



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 200

semana del 28 de abril al 4 de mayo de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

7

IP advertidas en múltiples campañas de phishing y de malware.



URL ADVERTIDAS

13

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

12

Las mitigaciones son útiles en productos de Apache, TP-Link, Cisco, Apple y Zyxel.

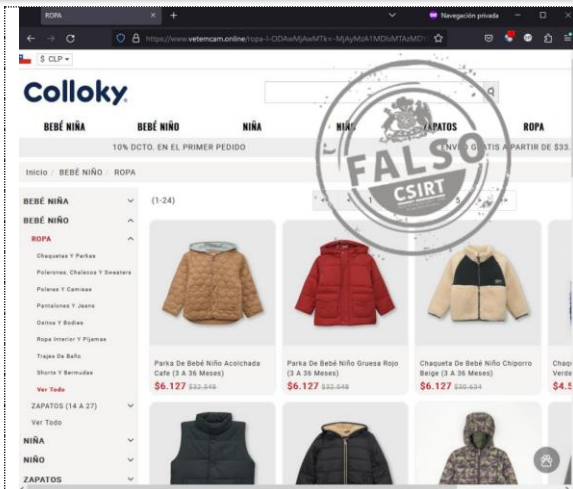


CONTENIDO

1.	Sitios fraudulentos	3
2.	Phishing	4
3.	Vulnerabilidades	6
4.	Concientización	9
5.	Recomendaciones y buenas prácticas	14
6.	Muro de la Fama	15

11111<

1. Sitios fraudulentos



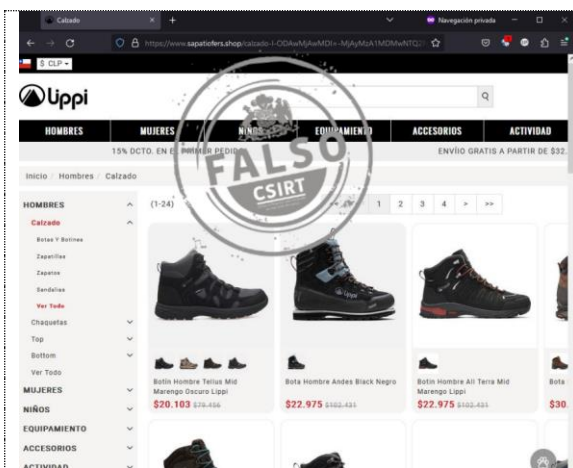
CSIRT alerta de página fraudulenta que suplanta a Colloky

Alerta de seguridad cibernética	8FFR23-01305-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2023
Última revisión	2 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	https://www.vetemcam[.]online/
Dirección IP	[167.160.3.13]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01305-01



CSIRT alerta de sitio fraudulento que suplanta a Banco Falabella

Alerta de seguridad cibernética	8FFR23-01306-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2023
Última revisión	2 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	https://falabella.cl-informaf[.]com/home
Dirección IP	[172.67.146.85]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01306-01



CSIRT alerta de página fraudulenta que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01307-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de mayo de 2023
Última revisión	3 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	https://www.sapatiofers[.]shop/
Dirección IP	[167.160.3.20]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01307-01

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

2. Phishing

	<p>CSIRT alerta ante campaña de smishing que suplanta a Banco Santander</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00801-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Phishing</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>26 de abril de 2023</td> </tr> <tr> <td>Última revisión</td> <td>26 de abril de 2023</td> </tr> </table> <p>URL redirección https://bit.ly/3HgiyYp?l=www.officebanking.cl http://wordpress.zuliatec.com/.jve/activacion/cuenta-ufbq/</p> <p>URL sitio falso https://officebanking.sitio-cl[.]buzz/1682515743/default.htm</p> <p>Dirección IP [172.67.212.81]</p> <p>Enlace para revisar loC: https://www.csirt.gob.cl/alertas/8fph23-00801-01/</p>	Alerta de seguridad cibernética	8FPH23-00801-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	26 de abril de 2023	Última revisión	26 de abril de 2023
Alerta de seguridad cibernética	8FPH23-00801-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	26 de abril de 2023														
Última revisión	26 de abril de 2023														

