Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

25-03-2022 | Año 4 | N°142

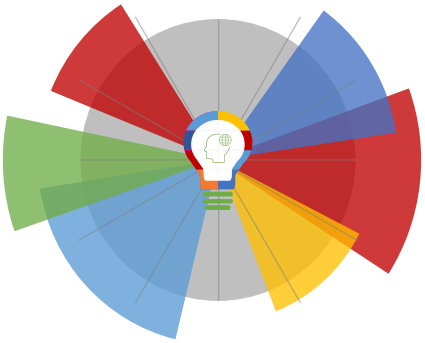
# Boletín de Seguridad Cibernética

Semana del 18 al 24 de marzo de 2022

# La semana en cifras

**Hash**
**18**
**SHA**
Asociadas a múltiples campañas de phishing con archivos que contienen malware

**Se advirtieron**
**28**
**URL**
Asociadas a sitios fraudulentos y campañas de phishing y malware.



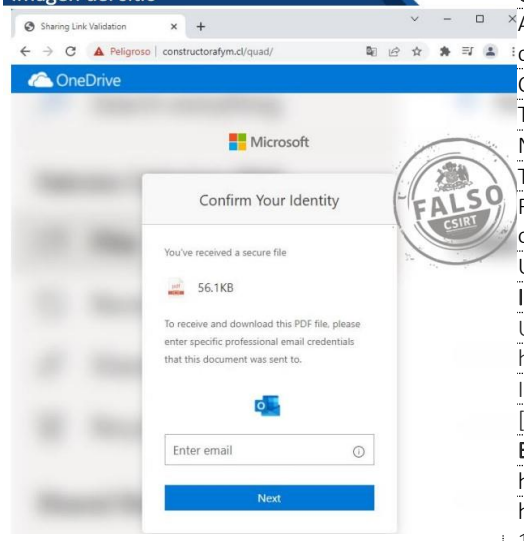
**Parches**
**13**
**para vulnerabilidades**
Las mitigaciones son útiles en productos Red Hat, HP y McAfee.

**IP**
**23**
**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

# Sitios fraudulentos

| Imagen del sitio | | |
|---|---|---|
|  | **CSIRT informa sitio web falso de Microsoft Onedrive** | |
| | Alerta de seguridad cibernética | 8FFR22-01064-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Falsificación de Registros o Identidad |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 22 de marzo de 2022 |
| | Última revisión | 22 de marzo de 2022 |
| | **Indicadores de compromiso** | |
| | URL sitio falso | |
| | http://www.constructorafym.cl/quad/ | |
| | IP | |
| | [192.3.201.45] | |
| | **Enlaces para revisar el informe:** | |
| | https://www.csirt.gob.cl/alertas/8ffr22-01064-01/ | |
| | https://www.csirt.gob.cl/media/2022/03/8FFR22-01064-01.docx-1.pdf | |

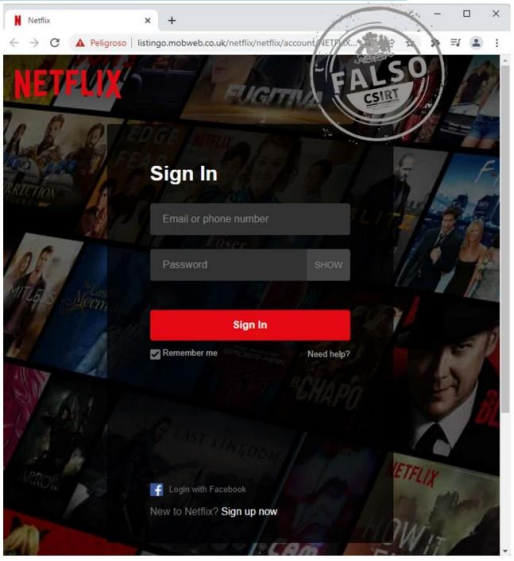
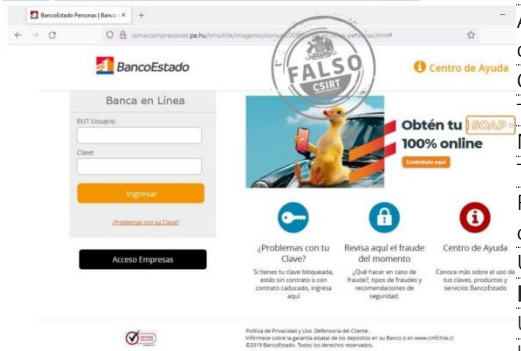
| Imagen del sitio | | |
|---|---|---|
|  | **CSIRT alerta de sitio web falso de Netflix** | |
| | Alerta de seguridad cibernética | 8FFR22-01065-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Falsificación de Registros o Identidad |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 22 de marzo de 2022 |
| | Última revisión | 22 de marzo de 2022 |
| | **Indicadores de compromiso** | |
| | URL sitio falso | |
| | https://listingo.mobweb.co[.]uk/netflix/netflix/account/NETFLIX/login | |
| | IP | |
| | [23.231.24.26] | |
| | **Enlaces para revisar el informe:** | |
| | https://www.csirt.gob.cl/alertas/8ffr22-01065-01/ | |
| | https://www.csirt.gob.cl/media/2022/03/8FFR22-01065-01.pdf | |

