Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

26-08-2022 | Año 4 | N°164

# Boletín de Seguridad Cibernética

Semana del 19 al 25 de agosto de 2022

## La semana en cifras

**Parches**

4

**para vulnerabilidades**

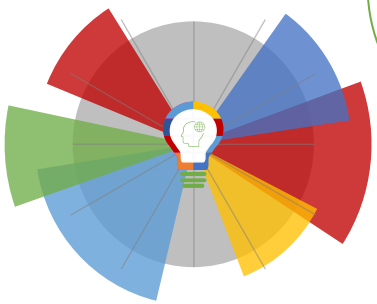
Las mitigaciones son útiles en productos de Chrome, Cisco, Linux y Palo Alto.

**IP**

8

**Informadas**

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



**Se advirtieron**

12

**URL**

Asociadas a sitios fraudulentos y campañas de phishing y malware.

**Hash**

21

**SHA**

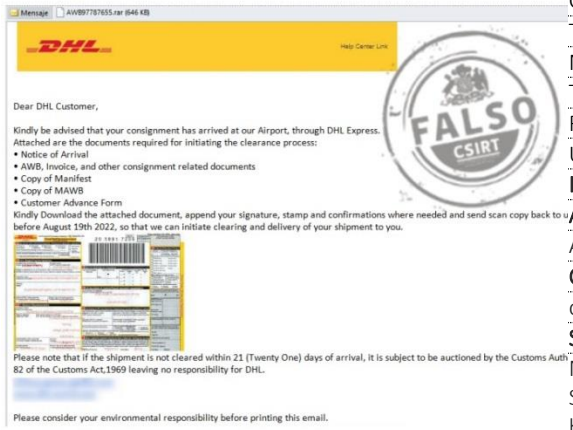
Asociadas a múltiples campañas de phishing con archivos que contienen malware

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

## Contenido

# Malware

## Imagen del Mensaje




| CSIRT alerta por campaña de phishing con malware que suplanta a DHL | |
|---|---|
| Alerta de seguridad cibernética | 2CMV22-00327-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de agosto de 2022 |
| Última revisión | 22 de agosto de 2022 |

**Indicadores de compromiso**

**Asunto**

AWB: Air Waybill Delivery Receipt – BL / Packing List

**Correo de salida**

delivery-dhl@mail.com

**SHA256**

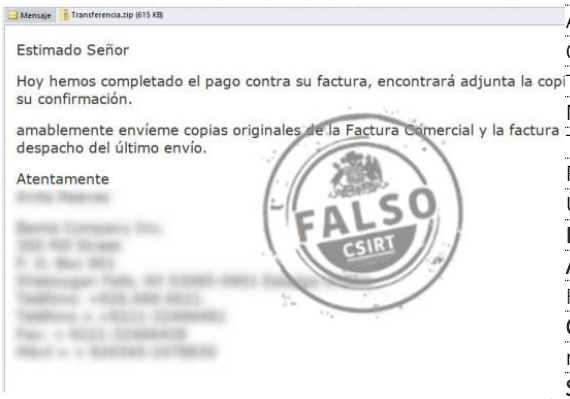
Nombre: AWB97787655.rar
SHA256:
bb3c85108b3140c8062307ba6c763e4fba328ff6b737c89c97271f0d53891377

Nombre: AWB97787655.exe
SHA256:
a96a34c47ca8192a0e77c99c8993a08bc4f66824bb243f423db8632491df13a6

**Enlaces para revisar el informe:**

https://www.csirt.gob.cl/alertas/2cmv22-00327-01/
https://www.csirt.gob.cl/media/2022/08/2CMV22-00327-PH-01.pdf

**Imagen del Mensaje**




| CSIRT alerta por campaña de phishing que contiene el malware Agent Tesla | |
|---|---|
| Alerta de seguridad cibernética | 2CMV22-00328-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de agosto de 2022 |
| Última revisión | 22 de agosto de 2022 |