	<p>CSIRT alerta campaña de phishing que suplanta a Banco Ripley</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00802-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Phishing</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>28 de abril de 2023</td> </tr> <tr> <td>Última revisión</td> <td>28 de abril de 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL sitio falso https://sam-tech[.]jp/ripley/activacion-ooph/</p> <p>URL redirección: https://web-bancoripley-cl.web-bancoripley-cl[.]club/1682711530/login/index.html</p> <p>Dirección IP sitio falso [172.67.178.221]</p> <p>Enlace para revisar loC: https://www.csirt.gob.cl/alertas/8fph23-00802-01/</p>	Alerta de seguridad cibernética	8FPH23-00802-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	28 de abril de 2023	Última revisión	28 de abril de 2023
Alerta de seguridad cibernética	8FPH23-00802-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	28 de abril de 2023														
Última revisión	28 de abril de 2023														

Boletín de Seguridad Cibernética N° 200

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

BOLETÍN 13BCS23-00209-01 | Semana del 28 de abril al 4 de mayo de 2023

	CSIRT alerta ante nueva campaña de phishing que suplanta a BancoEstado	
	Alerta de seguridad cibernética	8FPH23-00803-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	28 de abril de 2023
	Última revisión	28 de abril de 2023
	Indicadores de compromiso	
	URL sitio falso	
https://reachercontact[.]com/activacion/cuenta-bqdc/		
URL redirección:		
https://contachincher[.]com/1682712333/imagenes/_personas/home/default.asp		
Dirección IP sitio falso		
[138.128.170.234]		
Enlace para revisar loC:		
https://www.csirt.gob.cl/alertas/8fph23-00803-01/		

	CSIRT alerta ante nueva campaña de phishing que suplanta al Banco Ripley	
	Alerta de seguridad cibernética	8FPH23-00804-01
	Clase de alerta	Fraude
	Tipo de incidente	Phishing
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	4 de mayo de 2023
	Última revisión	4 de mayo de 2023
	Indicadores de compromiso	
	URL redirección:	
https://bit[.]ly/3ANY9pZ?l=www.bancoripley.cl		
URL sitio falso:		
https://conciERGE.casasre[.]com/seguros/bancoripley-twub/ https://web.bancoripley.cl.chromedental[.]com.au/1683146472/login		
Dirección IP sitio falso		
[122.201.64.137]		
Enlace para revisar loC:		
https://www.csirt.gob.cl/alertas/8fph23-00804-01/		

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

3. Vulnerabilidades



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00824-01
CSIRT comparte vulnerabilidad parchada para TP-Link Archer AX-2

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl



CSIRT comparte vulnerabilidad parchada por TP-Link para Archer AX-2	
Alerta de seguridad cibernética	9VSA23-00824-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de mayo de 2023
Última revisión	2 de mayo de 2023
CVE	
CVE-2023-1389	
Fabricantes	
TP-Link	
Productos afectados	
TP-Link Archer AX-1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00824-01/	



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00825-01
CSIRT comparte vulnerabilidad parchada para Apache Superset

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl



CSIRT comparte información de vulnerabilidades parchadas en Apache Superset	
Alerta de seguridad cibernética	9VSA23-00825-01
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 2023
Última revisión	3 de mayo de 2023
CVE	
CVE-2023-27524	
Fabricantes	
Apache	
Productos afectados	
Apache Superset, versión 2.0.1 y anteriores	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00825-01/	

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>

Boletín de Seguridad Cibernética N° 200

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

BOLETÍN 13BCS23-00209-01 | Semana del 28 de abril al 4 de mayo de 2023



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00826-01
CSIRT comparte vulnerabilidad parchada para audifonos Apple AirPods y Beats

