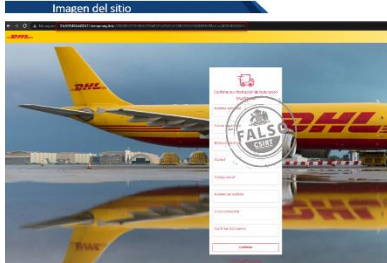
CSIRT alerta de página fraudulenta que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR21-00999-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de agosto de 2021
Última revisión	2 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	https://jbshtl.secure52serv[.]com/receipt/secureNetflix/facc09273c45d37bf42472c456d9d738/login
IP	[104.244.125.41]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr21-00999-01/
	https://www.csirt.gob.cl/media/2021/08/8FFR21-00999-01.pdf

Imagen del sitio

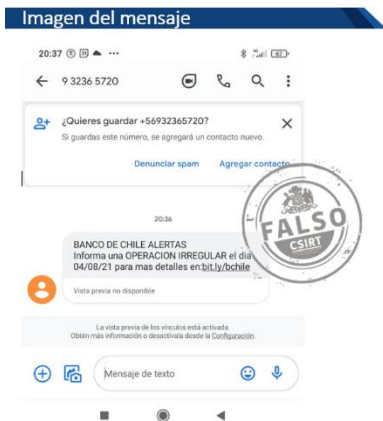


CSIRT alerta de página fraudulenta que suplanta a Excel	
Alerta de seguridad cibernética	8FFR21-01000-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de agosto de 2021
Última revisión	4 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	
	https://maderclean[.]cl/fan/_notes/index.php
IP	
	[66.232.107.218]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8ffr21-01000-01/
	https://www.csirt.gob.cl/media/2021/08/8FFR21-01000-01.pdf

Phishing



CSIRT alerta de campaña de phishing que suplanta a DHL	
Alerta de seguridad cibernética	8FPH21-00422-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de agosto de 2021
Última revisión	5 de agosto de 2021
Indicadores de compromiso	
URL sitio falso	http://31c5ff24944432411 temporary[.]link//SOD2EFZGTRY8HGZD548TEF4Z5HY//EZ0B3GF6SF56SDEFMPR/cl-es/BOBMSX02X1/
IP	[133.130.69.156]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph21-00420-01/
	https://www.csirt.gob.cl/media/2021/08/8FPH21-00420-01.pdf



CSIRT alerta ante campaña de smishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00423-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de agosto de 2021
Última revisión	5 de agosto de 2021
Indicadores de compromiso	
URL de SMS	bit[.]ly/bchile
URL sitio falso	https://xn--wbprsns-prtlbncdchl-chle-q8bfcc8scrd4kf9pf[.]com/1628171977/bcochile-web/persona/login/index.html/login
IP	[66.29.141.130]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph21-00423-01/
	https://www.csirt.gob.cl/media/2021/08/8FPH21-00423-01.pdf

Vulnerabilidades



CSIRT alerta ante vulnerabilidades que afectan a Mozilla Thunderbird	
Alerta de seguridad cibernética	9VSA21-00477-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de agosto de 2021
Última revisión	3 de agosto de 2021
CVE	
CVE-2021-29969	
CVE-2021-29970	
CVE-2021-29976	
CVE-2021-30547	
Fabricante	
Mozilla	
Productos afectados	
Mozilla Thunderbird 78.3.1-1.el8_2 a la 78.11.0-1.el8_2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00477-01	
https://www.csirt.gob.cl/media/2021/08/9VSA21-00477-01.pdf	



CSIRT alerta de vulnerabilidad en IBM QRadar	
Alerta de seguridad cibernética	9VSA21-00478-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de agosto de 2021
Última revisión	5 de agosto de 2021
CVE	
CVE-2021-29757	
Fabricante	
IBM	
Productos afectados	
IBM QRadar User Behavior Analytics 4.1.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00478-01	
https://www.csirt.gob.cl/media/2021/08/9VSA21-00478-01.pdf	