**Indicadores de compromiso**

**Asunto**

Rv: Transferencia

**Correo de Salida**

reply@spuredge.com

**SHA256**

Nombre: Transferencia.zip
SHA256:
dbd93d419298e4d7a98f0f3632987913dc0896211bdb91a48b68022c1477d685

Nombre: LGri43t5b5MMet7.exe
SHA256:
ad88e4f04caf933d6611f203982d08b641ee9260d7a483e147ecfffdfb8646fb

Nombre: Cgip.exe
SHA256:
eed3816c78dea9e300f09db358b1112d3bc6a71cfd8d19236526732db9851240

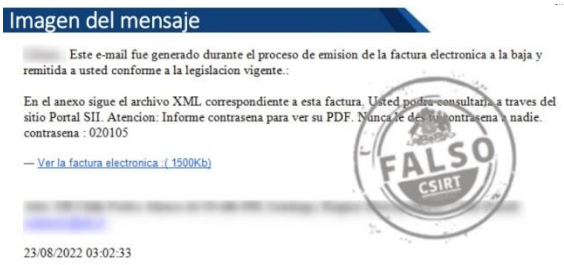
**Enlaces para revisar el informe:**

https://www.csirt.gob.cl/alertas/2cmv22-00328-01/
https://www.csirt.gob.cl/media/2022/08/2CMV22-00328-PH-01.pdf

Imagen del mensaje


| CSIRT alerta por phishing que suplanta a laboratorio AC Farma | |
|---|---|
| Alerta de seguridad cibernética | 2CMV22-00329-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de agosto de 2021 |
| Última revisión | 23 de agosto de 2021 |
| **Indicadores de compromiso** | |
| **Asunto** | |
| RE: [EXTERNAL] RE: RE: Nuevo orden | |
| **Correo de Salida** | |
| ventas@acfarma.com | |
| **SHA256** | |
| Nombre: se adjunta una nueva_lista de pedidos.zip<br>SHA256:<br>d7afb55c8de595f9082e1110cdc1a0eb2f7672df7387f53a6863cc415961844a<br><br>Nombre: se adjunta una nueva lista de pedidos.ex<br>SHA256:<br>d5ea63b4008d1614f902be96fdc7d37898a7254ec22fc52e0f4eb11418a6893c | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/2cmv22-00329-01/ | |
| https://www.csirt.gob.cl/media/2022/08/2CMV22-00329-PH-01.pdf | |

Imagen del mensaje




| CSIRT alerta de campaña de phishing enviada desde email de la Organización Mundial de Agricultores | |
|---|---|
| Alerta de seguridad cibernética | 2CMV22-00330-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de agosto de 2021 |
| Última revisión | 23 de agosto de 2021 |
| **Indicadores de compromiso** | |
| **Asunto** | |
| ✓FACTURA – Notificacion Giro Folio 012210001 del 15/08/2022 – SII – – ( 606787556782 ) | |
| **Correo de Salida** | |
| www-data@wfo-oma.org | |
| **SHA256** | |
| Nombre: FACTURA-IDSE-34ed1ecf.zip<br>SHA256:<br>5db643388dea02dd4cdeb73d3e864ff70e7d01fb5b09c782f7cb053bf6626f41 | |

| |
|---|
| Nombre: FACTURA-IDSE-34ed1ecf-1a2c-4d26-85ba-ba00014ssff74.msi<br>SHA256: 6a16db3db54167b246c1f2239e35c0c55d983b33537187f5c0870fba205333eb<br><br>Nombre: dns-sd-documento bajo_____.exe<br>SHA256: 6a27826b490457ccfecebaf98a01325cc1ccecc81917b156aa1e566d141b520c<br><br>Nombre: mi87we.exe<br>SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4<br><br>Nombre: AutoHotkey.exe<br>SHA256: b7f084f91a0a03ebad46d305d0fc5f8bddc144b0ce53087c6d219c6b601fe419 |
| **Enlaces para revisar el informe:** |
| https://www.csirt.gob.cl/alertas/2cmv22-00330-01/ |
| https://www.csirt.gob.cl/media/2022/08/2CMV22-00330-PH-01.pdf |

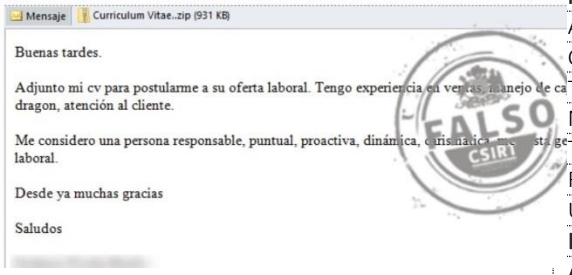
Imagen del Mensaje


| CSIRT alerta de campaña de phishing con malware que suplanta al SII | |
|---|---|
| Alerta de seguridad cibernética | 2CMV22-00331-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de agosto de 2022 |
| Última revisión | 23 de agosto de 2022 |
| **Indicadores de compromiso** | |
| **Asunto** | |
| SII \| Servicio de Impuestos Internos – Boleta de Honorarios<br>SII \| Servicio de Impuestos Internos – Declaracion de renta<br>FACTURA – GUILLERMO HURTADO, Notificacion Giro Folio 012210001 del 15/08/2022 – SII<br>Pago de contribuciones de bienes raices en SII – ChileAtiende<br>Contribuciones – SII \| Servicio de Impuestos Internos<br>SII \| Servicio de Impuestos Internos – ChileAtiende<br>Pago contribuciones – Internet – SII<br>SII \| Servicio de Impuestos Internos – Declaracion de renta<br>Contribuciones – SII \| Servicio de Impuestos Internos | |

| |
|---|
| SII \| Servicio de Impuestos Internos – Servicios online<br>Servicio de Impuestos Internos – SII Chile |
| **Correo de Salida** |
| www-data@wfo-oma.org<br>root@contactorutempresascl1.sending.contact<br>root@contactorutempresascl2.sending.contact<br>root@contactorutempresascl3.sending.contact<br>root@contactorutempresascl4.sending.contact<br>root@contactorutempresascl5.sending.contact<br>root@contactorutempresascl6.sending.contact<br>root@contactorutempresascl7.sending.contact<br>root@contactorutempresascl8.sending.contact<br>root@contactorutempresascl9.sending.contact<br>root@contactorutempresascl10.sending.contact<br>root@contactorutempresascl11.sending.contact<br>root@contactorutempresascl12.sending.contact<br>root@contactorutempresascl13.sending.contact<br>root@contactorutempresascl14.sending.contact<br>root@contactorutempresascl15.sending.contact<br>root@contactorutempresascl16.sending.contact<br>root@contactorutempresascl17.sending.contact<br>root@contactorutempresascl18.sending.contact<br>root@contactorutempresascl19.sending.contact<br>root@contactorutempresascl20.sending.contact<br>root@contactorutempresascl21.sending.contact<br>root@contactorutempresascl22.sending.contact<br>root@contactorutempresascl23.sending.contact<br>root@contactorutempresascl24.sending.contact<br>root@contactorutempresascl25.sending.contact<br>root@contactorutempresascl26.sending.contact<br>root@contactorutempresascl27.sending.contact<br>root@contactorutempresascl28.sending.contact<br>root@contactorutempresascl29.sending.contact<br>root@contactorutempresascl30.sending.contact<br>root@contactorutempresascl31.sending.contact<br>root@contactorutempresascl32.sending.contact<br>root@contactorutempresascl33.sending.contact<br>root@contactorutempresascl34.sending.contact<br>root@contactorutempresascl35.sending.contact<br>root@contactorutempresascl37.sending.contact<br>root@contactorutempresascl38.sending.contact<br>root@contactorutempresascl39.sending.contact<br>root@contactorutempresascl40.sending.contact |
| **URL Redirección** |
| http://ec2-18-220-159-252.us-east-2.compute[.]amazonaws.com/09907213678468573/?hash=dGVzdEB0ZXN0LnRlc3QuY2w= |
| **URL Sitio de Descarga** |
| http://ec2-18-230-196-74.sa-east- |

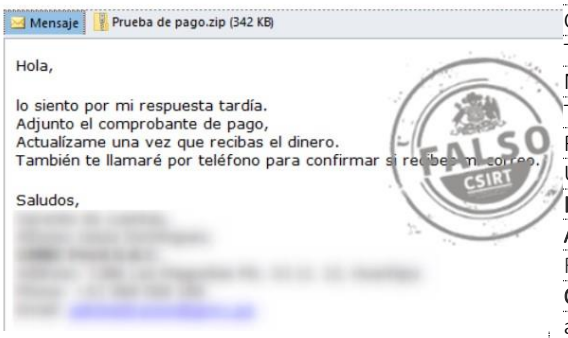
| |
|---|
| 1.compute.amazonaws[.]com/000912789894390/?=hTt0SaNNjNCs2u6A5ZcNfnYeC9rLWs8VXY6DOjGBdm34RCCmE2QHG3WZqOIs9NN56XU3HEE89M7NaWrCUXE7NM42VKnmfKRuDA6tjqtOPXOLjLcnthpGVpaNeK9t5c3TGppuUgZUZUAcZME1KJnEV74qENojdMjXuBZLXpATHc5BuDrVM9pEMNpt5VF4bFAWgNP5X0cra7p09P7OAG3eSJFZPrUHZ1V7JbXu0eIff5oVtQ0fFdPuBDc246sMVtZKbaPIYmfg0ndbXJMJMtrmpjt1KisJ6E5f78G4muiRl7ZdGBWjSnCjlOOdmEEAbHafHOmJUJW26RGHqeWLF1SVJP9tZI7mcf3FEDX2OWV4KgH4VZRhOimuS7CdXRW6fi1BAoj8Y4VHVBhhCBTl7NKO0u3G1NYF7ZOP5MRK0JNtAKLC1YQTBFOoBuKH0UBoF1Nu8eVl3CmpIelXuLMO9N0YoDl94eTEfBLSpe8ZPcH |
| SHA256 |
| Nombre: 01029714774265617 23.zip<br>SHA256:<br>47025b68e8957a74103d8cde53aa69f45c736b72d42124da901909dbcbd38af3<br><br>Nombre: 012939788487563891871219283.msi<br>SHA256:<br>315be91e3fa83ae53779ba5790d56c63d94d059415a37f61b4d74aa2583a5571<br><br>Nombre: AICustAct.dll<br>SHA256:<br>f3d3093654091a85076c0b7de00930f2760d4b2e42b94c7e3813ec94e7c369d9<br><br>Nombre: bozondah2.exe<br>SHA256:<br>3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4<br><br>Nombre: AutoHotkey.exe<br>SHA256:<br>b7f084f91a0a03ebad46d305d0fc5f8bddc144b0ce53087c6d219c6b601fe419 |
| Enlaces para revisar el informe: |
| https://www.csirt.gob.cl/alertas/2cmv22-00331-01/ |
| https://www.csirt.gob.cl/media/2022/08/2CMV22-00331-PH-01-1.pdf |

Imagen del mensaje




| CSIRT alerta de campaña de phishing con malware que simula oferta laboral | |
|---|---|
| Alerta de seguridad cibernética | 2CMV22-00332-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de agosto de 2022 |
| Última revisión | 23 de agosto de 2022 |
| **Indicadores de compromiso** | |
| **Asunto** | |
| Re : Cv: Vendedora | |
| **Correo de Salida** | |
| stefynoelia@hotmail.com | |
| **SHA256** | |
| Nombre: Curriculum Vitae..zip<br>SHA256:<br>28aab8fdff8a6b2176035ba362ceca68103e82b6be9b69f7101885aebd8c1835<br><br>Nombre: Curriculum Vitae..exe<br>SHA256:<br>e0a6911dc23cf10c99586f4a684b0772825d22e105b39e0945a71ade106fa47f | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alerts/2cmv22-00332-01/ | |
| https://www.csirt.gob.cl/media/2022/08/2CMV22-00332-PH-01.pdf | |

Imagen del mensaje




| CSIRT alerta ante campaña de phishing con falso documento de pago | |
|---|---|
| Alerta de seguridad cibernética | 2CMV22-00333-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de agosto de 2022 |
| Última revisión | 24 de agosto de 2022 |
| **Indicadores de compromiso** | |
| **Asunto** | |
| RE: [EXTERNAL] RE: RE: Pago | |
| **Correo de Salida** | |
| administracion@gmrc.pe | |
| **SHA256** | |
| Nombre: Prueba de pago.zip<br>SHA256:<br>43b6e8a635ff8c8d01113d9a689ff6018a619aed975294123143af3545bc1e68 | |

| |
|---|
| Nombre: Prueba de pago.exe<br>SHA256:<br>434bd3bb524489d6108cd451e649ccdd768ca678d06fb10685e620b117ff8384 |
| **Enlaces para revisar el informe:** |
| https://www.csirt.gob.cl/alertas/2cmv22-00333-01/ |
| https://www.csirt.gob.cl/media/2022/08/2CMV22-00333-PH-01.pdf |

# Phishing

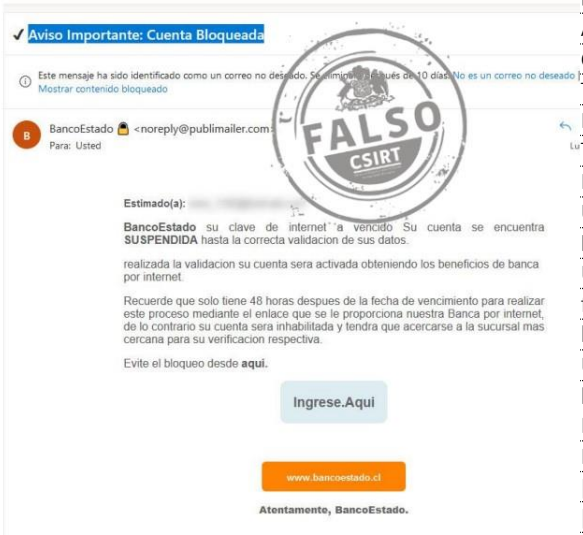
## Imagen del mensaje


| CSIRT alerta campaña de phishing que suplanta a Microsoft Office 365 | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00579-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de agosto de 2022 |
| Última revisión | 19 de agosto de 2022 |
| **Indicadores de compromiso** | |
| URL sitio redirección | |
| file:///C:/Users/%User%/Desktop/payment%20reciept%20copy.shtml | |
| https://semiotic-bigamies.000webhostapp.com/wp-includes/aabb.php | |
| URL sitio falso | |
| https://jumpshare.com/v/TmimdC0XEBvinTJCISUW | |
| IP | |
| [38.242.145.252] | |
| [34.205.35.74] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph22-00579-01/ | |
| https://www.csirt.gob.cl/media/2022/08/8FPH22-00579-01.pdf | |

## Imagen del mensaje

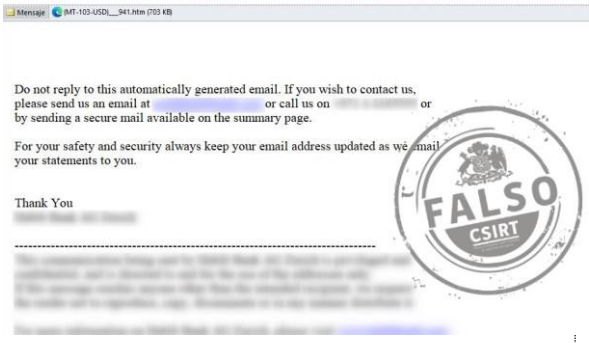

| CSIRT alerta ante nueva campaña de phishing con falso pago | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00580-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de agosto de 2022 |
| Última revisión | 19 de agosto de 2022 |
| **Indicadores de compromiso** | |
| URL sitio redirección | |
| file:///C:/Users/%User%/Desktop/Invoice%20settlement.shtml | |
| https://submit-form[.]com/eHYJ6VdY | |
| URL sitio falso | |
| https://submitted.formspark[.]io/?_formId=eHYJ6VdY&_status=OK&_title=Your%20form%20has%20been%20submitted | |
| IP | |
| [45.9.168.127] | |
| [108.159.227.11] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph22-00580-01/ | |
| https://www.csirt.gob.cl/media/2022/08/8FPH22-00580-01.pdf | |

Imagen del mensaje




| CSIRT alerta ante campaña de phishing que suplanta al BancoEstado | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00581-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de agosto de 2022 |
| Última revisión | 22 de agosto de 2022 |
| **Indicadores de compromiso** | |
| URL sitio redirección | |
| file:///C:/Users/%User%/Desktop/Invoice%20settlement.shtml | |
| https://submit-form[.]com/eHYJ6VdY | |
| URL sitio falso | |
| https://submitted.formspark[.]io/?_formId=eHYJ6VdY&_status=OK&_title=Your%20form%20has%20been%20submitted | |
| IP | |
| [168.232.165.161] | |
| [138.128.188.146] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph22-00581-01/ | |
| https://www.csirt.gob.cl/media/2022/08/8FPH22-00581-01.pdf | |

Imagen del mensaje




| CSIRT alerta ante nueva campaña de phishing que dirige a falso sitio de Office 365 | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00581-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de agosto de 2022 |
| Última revisión | 22 de agosto de 2022 |
| **Indicadores de compromiso** | |
| URL sitio redirección | |
| file:///C:/Users/%User%/Downloads/(MT-103-USD)___941.htm | |
| URL sitio falso | |
| https://drmwahiduzzaman[.]info/wp-includes/blocks/block/reportnewgeneral2pass.php | |
| IP | |
| [51.161.153.37] | |
| [162.241.194.201] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph22-00582-01/ | |
| https://www.csirt.gob.cl/media/2022/08/8FPH22-00582-01.pdf | |

# Vulnerabilidades


| CSIRT comparte vulnerabilidad crítica en ChromeOS | |
|---|---|
| Alerta de seguridad cibernética | 9VSA22-00693-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de agosto de 2022 |
| Última revisión | 22 de agosto de 2022 |
| **CVE** | |
| CVE-2022-2587 | |
| **Fabricantes** | |
| Google | |
| **Productos afectados** | |
| Google ChromeOS. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00693-01/ | |
| https://www.csirt.gob.cl/media/2022/08/9VSA22-00693-01.pdf | |


| CSIRT comparte vulnerabilidad en el kernel de Linux | |
|---|---|
| Alerta de seguridad cibernética | 9VSA22-00694-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de agosto de 2022 |
| Última revisión | 22 de agosto de 2022 |
| **CVE** | |
| CVE-2022-2588 | |
| **Fabricantes** | |
| Linux | |
| **Productos afectados** | |
| Linux kernel. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00694-01/ | |
| https://www.csirt.gob.cl/media/2022/08/9VSA22-00694-01.pdf | |


| CSIRT comparte vulnerabilidad grave en Cisco Secure Web Appliance | |
|---|---|
| Alerta de seguridad cibernética | 9VSA22-00692-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de agosto de 2022 |
| Última revisión | 22 de agosto de 2022 |
| **CVE** | |
| CVE-2022-20871 | |
| **Fabricantes** | |
| Cisco | |
| **Productos afectados** | |
| Cisco Secure Web Appliance | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00695-01/ | |
| https://www.csirt.gob.cl/media/2022/08/9VSA22-00695-01.pdf | |


| CSIRT comparte vulnerabilidad de alto riesgo en firewall PAN-OS | |
|---|---|
| Alerta de seguridad cibernética | 9VSA22-00696-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de agosto de 2022 |
| Última revisión | 23 de agosto de 2022 |
| **CVE** | |
| CVE-2022-0028 | |
| **Fabricantes** | |
| PAN-OS | |
| **Productos afectados** | |
| Productos que usan el software de firewall PAN-OS como los aparatos de las series PA, VM y CN.<br>Versiones de PAN-OS vulnerables a ataques incluyen PAN-OS anteriores a 10.2.2-h2, 10.1.6-h6, 10.0.11-h1, 9.1.14-h4, 9.0.16-h3 y 8.1.23-h1. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00696-01/ | |
| https://www.csirt.gob.cl/media/2022/08/9VSA22-00696-01.pdf | |

# Actualidad

## Segundo Ejercicio de Simulación en Gestión de Ciberseguridad para Funcionarios Públicos reúne más de 380 participantes


El CSIRT de Gobierno organizó la segunda versión del Ejercicio de Simulación en Gestión de Ciberseguridad para Funcionarios Públicos, llevado a cabo por Kaspersky y abierto a empleados del Estado y del Sistema de Empresas Públicas (SEP).

*Puede leer la nota completa en nuestro sitio: csirt.gob.cl/noticias/segundo-ejercicio-de-simulacion-en-gestion-de-ciberseguridad-para-funcionarios-publicos-reune-mas-de-380-participantes/.*

En la actividad participaron más de 380 personas de diferentes organizaciones del Estado, organizados en diferentes equipos como también de forma individual, superando la cifra de la edición anterior. Gracias a esta iniciativa, centenares de funcionarios pudieron enfrentar una simulación realista de un incidente de ciberseguridad, lo que les ayudará a estar más preparados para enfrentar la gestión de este tipo de situaciones en su vida profesional.

Los mayores puntajes del ejercicio fueron obtenidos por Héctor Saavedra, de la Subsecretaría de Relaciones Económicas Internacionales, el TEAM ISL compuesto por Tania Estrada y Miguel López del Instituto de Seguridad Laboral y Vicente Alarcón, de Ministerio de Hacienda.

Los organizadores destacaron que esta actividad permite a los participantes enfrentar problemáticas esenciales que se deben resolver en ciberseguridad, y a las organizaciones capacitar y concientizar a todos los funcionarios sin diferencia. Además, hicieron un llamado a reforzar que las credenciales sean clasificadas, almacenadas y procesadas de manera correcta y según políticas de seguridad previamente definidas, además de tener personal capacitado para la respuesta ante incidentes y un equipamiento que permita detectar de amenazas.

Asimismo, indicaron que cuando un atacante logra ingresar a nuestra infraestructura es porque descubrió una vulnerabilidad en los sistemas o explotó el factor humano, por lo que es importante contar con controles de autentificación adecuados para lograr detener a los ciberdelincuentes, así como con respaldos de la información de la organización en diferentes lugares físicos. Por último, señalaron que es importante establecer controles de seguridad acordes a la gestión de riesgo de la organización, y recalcaron que el factor humano es lo más importante: no basta invertir grandes montos en tecnología si no existe al mismo tiempo una adecuada capacitación a las personas.

## Día del Internauta

El 23 de agosto, el CSIRT de Gobierno aprovechó de compartir algunos de sus consejos de navegación más segura con motivo del denominado "día del internauta", celebrado ese día por ser un nuevo aniversario del primer acceso a una página web, un 23 de agosto pero de 1991.
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-navegacion-segura/

## Ciberdiccionario Volumen 15

Publicamos asimismo la decimoquinta edición del Ciberdiccionario del CSIRT de Gobierno, centrada en términos del mundo de la ciberseguridad. Pueden ser descargados como imágenes y PDF, aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-15/




## 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 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.

- Isamar Parada
- Giancarlo Barba
- Francisca Valenzuela
- Antonia Moyano
- Mariela Saldías
- Roberto Sapiain
- Gonzalo Araya
- Fabrizzio Moreno
- Kevin Anguita
- Martín Nagel