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl



CSIRT comparte información de vulnerabilidad parchada por Apple para AirPods y Beats

Alerta de seguridad cibernética	9VSA23-00826-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2023
Última revisión	4 de mayo de 2023

CVE

CVE-2023-27964

Fabricantes

Apple

Productos afectados

AirPods (5E133) incluyendo modelos Pro y Max, Beats (5B66) incluyendo Powerbeats Pro y Beats Fit Pro.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00826-01/>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00827-01
CSIRT comparte vulnerabilidades parchadas en productos Zyxel

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl



CSIRT comparte información de vulnerabilidades parchadas por Zyxel

Alerta de seguridad cibernética	9VSA23-00827-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2023
Última revisión	4 de mayo de 2023

CVE

CVE-2023-28771
CVE-2023-27991
CVE-2023-22913
CVE-2023-22914
CVE-2023-22915
CVE-2023-22916
CVE-2023-22917
CVE-2023-22918

Fabricantes

Zyxel

Productos afectados

ATP (versiones ZLD V4.60 a V5.35, parchada en ZLD V5.36)
USG FLEX (versiones ZLD V4.60 a V5.35, parchada en ZLD V5.36)
VPN (versiones ZLD V4.60 a V5.35, parchada en ZLD V5.36), and
ZyWALL/USG (versiones ZLD V4.60 a V4.73, parchada en ZLD V4.73 Patch 1)

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00827-01/>

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
[@csirtgob](https://twitter.com/csirtgob)
<https://www.linkedin.com/company/csirt-gob>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00828-01
CSIRT comparte vulnerabilidad que afecta adaptadores telefónicos Cisco

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl



CSIRT comparte vulnerabilidad que afecta adaptadores telefónicos Cisco SPA112 2-Port

Alerta de seguridad cibernética	9VSA23-00828-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	4 de mayo de 2023
Última revisión	4 de mayo de 2023

CVE

CVE-2023-20126

Fabricantes

Cisco





Productos afectados

Adaptadores telefónicos Cisco SPA112 2-Port

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00828-01/>

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

4. Concientización

El CSIRT de Gobierno y Microsoft capacitan a funcionarios públicos con simulación de ciberataque




Este viernes 28 de abril, el CSIRT de Gobierno, en conjunto con Microsoft, realizaron el segundo ejercicio de simulación de un ciberataque interactivo en tiempo real. La actividad contó con la asistencia de alrededor de 40 funcionarios públicos, principalmente encargados de ciberseguridad y de comunicaciones de distintas entidades.

La actividad tuvo como objetivo que los participantes vivieran en tiempo real un ciberataque que amenazaba la continuidad operacional y ponía en riesgo la reputación organizacional de una compañía. Durante el ejercicio, los asistentes analizaron una serie de escenarios, debiendo decidir cuáles eran los mejores pasos a seguir para la organización desde varios puntos de vista, tomando en cuenta así las necesidades financieras, las implicancias legales y el impacto comunicacional, entre otras.

El evento fue cubierto por el periodista Óscar Valenzuela de Las Últimas Noticias (pueden ver la nota lun.com/Pages/NewsDetail.aspx?dt=2023-04-29&NewsID=510104&BodyID=0&PaginaId=13)

Ingrid Inda, Directora del CSIRT de Gobierno, destaca la importancia de que confluyan en esta simulación las visiones tanto de las áreas tecnológicas como de las demás que forman parte de la organización, “porque cuando hay un incidente, tenemos el gran problema de que el encargado de ciberseguridad tiene que estar contestando preguntas a autoridades y también estar en la investigación, en todos los frentes. Es muy bueno que se produzcan estas instancias, para que en

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

cada servicio se hagan estas dinámicas y sepan que no estamos solos, que somos parte de una red de colaboración en el Gobierno”.

