CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 239

semana del 26 de enero al 1 de febrero de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

3

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

8

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

16

Las mitigaciones son útiles en productos de Ivanti, Jenkins, WatchGuard y Cisco.

HASH REPORTADOS

12

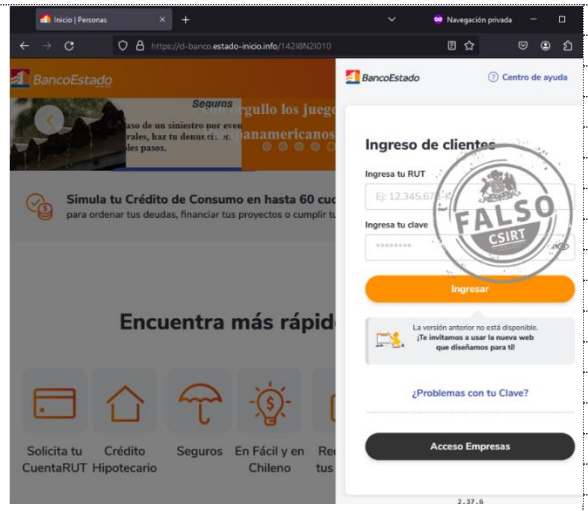
Hashes asociados a múltiples campañas de phishing con archivos que contienen malware.

CONTENIDO

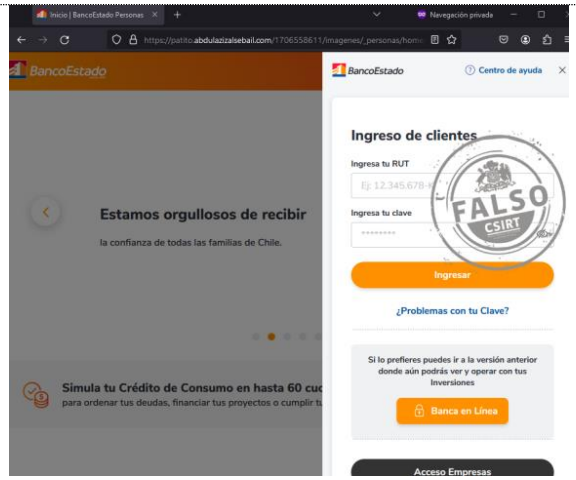
1|||||<

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

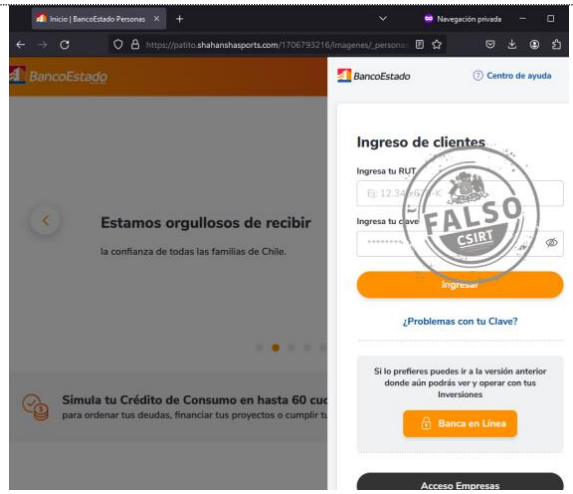


CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR24-01638-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 enero, 2024
Última revisión	29 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://cl-banco.estado-inicio[.]info	
URL de redirección	
N/A	
Dirección IP sitio falso	
[172.67.146.38]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01638-01/	



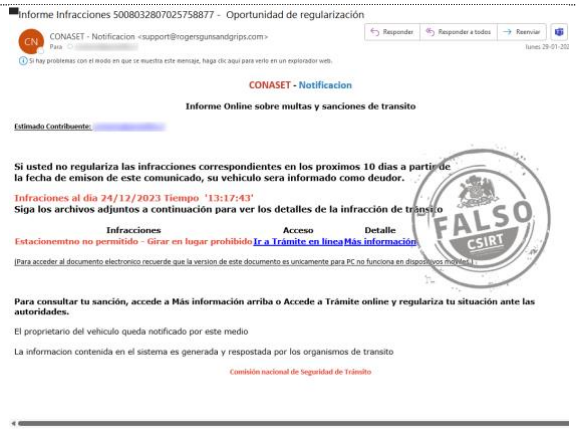
CSIRT alerta de nueva página web fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01639-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 enero, 2024
Última revisión	29 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://patito.abdulazizalsebail[.]com/1706558611/imagenes/_personas/home/default.asp	
URL de redirección	
N/A	
Dirección IP sitio falso	
[83.149.93.194]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr23-01639-01/	

2. Phishing



CSIRT alerta de nueva campaña de phishing en emails que suplantan al BancoEstado	
Alerta de seguridad cibernética	8FPH24-00925-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 febrero, 2024
Última revisión	1 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://patito.shahanshasports[.]com/1706793216/imagenes/_personas/home/default.asp	
URL de redirección	
https://maximocontaval[.]com/activacion/cuenta-kaoi/	
Dirección IP sitio falso	
[162.0.220.139]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00925-01/	

3. Malware



CSIRT alerta de nueva campaña de phishing con malware, que suplanta al Conaset	
Alerta de seguridad cibernética	2CMV24-00441-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 enero, 2024
Última revisión	30 enero, 2024
Indicadores de compromiso	
URL-Dominio	
https://windbender[.]com/conasetinfraccione/?hash={correo} https://plataformaepimexicoenganchate[.]org/111xxx/conasetnotificacioninfra.zip	
SHA256	
c1e0f5185a2efc13b4e821ee1a2d445634e87fb380306315c482c05ae26fbd55 17a6f57be6897d2a7456ad9b0f5bc798b951c6c41b2511886706edee16c5c14c 36a9e7f1c95b82ffb99743e0c5c4ce95d83c9a430aac59f84ef3cbfab6145068 52f41817669af7ac55b1516894ee705245c3148f2997fa0e6617e9cc6353e41e b55333f085db8ef18ca3ba73a7b3984b3917d95c4f3fa57f939ebfe89c82a03c 0831dbcb3799c9e36ea586582e8ef907dcefeb2045351d6774c7ad0ef02a9af2	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/2cmv24-00441-01/	

CSIRT alerta de nueva campaña de phishing con malware, difundido en falsa factura por vencer	
Alerta de seguridad cibernética	2CMV24-00442-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 enero, 2024
Última revisión	30 enero, 2024
Indicadores de compromiso	
URL-Dominio	
https://windbender[.]com/conasetinfraccione/?hash={correo} https://plataformaepimexicoenganchate[.]org/111xxx/conasetnotificacioninfra.zip	
SHA256	
c98da79639217f83596fe9959fcc15d907255e098b972dc00535858710204cd8 ac2e3c0663c9ce6f5791afbddbb0614d8417efd230b08a0d68f84b923999c0e7 d955856d80c8127ccd38b7a04be1b48984078e9e6416e3c1846b772956dda003 52f41817669af7ac55b1516894ee705245c3148f2997fa0e6617e9cc6353e41e 0831dbcb3799c9e36ea586582e8ef907dcefeb2045351d6774c7ad0ef02a9af2	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/2cmv24-00442-01/	

4. Vulnerabilidades

CSIRT alerta de nueva vulnerabilidad crítica en Jenkins	
Alerta de seguridad cibernética	9VSA24-00967-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 enero, 2024
Última revisión	30 enero, 2024

CVE

CVE-2024-23897	CVE-2024-23902	CVE-2024-23905
CVE-2024-23899	CVE-2024-23903	CVE-2023-6148
CVE-2024-23900	CVE-2024-23904	CVE-2023-6147
CVE-2024-23901		

Fabricante

Jenkins

Productos afectados

Jenkins weekly 2.441 y anteriores.
LTS 2.426.2 y anteriores.
Git server Plugin hasta e incluyendo 99.va_0826a_b_cdfa_d
GitLab Branch Source Plugin hasta e incluyendo 684.vea_fa_7c1e2fe3
Log Command Plugin hasta e incluyendo 1.0.2
Matrix Project Plugin hasta e incluyendo 822.v01b_8c85d16d2
Qualys Policy Compliance Scanning Connector Plugin hasta e incluyendo 1.0.5
Red Hat Dependency Analytics Plugin hasta e incluyendo 0.7.1

Enlaces para revisar el informe:

https://csirt.gob.cl/vulnerabilidades/9vsa24-00967-01/

CSIRT comparte información de vulnerabilidad crítica en Ivanti Connect Secure (ICS) VPN	
Alerta de seguridad cibernética	9VSA24-00968-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 enero, 2024
Última revisión	30 enero, 2024

CVE

CVE-2023-46805
CVE-2024-21887

Fabricante

Ivanti

Productos afectados

Ivanti Connect Secure (ICS) 9.x, 22.x
Ivanti Policy Secure

Enlaces para revisar el informe:

https://csirt.gob.cl/vulnerabilidades/9vsa24-00968-01/

CSIRT alerta de vulnerabilidades que afectan a productos de WatchGuard y Panda Security	
Alerta de seguridad cibernética	9VSA24-00969-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 enero, 2024
Última revisión	30 enero, 2024
CVE	
CVE-2023-6330 CVE-2023-6331 CVE-2023-6332	
Fabricante	
WatchGuard	
Productos afectados	
Actualizar Panda Dome a la versión 22.02.01. Actualizar WatchGuard EPDR y AD360 a 8.0.22.0023.	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa24-00969-01/	

CSIRT alerta de nueva vulnerabilidad crítica que afecta a Cisco Unified Communications y Cisco Contact Center Solutions	
Alerta de seguridad cibernética	9VSA24-00970-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 enero, 2024
Última revisión	30 enero, 2024
CVE	
CVE-2024-20253	
Fabricante	
Cisco	
Productos afectados	
Unified Communications Manager (Unified CM) (CSCwd64245) Unified Communications Manager IM & Presence Service (Unified CM IM&P) (CSCwd64276) Unified Communications Manager Session Management Edition (Unified CM SME) (CSCwd64245) Unified Contact Center Express (UCCX) (CSCwe18773) Unity Connection (CSCwd64292) Virtualized Voice Browser (VVB) (CSCwe18840)	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa24-00970-01/	

5. Noticias y concientización

CSIRT comparte las principales amenazas online para los adultos mayores en El Mercurio

Esta semana en el suplemento Mundo Mayor de El Mercurio, el CSIRT del Ministerio del Interior participó de la nota «Estas son las estafas online más comunes que afectan a las personas mayores». Compartimos aquí la participación del jefe del CSIRT, Cristian Bravo Lillo. Para ver la nota completa pueden dirigirse al suplemento Mundo Mayor, página 4, o en internet: https://digital.elmercurio.com/2024/01/29/EE-TAB-J/9D4CAVUC#zoom=page-width.

Muchas gracias a la periodista Constanza Menares por la invitación a participar de este reportaje.

«La mayoría de ellos no ha tenido exposición suficiente a internet como para entender los flujos de información, y la mayor parte de los cursos se concentran en tareas mecánicas, como aprender a usar el computador, ocupar planillas o navegar online, sin contar con nociones básicas de cómo funciona internet", explica Cristian Bravo Lillo, jefe del CSIRT de Gobierno.

Y añade: «Por ello es necesario enseñar a los adultos mayores esas nociones clave, para que entiendan qué ocurre cuando navegan online y sepan cómo protegerse». En esta línea, el jefe del CSIRT aclara que las estafas virtuales más comunes en las que cae este segmento etario son las mismas en las que cae la población en general, solo que «agudizadas por los cambios propios de la edad avanzada».

Una de ellas es el phishing, tipo de engaño en que los delincuentes hacen pasar enlaces, sitios o programas maliciosos como si fueran los verdaderos, con la intención de robar información o infectar los dispositivos con virus. «La falta de conocimiento y peor agudeza visual podría hacer más difícil distinguir las URL, que son las direcciones de las páginas web», supone Bravo.

Si bien no hay una forma infalible de chequear las URL, la recomendación del especialista es fijarse en que las direcciones estén bien escritas, que no haya palabras con faltas de ortografía o letras de más o menos, ya que es algo que los delincuentes utilizan mucho para disfrazar sitios maliciosos».

Estar informado sobre los nuevos timos cibernéticos es una forma de prevenirlos.

Ciberseguridad:

Estas son las estafas *online* más comunes que afectan a las personas mayores

El "cuento del tío" usando inteligencia artificial para imitar la voz de los familiares o fraudes románticos aprovechando la soledad de algunos séniors son parte de los delitos frecuentes. Expertos dan recomendaciones para evitarlos.

Constanza Menares

Quienes hoy tienen más de 60 años de edad nacieron antes de 1964. "Internet llegó comercialmente a Chile a mediados de los 90, por lo que los séniors actuales llevaban ya varios años trabajando cuando internet hizo su debut en el país", asegura Cristian Bravo, jefe del CSIRT de Gobierno, que es el Equipo de Respuesta a Incidentes de Seguridad dependiente del Ministerio del Interior.

Con este dato, el experto busca ilustrar por qué las personas mayores pueden ser más propensas a caer en estafas virtuales.

"La mayoría de ellos no ha tenido exposición suficiente a internet como para entender los flujos de información, y la mayor parte de los cursos se concentran en tareas mecánicas, como aprender a usar el computador, ocupar planillas o navegar *online*, sin contar con nociones básicas de cómo funciona internet", precisa Bravo.

Y añade: "Por ello es necesario enseñar a los adultos mayores esas nociones clave, para que entiendan qué ocurre cuando navegan *online* y sepan cómo protegerse".

En esta línea, el jefe del CSIRT aclara que las estafas virtuales más comunes en las que cae este segmento etario son las mismas en las que cae la población en general, solo que "agudizadas por los cambios propios de la edad avanzada".

Una de ellas es el *phishing*, tipo de engaño en que los delincuentes hacen pasar enlaces, sitios o programas maliciosos como si fueran los verdaderos, con la intención de robar información o infectar los dispositivos con virus.

"La falta de conocimiento y peor agudeza visual podría hacer más difícil distinguir las URL, que son las direcciones de las páginas de web", supone Bravo.

Si bien no hay una forma infalible de chequear las URL, la recomendación del especialista es fijarse que las direcciones estén bien escritas, que no haya palabras con faltas de ortografía o letras de más o menos, ya que es algo que los delincuentes utilizan mucho para disfrazar sus sitios maliciosos.

Julio Vargas, subcomisario de la Brigada Investigadora del Cibercrimen de la PDI, añade que el "cuento del tío virtual" es otra estafa muy común entre la gente mayor de 60 años.

"Son estafas en que los delincuentes se hacen pasar por familiares cercanos, generalmente hijos o nietos, y les piden dinero urgentemente por algún motivo falso, como un accidente, un arresto o un viaje. Estas estafas se realizan por teléfono, pero también por correo electrónico, mensaje de texto o en redes sociales. A veces, incluso usan la inteligencia artificial para imitar la voz de los familiares".

El subcomisario cuenta que otro fraude común en el país es el de tipo romántico.

"Los delincuentes, aprovechando la situación de soledad de algunos adultos mayores, se hacen pasar por interesados en tener una relación sentimental con sus víctimas, a través de sitios y aplicaciones de citas, o por redes sociales. El objetivo de los estafadores es ganarse la confianza y el afecto de sus víctimas, para luego pedirles dinero o información personal que les permita robar su identidad", puntualiza.

Otro método común, suma Vargas, "es la falsa encomienda internacional, que consiste en hacer creer a los séniors que recibirán un paquete con regalos, enviado por un familiar o amigo que vive en el extranjero. Tras estudiar el perfil de una persona que vive en otro país, los estafadores lo copian y se comunican con las víctimas por redes sociales o correo y les piden sus datos para el envío. Después, les informan que la encomienda fue retenida por las autoridades aduaneras y que deben pagar una multa o impuesto para liberarla".

En este caso, los antisociales usan documentos falsos y la imagen de empresas de transporte o de aduana para convencer a sus víctimas y les piden que hagan la transferencia por medios difíciles de rastrear o recuperar.

Obviamente, apenas reciben el dinero, los estafadores desaparecen y las personas mayores notan que nunca existió tal encomienda.

Ciberhigiene

"La frecuencia y el nivel de sofisticación de los ataques cibernéticos ha aumentado exponencialmente. Estos afectan a todos los usuarios de canales digitales, pero dentro de los segmentos que se encuentran expuestos, las personas mayores son un objetivo común", afirma Rocío Ortiz, jefa de Industrias del Futuro del Centro de Innovación de la U. Católica.

La entidad lanzó en diciembre de 2022 una "hoja de ruta de ciberseguridad" junto a Microsoft, en la que se propone una serie de proyectos concretos ejecutables en un plazo de tres años. El trabajo puede verse o descargarse en el *link* http://rb.gy/aeewoz.

¿Cómo pueden los séniors (y el resto de la población) evitar caer en este tipo de timos? Según la experta, lo más importante para "enfrentar estos riesgos es el desarrollo de la ciberhigiene. Es decir, la adopción de conductas responsables y efectivas de prevención".

En esa línea, "la recomendación principal es una conducta de confianza cero. Hay múltiples formas de robar datos: vía enlaces maliciosos en correos, páginas web falsas, mensajes de texto fraudulentos, mensajes de WhatsApp, videollamadas e incluso códigos QR alterados. No acceder a estos *links* ni compartir información con fuentes sospechosas, desconfiar y siempre verificar la fuente antes, asegurándose de que sean sitios oficiales y seguros. Fijarse en el nombre de las páginas, usualmente la dirección o URL es la forma de notar si es fraudulento".

Asimismo, aconseja Ortiz, "verificar las configuraciones de los equipos, porque muchas veces tienen activada la descarga automática (de aplicaciones) que puede ser muy peligrosa. En WhatsApp, en Configuración se puede desactivar la opción. En teléfonos Android, en Seguridad y Privacidad está la opción de 'Instalar aplicaciones desconocidas', la que debe estar desactivada. Por último, hay que mantenerse informados siempre. Estar atentos a las nuevas formas de estafas cibernéticas que se informan en medios oficiales y ojalá capacitarse constantemente en el uso de las nuevas tecnologías. La educación y concientización son claves para la prevención y evitar incidentes digitales".

Ciberconsejos | ¿Cómo proteger tus datos?

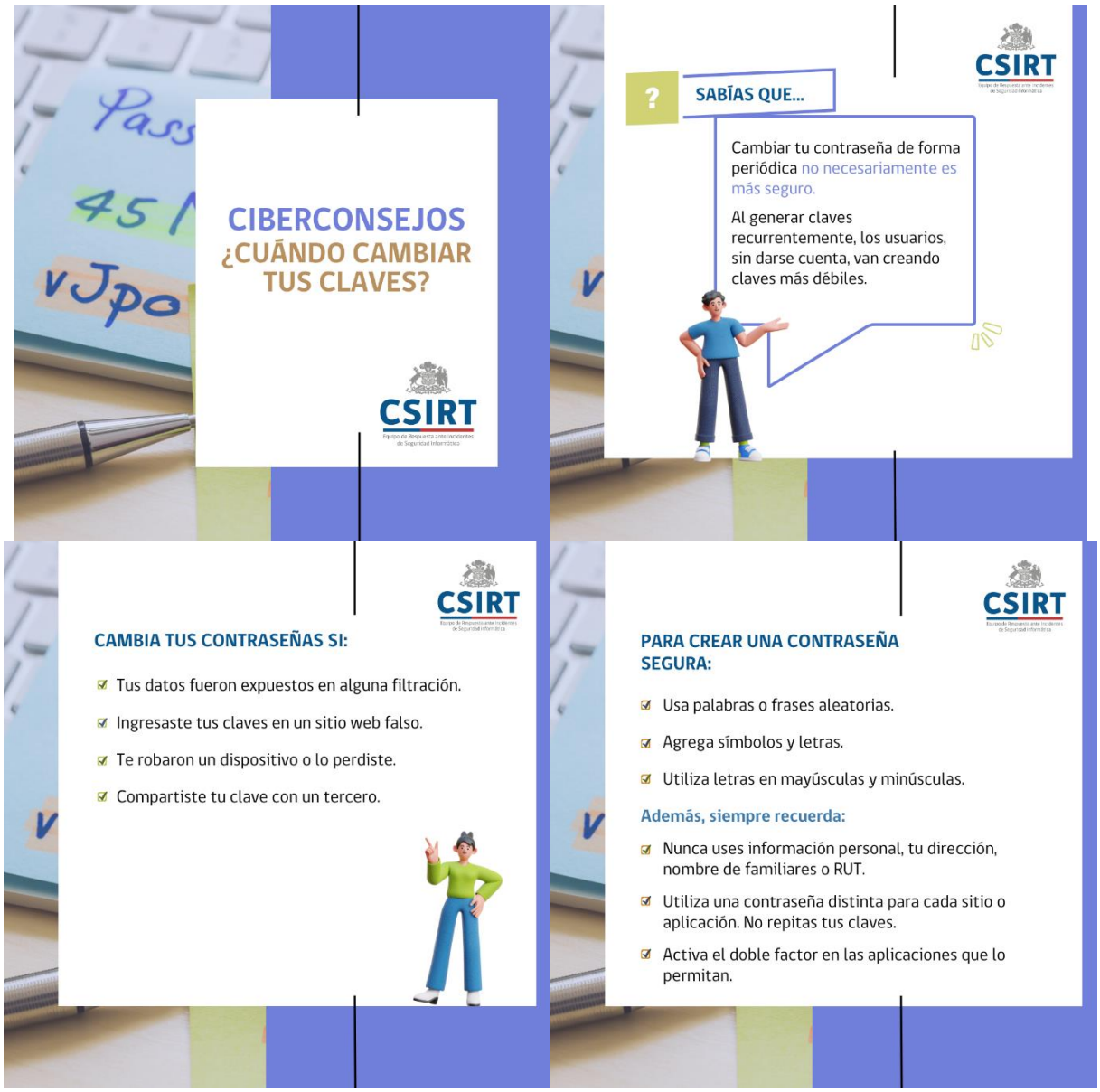
El 28 de enero se conmemora el Día Internacional de la Protección de Datos Personales, con el objetivo de crear conciencia sobre la importancia de la privacidad y la protección de los datos personales en línea. Por eso, este día queremos entregarte algunos consejos sobre cómo cuidar tu información. Revísalos aquí: https://csirt.gob.cl/recomendaciones/ciberconsejos-como-proteger-tus-datos/.

Recueden que siempre los pueden compartir con sus compañeros y trabajadores.

Ciberconsejos | ¿Cuándo cambiar tus contraseñas?

Cambiar contraseñas regularmente no es siempre más seguro. Por eso en el CSIRT de Gobierno te recomendamos renovar tus claves solo si se cumplen las siguientes situaciones, que explican los ciberconsejos de esta semana. Además, te compartimos un sitio donde chequear la fortaleza de tus contraseñas.

Estos tips también los puedes obtener en formato PDF: https://csirt.gob.cl/recomendaciones/ciberconsejos-cambio-contrasenas/



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 que los sitios web a los que se ingrese sean los oficiales.

6. 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 campañas de phishing, malware y/o sitios fraudulentos.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono 1510), siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Francisco Jiménez Alcántara
- Hernán Francisco Diaz Farías
- Luis Rojas
- David Soto
- Alonso Ignacio Villalobos González
- Jair Palma
- Valentina Céspedes Gutiérrez

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.02.05 10:07:29 -03'00'