CSIRT alerta ante vulnerabilidades que afectan a VMware

Alerta de seguridad cibernética	9VSA21-00479-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de agosto de 2021
Última revisión	5 de agosto de 2021
CVE	
CVE-2021-22002	
CVE-2021-22003	
Fabricante	
VMware	
Productos afectados	
VMware Workspace One Access (Access)	
VMware Identity Manager (vIDM)	
VMware vRealize Automation (vRA)	
VMware Cloud Foundation 4.0 a 4.2.1.	
vRealize Suite Lifecycle Manager	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00479-01	
https://www.csirt.gob.cl/media/2021/08/9VSA21-00479-01.pdf	

Actualidad

Ministerio del Interior y Subsecretaría de la Niñez lanzan junto a Entel nueva ciberguía de consejos para que los padres enfrenten junto a sus hijos las amenazas en la red

Ministerio del Interior y Seguridad Pública

Ciberguía de mediación parental

Consejos de uso responsable de la internet por parte de los niños, niñas y adolescentes.



En el marco de la celebración del Día del Niño esta semana, el Ministerio del Interior, a través del CSIRT de Gobierno, el Ministerio de Desarrollo Social y Familia, a través de la Subsecretaría de la Niñez, la Fundación Katy Summer y Entel, a través de una alianza público privada, presentaron una nueva Ciberguía de Mediación Parental.

“Nuestros niños necesitan del acompañamiento y la enseñanza de sus padres para usar internet, ya que necesitan conocer de los peligros que conlleva el ciberespacio y cómo protegerse”, explicó el Subsecretario del Interior, Juan Francisco Galli. “Por eso creamos esta nueva ciberguía, que además de ayudar a los padres a educar a sus hijos en prácticas digitales ciberseguras, representa un nuevo ejemplo de colaboración público-privada, algo que ha estado impulsando el CSIRT de Gobierno, dependiente de esta Subsecretaría”, agregó.

Más información y la guía, aquí: <https://csirt.gob.cl/noticias/nueva-ciberguia-diadelnino2021/>.

CSIRT de Gobierno abre 6° Exhibición Internacional de Seguridad Integral en panel con Senador Pugh y representantes del BID



Esta semana inició la sexta versión de SeguridadExpo Chile, convención que reúne especialistas de seguridad en diversos ámbitos, como la seguridad industrial, laboral y bioseguridad, prevención de incendios y riesgos naturales, y por supuesto, ciberseguridad.

Fue precisamente la ciberseguridad la que inició la jornada, con una conversación entre el Director Nacional del CSIRT de Gobierno, Carlos Landeros, y el Especialista Sectorial en Ciberseguridad del Banco Interamericano de Desarrollo (BID), Santiago Paz, moderado por el senador Kenneth Pugh, parlamentario que se ha enfocado en impulsar iniciativas de seguridad digital. El encuentro virtual contó además con las presentaciones del Subsecretario de Telecomunicaciones, Francisco Moreno, y la Representante del BID en Chile, María Florencia Attademo-Hirst.

Encuentra los detalles aquí: <https://www.csirt.gob.cl/noticias/csirt-de-gobierno-abre-6-exhibicion-internacional-de-seguridad-integral-en-panel-con-senador-pugh-y-representantes-del-bid/>.

El Comando de la Semana | No. 11 SQLMAP

Esta vez, la sección El Comando de la Semana trajo a SQLMAP, una herramienta de prueba de penetración de código abierto que automatiza el proceso de detección y explotación de fallas de inyección SQL y la toma de control de los servidores de bases de datos.