Asimismo, Carlos Silva, Jefe del CSIRT de Gobierno, explicó que «el enfoque de esta jornada es unir a los sectores público y privado y colaborar para enfrentar en conjunto las amenazas cibernéticas», ya que «siempre habrá una mala configuración, una vulnerabilidad no parchada o un phishing que logró engañar a un usuario, nadie es invulnerable. Por eso debemos estar preparados, haber diseñado e implementado planes de contingencia y compenetrar a toda la organización con los pasos a seguir ante la eventualidad de un incidente».

La actividad ha tenido una positiva recepción por parte de los participantes. Paola Fuentes, una de las asistentes de Ministerio de Educación al primer ejercicio, señaló que éste fue muy provechoso “porque nos presentó el problema desde una tercera parte y por qué pudimos participar, entregar nuestras opiniones y escuchar también lo que le está pasando a los otros servicios, así que fue muy valioso”.

Las Últimas Noticias / Sábado 29 de abril de 2023

EMPLEO Y EDUCACIÓN 16

“A nivel mundial hay más de tres millones de cargos vacíos en ciberseguridad”, dice experto de Microsoft

¿Conviene pagar rescate en caso de un ciberataque?

Esa fue una de las dudas que enfrentaron los encargados de ciberseguridad del Estado en un hackeo simulado.

OSCAR VALENZUELA

A las 15 horas del inicio del Black Friday, la empresa de retail Contoso comienza a recibir quejas de sus clientes: no pueden pagar sus carros de compra y el sistema rechaza las transacciones con tarjetas de crédito.

Tras investigar, los expertos en ciberseguridad de la firma descubren que están siendo víctimas de un ciberataque. Un hacker logró colarse en el sistema de la compañía y robó los datos de sus clientes. Amenaza con publicarlos, a menos que le depositen 10 millones de dólares en bitcoins.

Así comienza el ejercicio de ciberataque simulado que dos expertos de Microsoft presentaron ante cerca de 30 encargados de seguridad de distintos ministerios y servicios públicos. La idea era abordar con ellos la mejor forma de enfrentar una disyuntiva de este tipo.

“Microsoft sigue a más de 40 bandadas internacionales que atacan a distintos sectores. Queremos concienciar sobre los efectos probables que puede tener en un ministerio, que podría quedar abajo si una de estas bandadas ingresa”, explica Roberto Alvarado, especialista técnico en ciberseguridad de la firma.

“Pasa todos los días, desde ataques a usuarios e ataques a las pymes, microempresas, empresas grandes y gobiernos. Todos tenemos que estar preocupados de protegernos y entender que esto está sucediendo cada vez más”, agrega.

Estas mafias del cibercrimen se alojan en países remotos, por lo que resulta complicado rastrearlas. También utilizan técnicas que van más allá del típico virus que funciona en forma automática: ahora los ataques son del tipo ransomware- robo de datos de clientes- y operados por humanos.

“El atacante entra a la empresa, adquiere las credenciales y se empieza a mover. Es como tomar las llaves y empezar a hacer copias; puede entrar a toda la empresa y se dedica a observar. Una vez que entiende cómo funciona, genera el ataque. Hay



Francisca Yañez y Roberto Alvarado, de Microsoft, dando la charla a los expertos en ciberseguridad del Estado.

\$1.800.000
ES EL SUELDO
que más se repite para un ingeniero en ciberseguridad junior en una empresa privada grande, según IT Hunter.

un grupo aquí que tiene táctica, está preparando las amenazas y las ejecuta en un momento que puede generar daño y obtener algo”, advierte.
“¿Hay que pagar rescates? “No, porque no hay garantía alguna y estamos alimentando a la delincuencia. La tendencia es que aparezcan regulaciones a niveles nacionales para evitar los pagos y esta industria no siga creciendo. Nuestra invitación es más bien a tomar resguardos antes y no tener que llegar a pagar, como han hecho muchas instituciones grandes a nivel mundial, que han pagado y no les ha ido bien”, señala el experto.

