



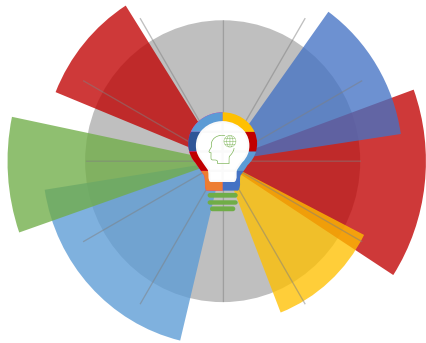
25-02-2022 | Año 4 | N°138

Boletín de Seguridad Cibernética

Semana del 18 al 24 de
febrero de 2021



La semana en cifras



Parches

1

para vulnerabilidades

Las mitigaciones son útiles en productos de Adobe.

Se advirtieron

4

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

IP

4

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Phishing	2
Vulnerabilidades	5
Actualidad.....	6
Muro de la Fama	9

Phishing



CSIRT alerta campaña de phishing que suplanta al Banco Itaú

Alerta de seguridad cibernética	8FPH22-00476-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de febrero de 2022
Última revisión	22 de febrero de 2022
Indicadores de compromiso	
URL sitio falso	https://itauapp.canjea-empresas-y-personas[.]com/726a292db52f7f5/html/index.php
IP	[104.21.11.32]
Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/8fph22-00476-01/
	https://www.csirt.gob.cl/media/2022/02/8FPH22-00476-01.pdf

Sitios fraudulentos

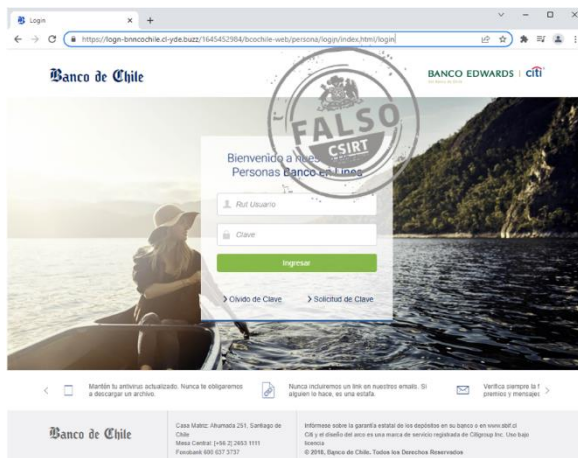


CSIRT alerta de nueva página fraudulenta que suplanta al BancoEstado

Alerta de seguridad cibernética	8FFR22-01054-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de febrero de 2022
Última revisión	21 de febrero de 2022

Indicadores de compromiso

URL sitio falso	https://wwwbancoestado-cl.judithmartens.[.]nl/
IP	[185.69.233.105]
Enlaces para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr21-01054-01/ https://www.csirt.gob.cl/media/2022/02/8FFR22-01054-01.pdf



CSIRT alerta de nueva página fraudulenta que suplanta al Banco de Chile

Alerta de seguridad cibernética	8FFR22-01055-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de febrero de 2022
Última revisión	8 de febrero de 2022

Indicadores de compromiso

URL sitio falso	https://logn-bnncochile.cl-yde[.]buzz/
IP	[172.67.205.202]
Enlaces para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr22-01055-01/ https://www.csirt.gob.cl/media/2022/02/8FFR22-01055-01.pdf



CSIRT alerta ante nueva página fraudulenta que suplanta al BancoEstado

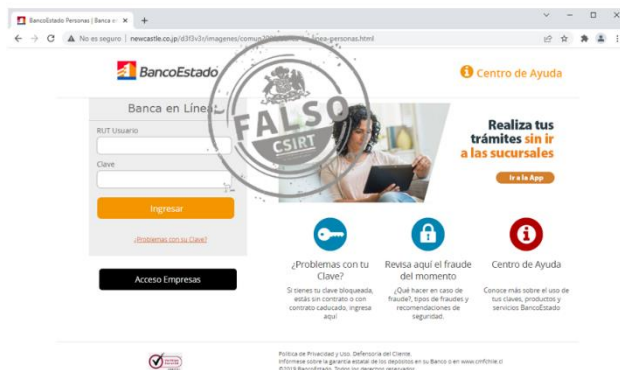
Alerta de seguridad cibernética	8FFR22-01056-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de febrero de 2022
Última revisión	21 de febrero de 2022

Indicadores de compromiso

URL sitio falso	https://bancoestado-personas-webb[.]ga/logica-negocios?23r6f5tcgim7aql63mja
IP	[111.90.143.245]

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/8ffr22-01056-01/
https://www.csirt.gob.cl/media/2022/02/8FFR22-01056-01.pdf



CSIRT alerta sobre nuevo sitio web fraudulento que suplanta al BancoEstado

Alerta de seguridad cibernética	8FFR22-01057-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de febrero de 2022
Última revisión	21 de febrero de 2022

Indicadores de compromiso

URL sitio falso	http://newcastle.co[.]jp/d3f3v3r/imagenes/comun2008/banca-en-linea-personas.html
IP	[1.33.169.198]

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/8ffr22-01057-01/
https://www.csirt.gob.cl/media/2022/02/8FFR22-01057-01.pdf

Vulnerabilidades



CSIRT alerta de una nueva vulnerabilidad crítica en Adobe Commerce y Magento

Alerta de seguridad cibernética	9VSA22-00580-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de febrero de 2022
Última revisión	21 de febrero de 2022

CVE

CVE-2022-24087

Fabricante

Adobe

Productos afectados

Adobe Commerce 2.4.3-p1 y versiones anteriores, 2.3.7-p2 y versiones anteriores.
Magento Open Source 2.4.3-p1 y versiones anteriores, 2.3.7-p2 y versiones anteriores.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00580-01/>

<https://www.csirt.gob.cl/media/2022/02/9VSA22-00580-01-1.pdf>

Actualidad

Ciberconsejos para lograr comunidades educativas más seguras

Vuelven las clases y con ello la importancia de mantener seguras nuestras comunidades educativa, una responsabilidad de todos, alumnos, apoderados y las escuelas. Por eso les dejamos con recomendaciones clave en los Ciberconsejos de esta semana. Los pueden descargar y compartir en PDF: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-comunidades-educativas/>.



Ministerio del Interior y Seguridad Pública

CIBERCONSEJOS para comunidades educativas más seguras

Escuelas y universidades son atractivas para delincuentes

- Acceso no autorizado a plataformas escolares:** Delincuentes pueden robar identidades, realizar declaraciones de impuestos falsas, generar pagos a terceros, alterar el registro de los alumnos y secuestrar sitios web o cuentas de redes sociales, entre otros riesgos.
- Phishing y ransomware:** Con listas de correos de alumnos o funcionarios pueden enviar emails, SMS o WhatsApp haciéndose pasar por el colegio y robar datos personales o convencer a sus víctimas de descargar programas maliciosos, como los que posibilitan el ransomware (cifrado de su PC para exigir un rescate).

Ministerio del Interior y Seguridad Pública

CIBERCONSEJOS para comunidades educativas más seguras

Ciberconsejos para profesores e instituciones

- No exponer** información de los alumnos y apoderados en el sitio web, como fotos, horarios y matrículas. Si necesita subir estos datos, resguárdelos con usuario y contraseña, dando acceso solo a quienes lo necesitan.
- Fomentar** la creación de contraseñas fuertes por profesores y alumnos, y la activación de doble factor de autenticación en dispositivos y apps.

[csirt.gob.cl/recomendaciones/ciberconsejos-para-crear-contrasenas-seguras/](https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-crear-contrasenas-seguras/)

Ministerio del Interior y Seguridad Pública

CIBERCONSEJOS para comunidades educativas más seguras

Ciberconsejos para instituciones educacionales

- **Elaborar** una estrategia de ciberseguridad y planes de defensa y prevención.
- **Crear** un protocolo de respuesta ante incidentes, para que los usuarios sepan qué hacer frente a un ciberataque.
- **Monitorear** regularmente redes y datos para identificar actividades maliciosas
- **Implementar** controles de protección como firewall, sistemas de prevención de intrusos, filtrado de URL, seguridad en emails y filtros de privacidad.

Ministerio del Interior y Seguridad Pública

CIBERCONSEJOS para comunidades educativas más seguras

Ciberconsejos para profesores e instituciones

- **Usar** sistemas de protección en capas para el bloqueo de amenazas y niveles de privilegio para los usuarios.
- **Considerar** la ciberseguridad de sistemas como escritorios remotos (RDP) y redes privadas virtuales (VPN).
- **Procurar** plataformas de educación a distancia seguras en cuanto a confidencialidad, integridad y disponibilidad de los datos procesados, almacenados y transmitidos.

Ministerio del Interior y Seguridad Pública



CIBERCONSEJOS para comunidades educativas más seguras



Ciberconsejos para instituciones educativas

- **Los profesores** deben usar computadores de la institución y de usar un equipo personal, se debe verificar que cumpla requisitos de seguridad.
- **Crear copias de seguridad** periódicas, con mínima conectividad con otros sistemas e internet. Realizar regularmente pruebas de recuperación.
- **Capacitar** a toda la comunidad sobre ciberseguridad y reforzar las medidas de precaución.

Ministerio del Interior y Seguridad Pública



CIBERCONSEJOS para comunidades educativas más seguras



Ciberconsejos para toda la comunidad

1. **Ingresar** a las plataformas educativas desde sitios seguros y evitar wifi públicas.
2. **Cerrar** la sesión de la plataforma cada vez que se deje de utilizar.
3. **Usar software original**. Actualizar software regularmente y especialmente cuando se descubren nuevas vulnerabilidades
4. **Contar** con antivirus y antispam actualizados y de proveedores con buena reputación.

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 (csirt.gob.cl o al 1510) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Bárbara Palacios
- Kevin Anguita
- Christian Campodónico
- Carlos Humberto de la Fuente Castro