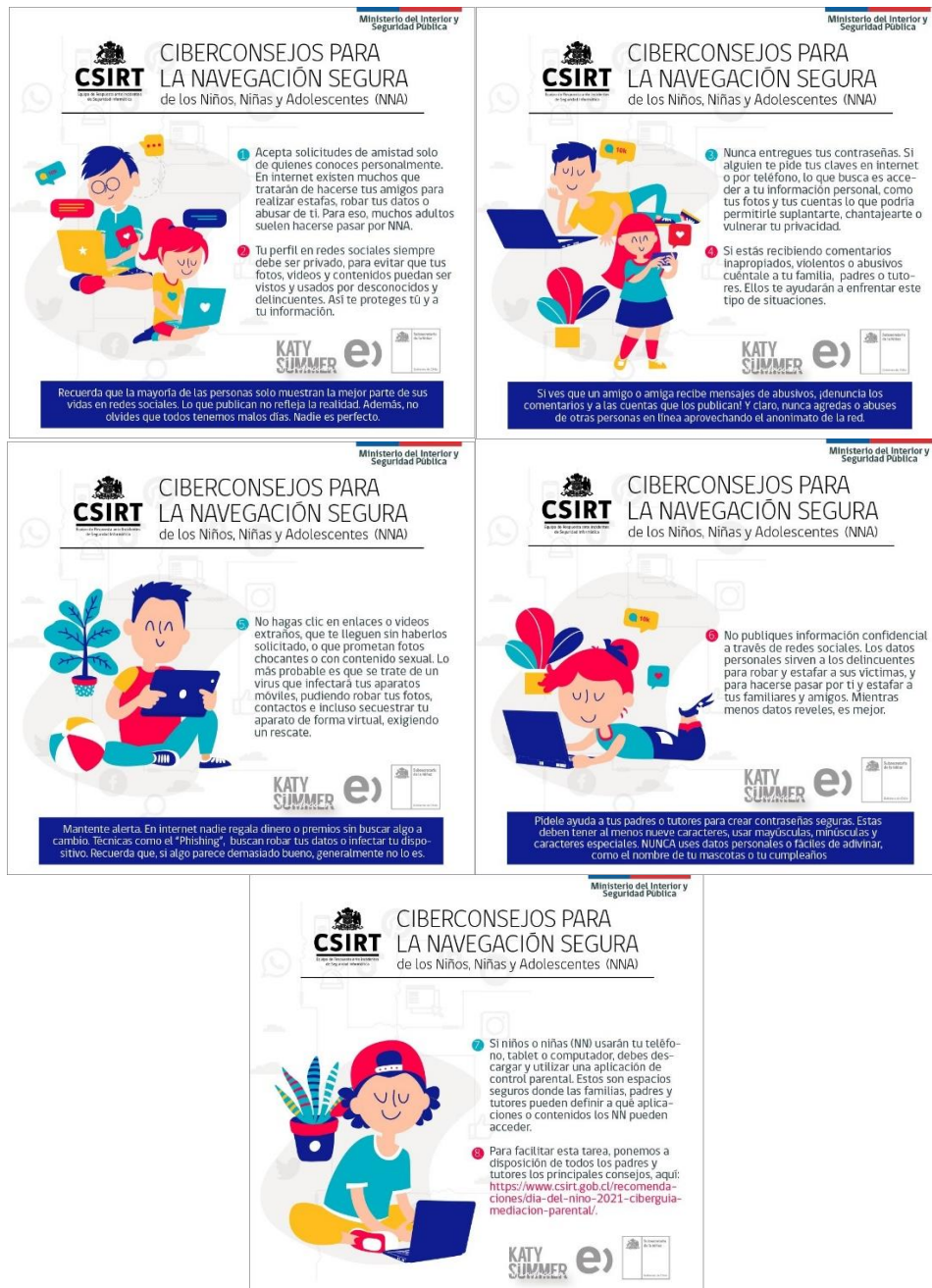
El objetivo de estos comandos que compartimos semanalmente no es reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por el CSIRT de Gobierno.

Encuentra el comando de esta semana aquí: <https://csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-11/>.



Ciberconsejos | Navegación Segura para Niños, Niñas y Adolescentes

Por el Día del Niño, recopilamos con la Subsecretaría de la Niñez, Fundación Katy Summer y Entel consejos clave para tener niños más ciberseguros: csirt.gob.cl/recomendaciones/ciberconsejos-navegacion-segura-para-ninos-ninas-y-adolescentes/.



CIBERCONSEJOS PARA LA NAVEGACIÓN SEGURA de los Niños, Niñas y Adolescentes (NNA)

1. Acepta solicitudes de amistad solo de quienes conoces personalmente. En internet existen muchos que tratarán de hacerse tus amigos para realizar estafas, robar tus datos o abusar de ti. Para eso, muchos adultos suelen hacerse pasar por NNA.
2. Tu perfil en redes sociales siempre debe ser privado, para evitar que tus fotos, videos y contenidos puedan ser vistos y usados por desconocidos y delincuentes. Así te proteges tú y a tu información.

Recuerda que la mayoría de las personas solo muestran la mejor parte de sus vidas en redes sociales. Lo que publican no refleja la realidad. Además, no olvides que todos tenemos malos días. Nadie es perfecto.

CIBERCONSEJOS PARA LA NAVEGACIÓN SEGURA de los Niños, Niñas y Adolescentes (NNA)

1. Nunca entregues tus contraseñas. Si alguien te pide tus claves en internet o por teléfono, lo que busca es acceder a tu información personal, como tus fotos y tus cuentas lo que podría permitirle suplantarte, chantajearte o vulnerar tu privacidad.
2. Si estás recibiendo comentarios inapropiados, violentos o abusivos cuéntale a tu familia, padres o tutores. Ellos te ayudarán a enfrentar este tipo de situaciones.

Si ves que un amigo o amiga recibe mensajes de abusivos, denuncia los comentarios y a las cuentas que los publican! Y claro, nunca agregas o abusos de otras personas en línea aprovechando el anonimato de la red.

CIBERCONSEJOS PARA LA NAVEGACIÓN SEGURA de los Niños, Niñas y Adolescentes (NNA)

1. No hagas clic en enlaces o videos extraños, que te lleguen sin habertlos solicitado, o que prometan fotos chocantes o con contenido sexual. Lo más probable es que se trate de un virus que infectará tus aparatos móviles, pudiendo robar tus fotos, contactos e incluso secuestrar tu aparato de forma virtual, exigiendo un rescate.

Mantente alerta. En internet nadie regala dinero o premios sin buscar algo a cambio. Técnicas como el "Phishing", buscan robar tus datos o infectar tu dispositivo. Recuerda que, si algo parece demasiado bueno, generalmente no lo es.

CIBERCONSEJOS PARA LA NAVEGACIÓN SEGURA de los Niños, Niñas y Adolescentes (NNA)

1. No publiques información confidencial a través de redes sociales. Los datos personales sirven a los delincuentes para robar y estafar a sus víctimas, y para hacerse pasar por ti y estafar a tus familiares y amigos. Mientras menos datos reveles, es mejor.

Pídele ayuda a tus padres o tutores para crear contraseñas seguras. Estas deben tener al menos nueve caracteres, usar mayúsculas, minúsculas y caracteres especiales. NUNCA uses datos personales o fáciles de adivinar, como el nombre de tu mascotas o tu cumpleaños.

CIBERCONSEJOS PARA LA NAVEGACIÓN SEGURA de los Niños, Niñas y Adolescentes (NNA)

1. Si niños o niñas (NN) usarán tu teléfono, tablet o computador, debes descargar y utilizar una aplicación de control parental. Estos son espacios seguros donde las familias, padres y tutores pueden definir a qué aplicaciones o contenidos los NN pueden acceder.
2. Para facilitar esta tarea, ponemos a disposición de todos los padres y tutores los principales consejos aquí: <https://www.csirt.gob.cl/recomendaciones/dia-del-nino-2021-ciberguia-mediacion-parental/>.

Recomendaciones y buenas prácticas

Recomendaciones generales de seguridad

- 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.

- María Macarena Susana Puyol Wilson.
- Felipe Osvaldo Garrido Sanhueza.
- Miguel Andrés Zelaya Méndez.
- Gonzalo Atabales Coliqueo.
- Pedro Enrique Díaz Castillo.
- Camila González Piucol.
- Valentina Andrade.
- Christian Abarca.
- Andrés Aldana F.
- Nacho Parra.
- Luis Álvarez.
- Hanz.