La firma de software Sophos encuestó en 2021 a 200 empresas medianas chilenas para su informe sobre malware. De ellas, 129 reportaron haber sufrido algún ciberataque y 32 afirmaron haber pagado rescate.

Trabajo conjunto

Ingrid Jefa, de la División de Redes y Seguridad Informática del Ministerio del Interior, plantea que ejercicios de simulación como el que desarrollaron contribuyen a tener una visión en conjunto de cómo actuar en momentos de crisis.

“Cuando hay un incidente, tenemos el gran problema que el encargado de ciberseguridad tiene que estar contestando preguntas a autoridades y también estar en la investigación, en todos los frentes”, afirma.

“Es muy bueno que se produzcan estas instancias, para que en cada servicio se hagan estas dinámicas y sepan que no estamos solos, que somos parte de una red de colaboración en el gobierno”.

¿Hacen falta más especialistas en el sector público? “A nivel técnico hace falta que se especialicen en ciberseguridad, pero también en otros niveles, como las autoridades; no podemos hacer nada si no autorizan los presupuestos, todo lo que es renovación tecnológica tiene una razón de ser, si no quedamos expuestos a cualquier vulnerabilidad”.

Carlos Silva, jefe del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Gobierno, también valora el encuentro: “El enfoque de esta jornada es unir a los sectores público y privado y cola-

borar para enfrentar en conjunto las amenazas cibernéticas”.

“Siempre habrá una mala configuración, una vulnerabilidad no parchada o un phishing que logró engañar a un usuario, nadie es invulnerable. Por eso debemos estar preparados, haber diseñado planes de contingencia y compenetrar a toda la organización con los pasos a seguir ante la eventualidad de un incidente”, sostiene.

Sueldos en empresas

Actualmente existe un déficit de especialistas. “A nivel mundial hay más de tres millones de cargos vacíos en ciberseguridad. Hoy tenemos que usar tecnologías que nos ayuden con esto, como la inteligencia artificial”, expone Roberto Alvarado.

Para hacerse una idea de cuánto ganan estos especialistas en la empresa privada, según el Décimo Estudio Salarial TIC 2022 de la reclutadora IT Hunter, que entrevistó a 500 profesionales del rubro, para los ingenieros de ciberseguridad junior (menos de dos años de experiencia) el sueldo que más se repite en una empresa grande es de \$1.800.000.

En el caso de un senior (de dos a seis años de experiencia) la remuneración que más se repite es de \$2.600 y un ingeniero senior (más de seis años de experiencia) alcanza a \$4.500.000.

Comunicado de Seguridad Cibernética | Explotación de vulnerabilidad día cero PaperCut

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, informó de una vulnerabilidad de día cero en el sistema de gestión de fotocopia e impresión en línea PaperCut MF/NG. El respectivo informe puede ser leído y descargado en PDF aquí: <https://www.csirt.gob.cl/noticias/10cnd23-00099-01/>



CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO





 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Ciberdiccionario Volumen 35

Ciberhigiene, skimmer, vishing y lista negra y lista blanca. Conceptos que se suman hoy a nuestro extenso Ciberdiccionario. Todos los volúmenes del ciberdiccionario, junto al resto de nuestras recomendaciones están en: <http://csirt.gob.cl/recomendaciones>.