Imagen del sitio




| CSIRT informa página web falsa del Banco Estado | |
|---|---|
| Alerta de seguridad cibernética | 8FFR22-01066-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de marzo de 2022 |
| Última revisión | 23 de marzo de 2022 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| http://remaccompressores.pe[.]hu/smschile/imagenes/comun2008/banca-en-linea-personas.html# | |
| IP | |
| [31.220.106.21] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr22-01066-01/ | |
| https://www.csirt.gob.cl/media/2022/03/8FFR22-01066-01.pdf | |

# Phishing

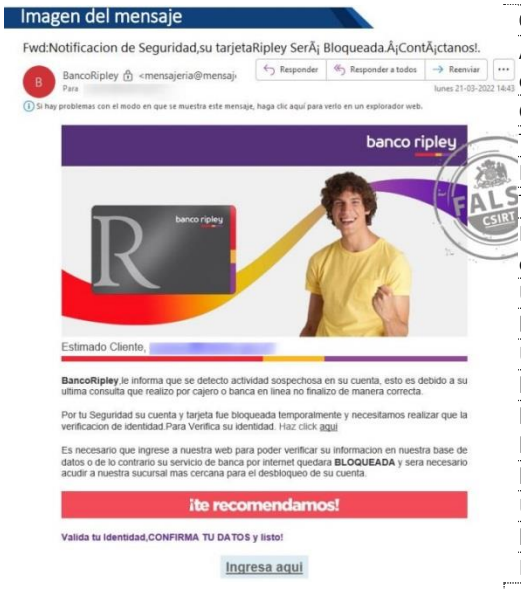
Imagen del mensaje


| CSIRT advierte phishing con falsa tarjeta bloqueada | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00482-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 18 de marzo de 2022 |
| Última revisión | 18 de marzo de 2022 |
| **Indicadores de compromiso** | |
| URL redirección | |
| https://bit[.]ly/3Ib7Job?l=www.bancofalabella.cl | |
| http://handvina[.]com/wp-includes/certificates/enviar03.php?l=856719433 | |
| URL sitio falso | |
| http://www-banc0falabella-cl.artncommerce[.]com/login | |
| IP | |
| [194.156.65.86] | |
| [104.168.137.228] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph22-00482-01/ | |
| https://www.csirt.gob.cl/media/2022/03/8FPH22-00482-01.pdf | |

Imagen del mensaje


| CSIRT informa de phishing que suplanta al Banco de Chile | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00483-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de marzo de 2022 |
| Última revisión | 21 de marzo de 2022 |
| **Indicadores de compromiso** | |
| URL sitio redirección | |
| https://bit[.]ly/disponible_cupo | |
| https://jeffiekaysanders[.]com/chile1.php | |
| URL sitio falso | |
| https://lggin-hnncochile.cl-lgnin[.]buzz/1647873442/bcochile-web/persona/login/index.html/login | |
| IP | |
| [144.217.129.197] | |
| [172.67.200.96] | |
| **Enlaces para revisar el informe:** | |

| |
|---|
| https://www.csirt.gob.cl/alertas/8fph22-00483-01/ |
| https://www.csirt.gob.cl/media/2022/03/8FPH22-00483-01.pdf |




| CSIRT alerta phishing que suplanta al Banco Ripley | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00484-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de marzo de 2022 |
| Última revisión | 21 de marzo de 2022 |
| **Indicadores de compromiso** | |
| URL sitio redirección | |
| https://bit[.]ly/3tq6v4e?l=www.bancoripley.cl | |
| http://xn--119-hy7mx2m78r[.]kr/assets/bootstrap/css/enviar02.php | |
| https://bit[.]ly/3D1RnNK?l=www.bancoripley.cl | |
| URL sitio falso | |
| https://wardatalwadirealestates[.]com/activacion/cuenta-zlft/ | |
| IP | |
| [46.101.52.30] | |
| [193.111.73.134] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph22-00484-01/ | |
| https://www.csirt.gob.cl/media/2022/03/8FPH22-00484-01.pdf | |

| Imagen del mensaje | CSIRT advierte phishing que suplanta al Banco Estado | |
|---|---|---|
|  | | |
| | Alerta de seguridad cibernética | 8FPH22-00485-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Phishing |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 22 de marzo de 2022 |
| | Última revisión | 22 de marzo de 2022 |
| | **Indicadores de compromiso** | |
| | URL sitio falso | |
| | http://hk54.hkwordpress[.]com/poque/pagina/imagenes/comun2008/banca-en-linea-personas.html | |
| | https://bit[.]ly/3D1RnNK?l=www.bancoripley.cl | |
| | IP | |
| | [190.114.253.236]<br>[192.254.165.156] | |
| | **Enlaces para revisar el informe:** | |
| | https://www.csirt.gob.cl/alertas/8fph22-00485-01/ | |
| | https://www.csirt.gob.cl/media/2022/03/8FPH22-00485-01.pdf | |

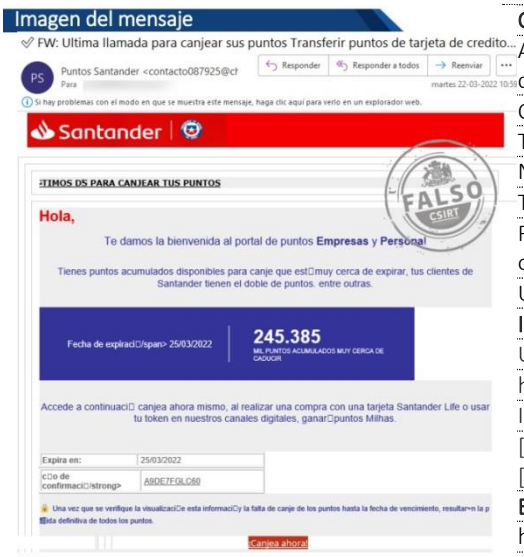
| Imagen del mensaje | CSIRT advierte phishing que suplanta al Banco Santander | |
|---|---|---|
|  | | |
| | Alerta de seguridad cibernética | 8FPH22-00486-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Phishing |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 22 de marzo de 2022 |
| | Última revisión | 22 de marzo de 2022 |
| | **Indicadores de compromiso** | |
| | URL sitio falso | |
| | https://santanderclpuntos[.]net/control.php | |
| | IP | |
| | [51.158.78.80]<br>[212.192.246.72] | |
| | **Enlaces para revisar el informe:** | |
| | https://www.csirt.gob.cl/alertas/8fph22-00486-01/ | |
| | https://www.csirt.gob.cl/media/2022/03/8FPH22-00486-01.pdf | |

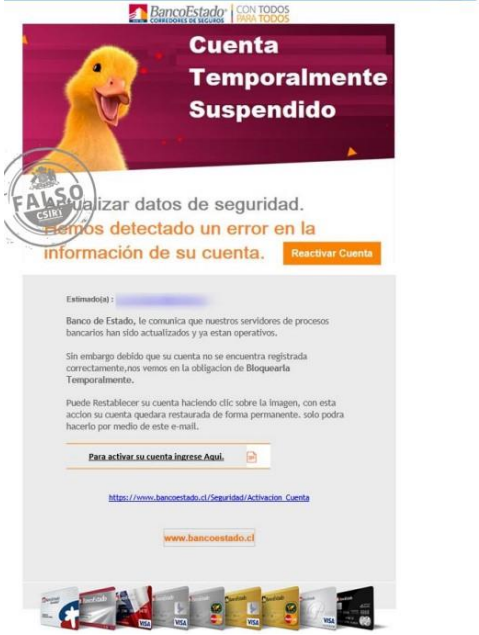
Imagen del mensaje


| CSIRT advierte phishing que suplanta al Banco Santander | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00487-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de marzo de 2022 |
| Última revisión | 22 de marzo de 2022 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| http://ec2-54-233-216-95.sa-east-1.compute.amazonaws[.]com/67333000 | |
| https://puntosytarjetas.targetapuntosiup[.]com/App6b99584/access.php | |
| IP | |
| [51.195.119.89] | |
| [172.67.158.16] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph22-00487-01/ | |
| https://www.csirt.gob.cl/media/2022/03/8FPH22-00487-01-1.pdf | |

Imagen del mensaje


| CSIRT informa phishing donde suplanta a CorreosChile | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00488-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de marzo de 2022 |
| Última revisión | 22 de marzo de 2022 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://app-mob2[.]com/CL-TRACK/Y/ | |
| IP | |
| [78.128.81.155] | |
| [159.223.228.225] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph22-00488-01/ | |
| https://www.csirt.gob.cl/media/2022/03/8FPH22-00488-01.pdf | |

Imagen del mensaje



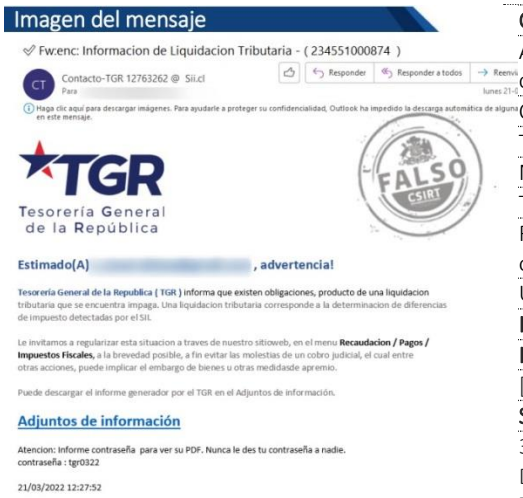

| CSIRT advierte phishing con supuesto bloqueo de tarjeta | |
|---|---|
| Alerta de seguridad cibernética | 8FPH22-00489-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de marzo de 2022 |
| Última revisión | 23 de marzo de 2022 |
| **Indicadores de compromiso** | |
| URL redirección | |
| http://ns1.inmystream.net/activacion/cuenta-fdun/ | |
| URL sitio falso | |
| https://www.bdslegalserv[.]com/Clientes/pagina/imagenes/comun2008/banca-en-linea-personas.html | |
| IP | |
| [45.7.230.246] | |
| [142.93.223.69] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph22-00489-01/ | |
| https://www.csirt.gob.cl/media/2022/03/8FPH22-00489-01.pdf | |

# Malware


| CSIRT advierte campaña de malware con falso pago rechazado | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00285-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de marzo de 2022 |
| Última revisión | 21 de marzo de 2022 |
| **Indicadores de compromiso** | |
| **IP** | |
| [2.56.57.142] | |
| **SHA256** | |
| 45F9C7A7FBF48209458B49A173C14BF4BCAD6F118DCABD16F36D5976E9B788DB<br>55DF447155FE7AE911B89FF68320374F6A0E4BD85C406B8C47FF3221D93AC782 | |
| **IoC URL** | |
| hhttps://rbmimport[.]com/emmk/transferencia.XlSx.zip | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/2cmv22-0285-01/ | |
| https://www.csirt.gob.cl/media/2022/03/2CMV22-00285-01.pdf | |


| CSIRT advierte campaña de malware que suplanta a la Tesorería General de la República | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00286-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de marzo de 2022 |
| Última revisión | 21 de marzo de 2022 |
| **Indicadores de compromiso** | |
| **IP** | |
| [203.115.100.91] | |
| **SHA256** | |
| 3316B967FFBE7806CCEC9E58C7991092BFD7BA35C8433B8D66BD2818AF6FB66B<br>10D9650FF8F30F631DC5708F91171569A5EC1BFD00EBEF8856BC6C3F25CAEBCB<br>3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4 | |

| |
|---|
| F0E24F78907C85916056A6E40C9B69D28B92C30038526FEE9CE2BE7C0C7686E7<br>0B02777C821B11F24B3F01C2DA7D85319CCB624E907075798A8D0DBFC3CE5ABC<br>C84B874E12794302DFE5507BC5E0BF21F64BC92357AD9382136A3EF66BB36244<br>3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4 |
| **IoC URL** |
| http://3.144.108[.]13/imbox/<br>https://agtta.co[.]in/userfile/down/<br>https://dkloja.com[.]br/signup/file/8u21R0s5i361w01.zip |
| **Enlaces para revisar el informe:** |
| https://www.csirt.gob.cl/alertas/2cmv22-00286-01/ |
| https://www.csirt.gob.cl/media/2022/03/2CMV22-00286-01.pdf |




| CSIRT advierte campaña de malware suplantando a la TGR | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00287-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de marzo de 2022 |
| Última revisión | 22 de marzo de 2022 |

| **Indicadores de compromiso** |
|---|
| **IP** |
| [159.69.42.89] |
| **SHA256** |
| 3316B967FFBE7806CCEC9E58C7991092BFD7BA35C8433B8D66BD2818AF6FB66B<br>7C3265CA51A663AFF433106C49303EDEBE6D7129748DB603DEB9D72FCAEA4375<br>3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4<br>853985D2A30CBAF89A21A0198B63475D3FE50718E9D6A28948E604578DFF4CA5<br>CA79C0C2A3F3C80BB8DFE22F0E3E4EEE778E8AFFA095BF25F7A76A14AF40B5B0<br>4F3F8F99DDECA9006024287F7A1DCA881AD2784F15FE055040B23AE743F372E9<br>8341BAAB4C8A940C780FBF2D427026616D3ED76B8C7568448F09768F35887BCC<br>3242E0A736EF8AC90430A9F272FF30A81E2AFC146FCB84A25C6E56E8192791E4 |
| **IoC URL** |
| http://54.242.169.255/imbox/?mail/u/0/#inbox/FMfcgxwLtkcJcn |

| |
|---|
| BvtbzkZMVxLsXfPCXv |
| https://dkloja.com.br/signup/file/10f3eZ79s5091ks202Ns.zip |
| **Enlaces para revisar el informe:** |
| https://www.csirt.gob.cl/alertas/2cmv22-00287-01/ |
| https://www.csirt.gob.cl/media/2022/03/2CMV22-00287-01.pdf |


| **CSIRT advierte campaña de malware donde se suplanta al Banco BBVA** | |
|---|---|
| Alerta de seguridad cibernética | 2CMV21-00288-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de marzo de 2022 |
| Última revisión | 24 de marzo de 2022 |
| **Indicadores de compromiso** | |
| **IP** | |
| [185.222.57.234] | |
| **SHA256** | |
| 0BC9EF8BE73524879B6B4556A3C290F52AB85873C94BA162309F7FE1BABB0E75<br>863712C3E12EFDD3FB492246FA8D8BEFF075D766886DF80FF17F4E4C881B7A2D | |
| **IoC URL** | |
| http://45.137.22.122/Oclxocw_Tjrwpzom.png | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/2cmv22-0288-01/ | |
| https://www.csirt.gob.cl/media/2022/03/2CMV22-00288-01.pdf | |

# Vulnerabilidades


| CSIRT alerta de vulnerabilidades que afectan a productos de Red Hat | |
|---|---|
| Alerta de seguridad cibernética | 9VSA22-00597-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de marzo de 2022 |
| Última revisión | 22 de marzo de 2022 |
| **CVE** | |
| CVE-2022-25235<br>CVE-2022-25236<br>CVE-2022-25315 | |
| **Fabricante** | |
| Red Hat | |
| **Productos afectados** | |
| Red Hat Enterprise Linux for x86_64 – Extended Update Support 8.4 x86_64<br>Red Hat Enterprise Linux Server – AUS 8.4 x86_64<br>Red Hat Enterprise Linux for IBM z Systems – Extended Update Support 8.4 s390x<br>Red Hat Enterprise Linux for Power, little endian – Extended Update Support 8.4 ppc64le<br>Red Hat Enterprise Linux Server – TUS 8.4 x86_64<br>Red Hat Enterprise Linux for ARM 64 – Extended Update Support 8.4 aarch64<br>Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions 8.4 ppc64le<br>Red Hat Enterprise Linux Server – Update Services for SAP Solutions 8.4 x86_64 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00597-01/ | |
| https://www.csirt.gob.cl/media/2022/03/9VSA22-00597-01.pdf | |


| CSIRT alerta de vulnerabilidades en McAfee ePO | |
|---|---|
| Alerta de seguridad cibernética | 9VSA22-00598-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Bajo |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de marzo de 2022 |
| Última revisión | 23 de marzo de 2022 |
| **CVE** | |
| CVE-2022-0842<br>CVE-2022-0857<br>CVE-2022-0858<br>CVE-2022-0859<br>CVE-2022-0861<br>CVE-2022-0862 | |
| **Fabricante** | |
| McAfee | |
| **Productos afectados** | |
| ePO 5.10.0 anteriores a CU 13 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00598-01/ | |
| https://www.csirt.gob.cl/media/2022/03/9VSA22-00598-01.pdf | |


| CSIRT alerta de vulnerabilidades en impresoras HP | |
|---|---|
| Alerta de seguridad cibernética | 9VSA22-00599-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 24 de marzo de 2022 |
| Última revisión | 24 de marzo de 2022 |
| **CVE** | |
| CVE-2022-24291<br>CVE-2022-24292<br>CVE-2022-24293<br>CVE-2022-24294 | |
| **Fabricante** | |
| HP | |
| **Productos afectados** | |
| HP Color LaserJet Pro, LaserJet Pro, PageWide, PageWide Pro y OfficeJet Pro. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00599-01-csirt/ | |
| https://www.csirt.gob.cl/media/2022/03/9VSA22-00599-01.pdf | |

# Noticias

## Ingrid Inda asume como nueva jefa de la División de Redes y Seguridad Informática de la Subsecretaría del Interior

Con vasta experiencia y éxito en el manejo y gestión de procesos y proyectos con componentes tecnológicas en la Administración Pública, Ingrid Inda Camino asumió el viernes 11 de marzo el desafío de liderar la División de Redes y Seguridad Informática, perteneciente al Ministerio del Interior.

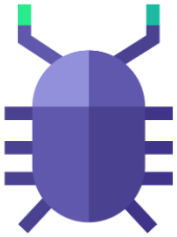
Inda es Ingeniera en Informática de la Universidad de Santiago de Chile. Entre los años 2006 y 2010 y de 2014 a 2018 se desempeñó en este mismo cargo, teniendo un importante rol al formar parte de varios comités relacionados con ciberseguridad. Fue así como participó del comité encargado de la adhesión de Chile al Convenio de Budapest, fue integrante del Comité Interministerial de Ciberseguridad, que tuvo por misión la generación de la Política Nacional de Ciberseguridad en 2017 y lideró el Comité Asesor de Ciberseguridad del Ministerio del Interior y Seguridad Pública.

Así también, estuvo a cargo del Programa Red de Conectividad del Estado (RCE) que enlaza en una red de 10GB a todos los ministerios y principales servicios del Estado, entregando servicios de monitoreo NOC/SOC, Internet y seguridad (alerta y atención a incidentes) a través del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno).

Posteriormente, sus conocimientos e intereses la llevaron al área académica, integrándose a la Universidad SEK como jefa de la carrera de Ingeniería de Ciberseguridad, y en marzo de 2022 vuelve a integrarse al Ministerio del Interior, como parte de la presidencia de Gabriel Boric.

“Estoy muy contenta y agradecida de la confianza que ha puesto en mí la nueva autoridad y de volver a la División de Redes y Seguridad Informática. Mi objetivo es velar por el adecuado funcionamiento de las redes del Estado y de potenciar aún más la ciberseguridad en nuestro país. Dentro de los proyectos y objetivos que tenemos para el CSIRT de Gobierno está el capacitar a los funcionarios del Estado en ciberseguridad, formar alianzas con entidades educativas, estar atentos a los proyectos de Ley que hoy se discuten en el Senado en materia de ciberseguridad y protección de datos, y el potenciamiento de la Política Nacional de Ciberseguridad, para involucrar a aquellos actores que aún no se suman y así generar alianzas que nos permitan construir entre todos una cultura potente y robusta de ciberseguridad”, asegura Inda.

## CSIRT alerta que ransomware Avoslocker está siendo usado para atacar máquinas VMware



El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comunica el reciente surgimiento de una campaña con una variante Linux del ransomware conocido como AvosLocker, que apunta a las máquinas virtuales VMware ESXi y a los archivos VMFS (Virtual Machine File System). Se conoce de al menos una víctima que recibió la exigencia de US$ 1 millón como extorsión a cambio de desencriptar sus archivos y no divulgar su información confidencial.

Atacar a las máquinas virtuales es cada día más valioso para los ciberdelincuentes, ya que cada día más empresas las usan en sus operaciones. Además, basta un solo comando para encriptar varios servidores. Ya desde octubre se han apreciado campañas similares que cifran tanto sistemas Linux en general como específicamente los de VMware, por parte de bandas que incluyen a REvil, Babuk, Mespinoza, GoGoogle, DarkSide, RansomExx/Defray y Hello Kitty.

### Modo de operación

Esta campaña de ransomware no está explotando una vulnerabilidad específica de los productos VMware, sino que usando Proxyshell para aprovechar vulnerabilidades conocidas en sistemas de Microsoft[2], como CVE-2021-34473[3], CVE-2021-31206, CVE-2021-34523 y CVE-2021-31207[4].

Cuando es lanzado en un sistema Linux, AvosLocker baja todas las máquinas ESXi en el servidor. Cuando empieza a trabajar en el sistema comprometido, el ransomware agrega la extensión .avoslinux a los archivos encriptados. También deja notas indicando que no se apaguen los computadores para evitar la corrupción de sus datos y que visiten un sitio de la red Tor para tener más datos sobre cómo pagar el rescate.

De acuerdo con Sophos[5], para poder desplegar su ransomware, los atacantes usan la herramienta PDQ Deploy, con scripts que pueden deshabilitar en segundos los productos de seguridad que se pueden ejecutar en modo seguro, deshabilitar Windows Defender y permitir que AnyDesk del delincuente se ejecute en modo seguro. Los scripts también conectan al controlador de dominio del objetivo para acceder a él de forma remota y ejecutar el ransomware.

Información oficial entregada por VMware, que comparte además indicadores de compromiso: https://blogs.vmware.com/security/2022/02/avoslocker-modern-linux-ransomware-threats.html

Más información aquí: https://www.csirt.gob.cl/noticias/csirt-ransomware-avoslocker/

# Actualidad

## Ciberguía | ¿Cómo identificar un phishing?

El aumento de las transacciones bancarias que hoy se realizan a través de internet no sólo ha significado comodidad para los clientes, sino que también han redundado en un incremento de su atractivo para los ciberdelincuentes, que tienen en la falsificación de las webs bancarias y de sus métodos de comunicación digital una oportunidad real de adueñarse no solo de los datos privados de las personas, sino también de sus cuentas bancarias.

Para realizar estos fraudes, los delincuentes requieren solo armar una página web y correos electrónicos o mensajes de texto para producir el engaño. Por eso, los mensajes fraudulentos son incesantes y, pese a que los bancos, el CSIRT de Gobierno y otras instituciones trabajamos permanentemente para advertir de ellos y bloquearlos, es indispensable que como usuarios estemos atentos a estos intentos de engaño y sepamos cómo no caer en ellos.

***Descarga la ciberguía aquí:*** https://www.csirt.gob.cl/recomendaciones/ciberguia-como-identificar-un-phishing/

## 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 (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.

- Reynaldo Araya
- Manuel Carvajal
- Palmira Armijo
- Matías Peña
- Carolina Lara
- Juan Alfonso Muñoz
- Paola García
- Ernesto Riquelme
- Darling Dávila
- Mario Rojas
- Víctor Cofré
- Matías Peña
- Patricio Muñoz