 <h3>Ciber diccionario</h3> <h4>Skimmer</h4> <p>Aparatos maliciosos usados para leer los datos de tarjetas de crédito y débito. Funcionan al ser instalados como parte de un cajero automático o punto de venta (las populares "maquinitas" usadas para hacer pagos con tarjeta físicamente en el comercio), al momento de insertar la tarjeta para pagar. El riesgo se reduce al usar pago con tarjeta sin contacto.</p> 	 <h3>Ciber diccionario</h3> <h4>Ciberhigiene</h4> <p>Prácticas que nos mantienen más seguros al interactuar con internet, y que por lo tanto, tal como la higiene en el mundo físico, deberíamos implementar permanentemente. Entre estos buenos hábitos podemos mencionar el contar con antivirus y firewall, usar contraseñas difíciles de descifrar o administradores de claves, hacer copias de seguridad de nuestra información frecuentemente y educarnos sobre las principales amenazas.</p> 
 <h3>Ciber diccionario</h3> <h4>Vishing</h4> <p>Variedad de phishing (esto es, ataques de engaños a sus víctimas haciéndose pasar por personas o instituciones de confianza para robar dinero o datos) que se realiza a través de servicios de voz. Para dar más credibilidad a la llamada, a veces los delincuentes logran falsificar la información del identificador de llamadas. Por esto, nunca debemos entregar datos sensibles por teléfono o mensajería.</p> 	 <h3>Ciber diccionario</h3> <h4>Lista blanca y lista negra</h4> <p>Medidas de seguridad implementadas con la finalidad de controlar quiénes pueden acceder a un sistema informático o qué programas pueden ser ejecutados. Así, una lista blanca define específicamente los usuarios que tienen permiso de acceso, o los códigos que pueden ser ejecutados, mientras que una lista negra explicita los usuarios que no tienen derecho a ingresar, o el software prohibido.</p> 

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Día Mundial de la Contraseña


Para conmemorar el Día Mundial de la Contraseña, que tuvo lugar este jueves 4 de mayo, volvimos a publicar estos consejos para elaborar claves más robustas. Pueden ser revisadas también aquí: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-clave-segura-2023/>.

 <h3>#Ciberconsejos Cómo crear una contraseña segura</h3> <p>Ejemplo de construcción de una clave robusta</p> <ol style="list-style-type: none">1. Empieza con una frase fácil de recordar, por ejemplo: CREANDO MI CLAVE SEGURA2. Cambia algunas letras por números: CR3ANDO_M1_CL4V3_S3GUR43. Intercala mayúsculas y minúsculas e incorpora símbolos: Cr3AndO_M1_CL4V3_S3guR4! 	 <h3>#Ciberconsejos Cómo crear una contraseña segura</h3> <p>Otro ejemplo que empieza de una frase fácil de recordar</p> <p>"Chile salió campeón de América en julio de 2015"</p> <p>Utilizando sólo las letras iniciales, combinadas entre mayúsculas y minúsculas, se podría usar CsCdAe7/15 como contraseña.</p> 
 <h3>#Ciberconsejos Cómo crear una contraseña segura</h3> <p>Al construir una clave:</p> <ul style="list-style-type: none">• NUNCA uses datos personales como RUT, teléfono o dirección.• NO USES cumpleaños, datos o nombres de familiares o mascotas• NUNCA repitas la misma contraseña en distintas cuentas. 	 <h3>#Ciberconsejos Cómo crear una contraseña segura</h3> <ul style="list-style-type: none">• Para tu frase de partida puedes usar la letra de alguna canción, nombres de películas o pasajes de libros.• Recuerda: entre más usada y frecuente sea una clave, menos segura es. En Chile algunas de las contraseñas más utilizadas, y que no recomendamos utilizar son "123456789" y "colocolo", que está dentro de las 10 claves más repetidas en el país.

5. 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.

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

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.

- Michel Díaz Ibeas
- Gonzalo Salazar
- María Parra
- María Rojas B.
- Rubén Dario M.
- Gisela Gatica
- Yerko Cáceres L.
- Roberto Metcalfe
- Darwin Bustos E.
- Jerson Cifuentes O.
- Juan Ortiz
- Manuel Rojas
- Marcelo Rodríguez K.
- Karina Puvogel
- Rodrigo Rivera R.
- Thaisse González Torres
- Iván Bello González
- Romina Tenorio Gómez
- Dennis Juárez Cantellano
- Juan Rodríguez López
- Pablo González Wall
- Paula Vera Matus

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO