Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

07-05-2021 | Año 3 | N°96

# Boletín de Seguridad Cibernética

Semana del 30 de abril al 06 de mayo de 2021

# La semana en cifras

**Hash**

0

**SHA**

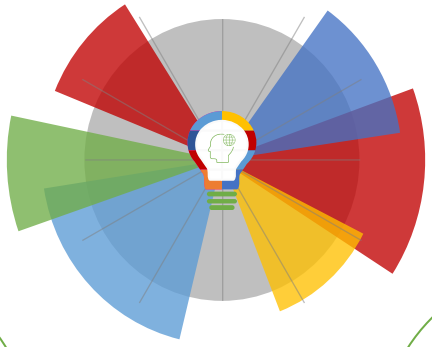
Asociadas a múltiples campañas de phishing con archivos que contienen malware

**Se advirtieron**

6

**URL**

Asociadas a sitios fraudulentos y campañas de phishing



**Parches**

59

**para vulnerabilidades**

Las mitigaciones son útiles en productos de Parallels Desktop, F5, Apple, WordPress, Mozilla, Dell, IBM y Cisco.

**IP**

5

**Informadas**

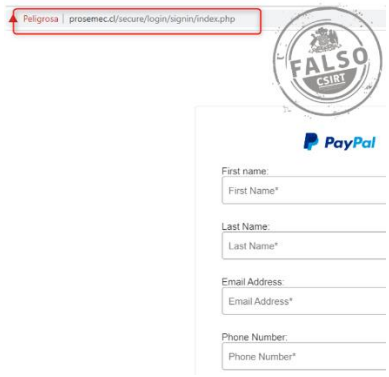
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

# Contenido

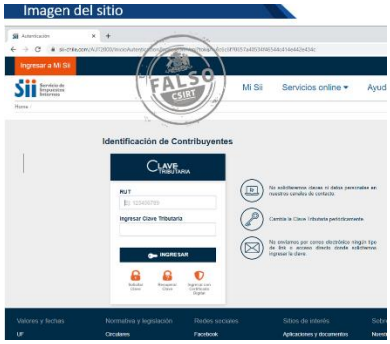
# Sitios fraudulentos

Imagen del sitio




| CSIRT alerta por sitio que suplanta a Paypal | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00942-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 30 de abril de 2021 |
| Última revisión | 30 de abril de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://prosemec[.]cl/secure/signin/index.php | |
| IP | |
| [131.72.236.173] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00942-01/ | |
| https://www.csirt.gob.cl/media/2021/04/8FFR21-00942-01.pdf | |

Imagen del sitio



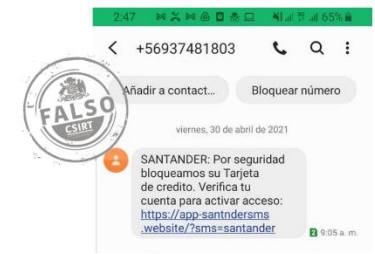

| CSIRT alerta por sitio fraudulento que suplanta al SII | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00943-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 30 de abril de 2021 |
| Última revisión | 30 de abril de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://sii-chile[.]com/AUT2000/InicioAutenticacion/IngresoSII.html?token=6c6c6f70657a40534f46544c414e442e434c | |
| IP | |
| [69.164.215.190] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00943-01/ | |
| https://www.csirt.gob.cl/media/2021/04/8FFR21-00943-01.pdf | |


| CSIRT alerta por sitio fraudulento que suplanta a Netflix | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00944-01 |
| 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 2021 |
| Última revisión | 3 de mayo de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://www.herreriaaconcagua[.]cl/login/vercheck/flixnet/Verify.php | |
| IP | |
| [186.64.117.195] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00944-01/ | |
| https://www.csirt.gob.cl/media/2021/05/8FFR21-00944-01.pdf | |


| CSIRT alerta de sitio fraudulento que suplanta a Microsoft Excel | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00945-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 5 de mayo de 2021 |
| Última revisión | 5 de mayo de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| http://dentalmanager[.]cl/pager/page.php | |
| IP | |
| [162.241.157.42] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00945-01/ | |
| https://www.csirt.gob.cl/media/2021/05/8FFR21-00945-01.pdf | |

# Phishing

Imagen del mensaje




| CSIRT alerta por smishing que suplanta al Banco Santander | |
|---|---|
| Alerta de seguridad cibernética | 8FPH21-00397-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 3 de mayo de 2021 |
| Última revisión | 3 de mayo de 2021 |
| **Indicadores de compromiso** | |
| URL de SMS | |
| https://app-santandersms[.]website/?sms=santander | |
| URL sitio falso | |
| https://smsvalida-santder[.]site/1619808193/personas/index.asp | |
| IP | |
| [198.54.125.152] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8fph21-00397-01/ | |
| https://www.csirt.gob.cl/media/2021/05/8FPH21-00397-01.pdf | |

# Vulnerabilidades


| CSIRT alerta por vulnerabilidades zero day en Parallels Desktop | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00434-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Crítico |
| TLP | Blanco |
| Fecha de lanzamiento original | 1 de mayo de 2021 |
| Última revisión | 1 de mayo de 2021 |
| **CVE** | |
| CVE-2021-31424<br>CVE-2021-31427 | |
| **Fabricante** | |
| Parallels Desktop | |
| **Productos afectados** | |
| Parallels Desktop 15.1.5-47309 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00434-01 | |
| https://www.csirt.gob.cl/media/2021/05/9VSA21-00434-01.pdf | |


| CSIRT advierte de vulnerabilidades en WordPress | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00435-01 |
| 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 2021 |
| Última revisión | 3 de mayo de 2021 |
| **CVE** | |
| CVE-2021-29447<br>CVE-2021-29450 | |
| **Fabricante** | |
| WordPress | |
| **Productos afectados** | |
| WordPress, versiones de la 4.7 a la 5.7. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00435-01 | |
| https://www.csirt.gob.cl/media/2021/05/9VSA21-00435-01.pdf | |


| CSIRT advierte de vulnerabilidades en productos de Apple | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00436-01 |
| 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 2021 |
| Última revisión | 3 de mayo de 2021 |
| **CVE** | |
| CVE-2021-30665<br>CVE-2021-30666<br>CVE-2021-30661<br>CVE-2021-30663 | |
| **Fabricante** | |
| Apple | |
| **Productos afectados** | |
| iPadOS, versiones de la 14.0 18A373 a la 14.5 18E199.<br>Apple iOS de la 12.0 16A366 a la 14.5 18E199.<br>watchOS 7.0 18R382 a la 7.4 18T195. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00436-01 | |
| https://www.csirt.gob.cl/media/2021/05/9VSA21-00436-01.pdf | |


| CSIRT alerta por vulnerabilidad grave en BIG-IP APM de F5 | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00437-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 4 de mayo de 2021 |
| Última revisión | 4 de mayo de 2021 |
| **CVE** | |
| CVE-2021-23008 | |
| **Fabricante** | |
| F5 | |
| **Productos afectados** | |
| BIG-IP APM 11.5.2 a 16.0.1.1 2. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00437-01 | |
| https://www.csirt.gob.cl/media/2021/05/9VSA21-00437-01.pdf | |


| CSIRT advierte de vulnerabilidades en productos de Apple | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00438-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 5 de mayo de 2021 |
| Última revisión | 5 de mayo de 2021 |
| **CVE** | |
| CVE-2021-29952<br>CVE-2021-29953 | |
| **Fabricante** | |
| Apple | |
| **Productos afectados** | |
| Mozilla Firefox 80.0 a 88.0.<br>Mozilla Firefox para Android 80.1.2 a 88.1.2 | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00438-01 | |
| https://www.csirt.gob.cl/media/2021/05/9VSA21-00438-01.pdf | |


| CSIRT alerta por vulnerabilidad grave en productos Dell | | |
|---|---|---|
| Alerta de seguridad cibernética | 9VSA21-00432-01 | |
| Clase de alerta | Vulnerabilidad | |
| Tipo de incidente | Sistema y/o Software Abierto | |
| Nivel de riesgo | Crítico | |
| TLP | Blanco | |
| Fecha de lanzamiento original | 5 de mayo de 2021 | |
| Última revisión | 5 de mayo de 2021 | |
| **CVE** | | |
| CVE-2021-21551 | | |
| **Fabricante** | | |
| Citrix | | |
| **Productos afectados** | | |
| ChengMing 3967, versión 1.11.0<br>ChengMing 3977 1.11.0<br>ChengMing 3980 2.17.0<br>ChengMing 3988 1.5.0<br>ChengMing 3990 1.3.1<br>ChengMing 3991 1.3.1<br>Dell G15 5510 1.3.1<br>Dell G3 3500 1.7.1<br>Dell G3 3579 1.14.0<br>Dell G3 3779 1.14.0 | Latitude 5591 1.14.1<br>Latitude 7200 2-in-1 1.10.1<br>Latitude 7210 2 in 1 1.5.1<br>Latitude 7275 1.9.0<br>Latitude 7280 1.20.2<br>Latitude 7290 1.18.0<br>Latitude 7300 1.12.0<br>Latitude 7310 1.5.1<br>Latitude 7320 1.5.0<br>Latitude 7370 1.22.3<br>Latitude 7380 1.20.2 | **También se ven afectadas las siguientes plataformas al fin de su ciclo de vida**<br><br>Alienware 14<br>Alienware 17 51m r2<br>Alienware Area 51<br>Alienware M14xr2<br>Alienware M15 R4<br>Alienware M17xr4<br>Alienware M18xr2<br>Asm100 |

| | | |
|---|---|---|
| Dell G5 5000 1.1.0 | Latitude 7389 1.22.2 | Asm100r2 |
| Dell G5 5090 1.4.0 | Latitude 7390 1.18.0 | Cheng Ming 3967 |
| Dell G5 5500 1.7.1 | Latitude 7390 2-in-1 1.17.0 | Dell Canvas |
| Dell G5 5587 1.15.0 | Latitude 7400 1.12.0 | Dell Latitude 14 Rugged Extreme |
| Dell G5 5590 1.14.0 | Latitude 7400 2in1 1.10.0 | Inspiron 1122 |
| Dell G7 7500 1.6.0 | Latitude 7410 1.5.1 | Inspiron 11-3162 |
| Dell G7 7588 1.15.0 | Latitude 7420 1.5.0 | Inspiron 1210 |
| Dell G7 7590 1.14.0 | Latitude 7480 1.20.2 | Inspiron 14-3452 |
| Dell G7 7700 1.6.0 | Latitude 7490 1.18.0 | Inspiron 14-5459 |
| Dell G7 7790 1.14.0 | Latitude 7520 1.5.0 | Inspiron 15-3552 |
| Dell Gaming G3 3590 1.12.0 | Latitude 9410 1.5.1 | Inspiron 1545 |
| Dell Precision 3430 Tower 1.10.0 | Latitude 9510 1.4.2 | Inspiron 15-5559 |
| Dell Precision 3430 XL 1.10.0 | Latitude E5270 1.24.3 | Inspiron 15-5565 |
| Dell Precision 3431 Tower 1.7.2 | Latitude E5470 1.24.3 | Inspiron 1564 |
| Dell Precision 3630 Tower 2.7.0 | Latitude E5570 1.24.3 | Inspiron 15z |
| Dell Precision 3930 Rack 2.10.0 | Latitude E7270 1.27.3 | Inspiron 17-5759 |
| Dell Precision 3930 XL Rack 2.10.0 | Latitude E7270 mobile thin client 1.20.3, | Inspiron 20-3052 |
| Dell Precision 5820 Tower 2.8.0 | Latitude E7470 1.27.3 | Inspiron 2330 |
| Dell Precision 7820 Tower 2.12.0 | Latitude Rugged 5420 1.12.0 | Inspiron 24-3452 |
| Dell Precision 7820 XL Tower .12.0 | Latitude Rugged 5424 1.12.0 | Inspiron 24-3455 |
| Dell Precision 7920 Tower 2.12.0 | Latitude Rugged 7424 1.12.0 | Inspiron 24-5475 |
| Dell Precision 7920 XL Tower 2.12.0 | Latitude Rugged Extreme 7424 1.12.0 | Inspiron 3043 |
| Embedded Box PC 5000 1.9.1 | Latitude Rugged Extreme Tablet 7220 1.9.1 | Inspiron 3048 |
| Inspiron 13 5370 1.17.0 | Latitude Rugged Extreme Tablet 7220EX 1.9.1 | Inspiron 3147 |
| Inspiron 14 (5468) 1.13.1 | OptiPlex 3040 1.14.2 | Inspiron 3157 |
| Inspiron 14 (7460) 1.14.1 | OptiPlex 3046 1.11.1 | Inspiron 3168 |
| Inspiron 14 Gaming (7466) 1.8.0 | OptiPlex 3050 1.15.1 | Inspiron 3252 |
| Inspiron 14 Gaming (7467) 1.13.1 | OptiPlex 3050 AIO 1.16.1 | Inspiron 3421 |
| Inspiron 15 (5566) 1.13.1 | OptiPlex 3060 1.9.1 | Inspiron 3437 |
| Inspiron 15 (5567) 1.4.1 | OPTIPLEX 3070 1.7.0 | Inspiron 3442 |
| Inspiron 15 (7560) | OptiPlex 3080 1.3.1 | Inspiron 3443 |
| | OptiPlex 3090 Ultra 1.0.10 | Inspiron 3520 |
| | OptiPlex 3240 All-in- | Inspiron 3521 |
| | | Inspiron 3537 |
| | | Inspiron 3542 |
| | | Inspiron 3543 |
| | | Inspiron 3646 |
| | | Inspiron 3647 |
| | | Inspiron 3655 |
| | | Inspiron 3656 |
| | | Inspiron 3847 |
| | | Inspiron 5323 |
| | | Inspiron 5348 |
| | | Inspiron 5423 |
| | | Inspiron 5443 |
| | | Inspiron 5448 |
| | | Inspiron 5485 2n1 |
| | | Inspiron 5520 |
| | | Inspiron 5521 |
| | | Inspiron 5537 |

| | | |
|---|---|---|
| 1.14.1 | One 1.11.1 | Inspiron 5543 |
| Inspiron 15 (7572) 1.6.1 | OPTIPLEX 3280 AIO 1.3.1 | Inspiron 5548 |
| Inspiron 15 5582 2-in-1 2.9.0 | OptiPlex 5040 1.17.1 | Inspiron 5576 |
| Inspiron 15 Gaming (7566) 1.8.0 | OptiPlex 5050 1.15.1 | Inspiron 5577 |
| Inspiron 15 Gaming (7567) 1.13.1 | OptiPlex 5055 A-Serial 1.2.9 | Inspiron 5676 |
| Inspiron 15 Gaming (7577) 1.12.1 | OptiPlex 5055 Ryzen APU 1.2.8 | Inspiron 5737 |
| Inspiron 17 (5767) 1.4.1 | OptiPlex 5055 Ryzen CPU 1.1.20 | Inspiron 5749 |
| Inspiron 3268 1.15.0 | OptiPlex 5060 1.9.1 | Inspiron 580s |
| Inspiron 3470 2.17.0 | OptiPlex 5070 1.7.0 | Inspiron 620 |
| Inspiron 3471 1.5.0 | OptiPlex 5080 1.3.10 | Inspiron 660 |
| Inspiron 3480 1.12.0 | OptiPlex 5250 All-in-One 1.16.1 | Inspiron 660s |
| Inspiron 3481 1.11.0 | OptiPlex 5260 All-In-One 1.12.0 | Inspiron 7359 |
| Inspiron 3490 1.10.0 | OptiPlex 5270 AIO 1.7.0 | Inspiron 7368 |
| Inspiron 3493 1.12.0 | OptiPlex 5480 AIO 1.4.0 | Inspiron 7437 |
| Inspiron 3501 1.4.0 | OptiPlex 7040 1.19.0 | Inspiron 7520 |
| Inspiron 3580 1.12.0 | OptiPlex 7050 1.15.1 | Inspiron 7537 |
| Inspiron 3581 1.11.0 | OptiPlex 7060 1.9.1 | Inspiron 7548 |
| Inspiron 3583 1.12.0 | OptiPlex 7070 1.7.2 | Inspiron 7558 |
| Inspiron 3584 1.11.0 | OptiPlex 7070 Ultra 1.7.0 | Inspiron 7559 |
| Inspiron 3590 1.10.0 | OptiPlex 7071 1.7.2 | Inspiron 7720 |
| Inspiron 3593 1.12.0 | OptiPlex 7080 1.13.0 | Inspiron 7737 |
| Inspiron 3668 1.15.0 | OptiPlex 7090 Ultra 1.0.10 | Inspiron 7746 |
| Inspiron 3670 2.17.0 | OptiPlex 7440 AIO 1.14.1 | Inspiron One 19 |
| Inspiron 3671 1.5.0 | OptiPlex 7450 All-In-One 1.16.1 | Inspiron One 2020 |
| Inspiron 3780 1.12.0 | OptiPlex 7460 All-In-One 1.12.0 | Latitude 3150 |
| Inspiron 3781 1.11.0 | OPTIPLEX 7470 AIO 1.7.0 | Latitude 3160 |
| Inspiron 3790 1.10.0 | OPTIPLEX 7480 AIO 1.6.2 | Latitude 3310 2in1 |
| Inspiron 3793 1.12.0 | OptiPlex 7760 AIO 1.12.0 | Latitude 3330 |
| Inspiron 3880 1.3.1 | OPTIPLEX 7770 AIO 1.7.0 | Latitude 3340 |
| Inspiron 3881 1.3.1 | OPTIPLEX 7780 AIO 1.6.2 | Latitude 3350 |
| Inspiron 3891 1.0.2 | OptiPlex XE3 1.9.1 | Latitude 3440 |
| Inspiron 5300 1.5.0 | Precision 17 M5750 | Latitude 3450 |
| Inspiron 5301 1.6.1 | | Latitude 3460 |
| Inspiron 5390 1.10.0 | | Latitude 3460 Wyse Tc |
| Inspiron 5391 1.11.0 | | Latitude 3550 |
| Inspiron 5400 2-in-1 1.5.0 | | Latitude 3560 |
| Inspiron 5400 AIO 1.3.1 | | Latitude 5250 |
| Inspiron 5401 1.5.1 | | Latitude 5285 |
| Inspiron 5402 1.4.1 | | Latitude 5450 |
| Inspiron 5406 2-in-1 1.4.1 | | Latitude 5520 |
| Inspiron 5408 1.5.1 | | Latitude 5550 |
| Inspiron 5409 1.4.1 | | Latitude 7285 |
| | | Latitude 7350 |
| | | Latitude E5420 |
| | | Latitude E5430 |
| | | Latitude E5440 |
| | | Latitude E5530 |
| | | Latitude E5540 |
| | | Latitude E6220 |
| | | Latitude E6230 |
| | | Latitude E6320 |

| | | |
|---|---|---|
| Inspiron 5480 2.9.0 | 1.7.2 | Latitude E6330 |
| Inspiron 5481 2-in-1 2.9.0 | Precision 3240 CFF 1.4.0 | Latitude E6430 |
| Inspiron 5482 2.9.0 | Precision 3420 Tower 2.17.1 | Latitude E6430 Atg |
| Inspiron 5490 1.12.0 | Precision 3440 1.13.0 | Latitude E6440 |
| Inspiron 5490 AIO 1.7.0 | Precision 3510 1.24.3 | Latitude E6530 |
| Inspiron 5491 2-in-1 1.8.1 | Precision 3520 1.19.3 | Latitude E6540 |
| Inspiron 5493 1.12.0 | Precision 3530 1.14.1 | Latitude E7240 |
| Inspiron 5494 1.10.0 | Precision 3540 1.10.1 | Latitude E7250 |
| Inspiron 5498 1.12.0 | Precision 3541 1.11.1 | Latitude E7270 Wyse Tc |
| Inspiron 5501 1.5.1 | Precision 3550 1.5.1 | Latitude E7440 |
| Inspiron 5502 1.4.1 | Precision 3551 1.4.3 | Latitude E7450 |
| Inspiron 5508 1.5.1 | Precision 3560 1.5.1 | Latitude Xt3 |
| Inspiron 5509 1.4.1 | Precision 3620 Tower 2.17.1 | OptiPlex 3010 |
| Inspiron 5570 1.4.1 | Precision 3640 1.4.3 | OptiPlex 3011 AIO |
| Inspiron 5580 2.9.0 | Precision 5510 1.16.1 | OptiPlex 3020 |
| Inspiron 5583 1.12.0 | Precision 5520 1.22.1 | OptiPlex 3030 AIO |
| Inspiron 5584 1.12.0 | Precision 5530 1.18.1 | OptiPlex 390 |
| Inspiron 5590 1.12.0 | Precision 5530 2-in-1 1.12.9 | OptiPlex 5055 |
| Inspiron 5591 2-in-1 1.8.1 | Precision 5540 1.9.1 | OptiPlex 7010 |
| Inspiron 5593 1.12.0 | Precision 5550 1.7.1 | OptiPlex 7020 |
| Inspiron 5594 1.10.0 | Precision 5720 AIO 2.8.1 | OptiPlex 7090 Ultra |
| Inspiron 5598 1.12.0 | Precision 5820 XL Tower 2.8.0 | OptiPlex 780 |
| Inspiron 5770 1.4.1 | Precision 7520 1.19.2 | OptiPlex 790 |
| Inspiron 7300 1.6.1 | Precision 7530 1.15.3 | OptiPlex 9010 |
| Inspiron 7300 2-in-1 1.2.4 | Precision 7540 1.11.2 | OptiPlex 9020 |
| Inspiron 7306 2-in-1 1.4.1 | Precision 7550 1.6.2 | OptiPlex 9030 AIO |
| Inspiron 7380 1.12.0 | Precision 7720 1.19.2 | OptiPlex 990 |
| Inspiron 7386 1.9.0 | Precision 7730 1.15.3 | OptiPlex Fx130 |
| Inspiron 7390 1.11.0 | Precision 7740 1.11.2 | OptiPlex Fx170 |
| Inspiron 7391 1.11.0 | Precision 7750 1.6.2 | OptiPlex Xe2 |
| Inspiron 7391 2-in-1 1.9.1 | Vostro 13 5370 1.17.0 | Precision 7510 |
| Inspiron 7400 1.6.1 | Vostro 14 (5468) 1.14.1 | Precision 7710 |
| Inspiron 7472 1.6.1 | Vostro 14 5471 1.17.0 | Precision M4600 |
| Inspiron 7490 1.6.0 | Vostro 15 (5568) 1.14.1 | Precision M4700 |
| Inspiron 7500 1.5.1 | Vostro 15 7570 1.12.1 | Precision M6600 |
| Inspiron 7500 2-in-1 Black 1.2.4 | Vostro 15 7580 G-Series 1.15.0 | Precision M6700 |
| Inspiron 7500 2-in-1 Silver 1.5.0 | Vostro 3070 2.17.0 | Precision R5500 |
| Inspiron 7501 1.5.1 | Vostro 3267 1.15.1 | Precision T1700 |
| Inspiron 7506 2-in-1 1.4.1 | Vostro 3268 1.15.1 | Precision T3500 |
| Inspiron 7580 1.12.0 | Vostro 3400 1.4.0 | Precision T3600 |
| Inspiron 7586 1.9.0 | Vostro 3401 1.1.0 | Precision T3610 |
| | Vostro 3470 2.17.0 | Precision T5500 |
| | Vostro 3471 1.5.0 | Precision T5600 |
| | Vostro 3480 1.12.0 | Precision T5610 |
| | | Precision T5810 |
| | | Precision T7500 |
| | | Precision T7600 |
| | | Precision T7610 |
| | | Precision T7810 |
| | | Precision T7910 |

| | | |
|---|---|---|
| Inspiron 7590 1.8.0 | Vostro 3481 1.11.0 | Vostro 14 3458 |
| Inspiron 7590 2-in-1 1.11.0 | Vostro 3490 1.10.0 | Vostro 14-3446 |
| Inspiron 7591 1.8.0 | Vostro 3491 1.15.0 | Vostro 1450 |
| Inspiron 7591 2-in-1 1.9.1 | Vostro 3500 1.4.0 | Vostro 14-5459 |
| Inspiron 7700 1.3.1 | Vostro 3501 1.1.0 | Vostro 15 3561 |
| Inspiron 7706 2-in-1 1.4.1 | Vostro 3580 1.12.0 | Vostro 1550 |
| Inspiron 7786 1.9.0 | Vostro 3581 1.11.0 | Vostro 20 3052 |
| Inspiron 7790 1.7.0 | Vostro 3583 1.12.0 | Vostro 20 3055 |
| Inspiron 7791 1.9.1 | Vostro 3584 1.11.0 | Vostro 220s |
| Inspiron 5491 AIO 1.7.0 | Vostro 3590 1.10.0 | Vostro 230 |
| Latitude 12 7285 1.9.2 | Vostro 3591 1.15.0 | Vostro 2521 |
| Latitude 12 Rugged Extreme 7214 1.28.0 | Vostro 3660 1.15.1 | Vostro 260 |
| Latitude 12 Rugged Tablet 7212 1.31.2 | Vostro 3667 1.15.1 | Vostro 270 |
| Latitude 14 Rugged 5414 1.28.0 | Vostro 3668 1.15.1 | Vostro 270s |
| Latitude 14 Rugged Extreme 7414 1.28.0 | Vostro 3669 1.15.1 | Vostro 3010 |
| Latitude 3120 1.0.5 | Vostro 3670 2.17.0 | Vostro 3252 |
| Latitude 3180 1.13.2 | Vostro 3671 1.5.0 | Vostro 3560 |
| Latitude 3189 1.13.2 | Vostro 3681 1.3.1 | Vostro 3800 |
| Latitude 3190 1.13.1 | Vostro 3690 1.0.2 | Vostro 3900 |
| Latitude 3190 2-in-1 1.13.1 | Vostro 3881 1.3.1 | Vostro 3900g |
| Latitude 3300 1.10.1 | Vostro 3888 1.3.1 | Vostro 3901 |
| Latitude 3301 1.13.0 | Vostro 3890 1.0.2 | Vostro 3902 |
| Latitude 3310 1.8.3 | Vostro 5090 1.5.0 | Vostro 3905 |
| Latitude 3310 2-in-1 1.17.1 | Vostro 5300 1.5.0 | Vostro 470 |
| Latitude 3380 1.13.1 | Vostro 5301 1.6.1 | Vostro 5480 |
| Latitude 3390 1.14.2 | Vostro 5390 1.10.0 | XPS 13 9343 |
| Latitude 3400 1.16.0 | Vostro 5391 1.11.0 | XPS 8700 |
| Latitude 3410 1.5.1 | Vostro 5401 1.5.3 | XPS 9350 |
| Latitude 3470 1.19.0 | Vostro 5402 1.4.1 | XPS 9530 |
| Latitude 3480 1.15.1 | Vostro 5410 1.5.1 | XPS One 2710 |
| Latitude 3480 mobile thin client 1.15.1 | Vostro 5481 2.9.0 | XPS 13 9343 |
| Latitude 3490 1.14.1 | Vostro 5490 1.12.0 | XPS 8700 |
| Latitude 3500 1.16.0 | Vostro 5491 1.12.0 | XPS 9350 |
| Latitude 3510 1.5.1 | Vostro 5501 1.5.1 | XPS 9530 |
| Latitude 3570 1.19.0 | Vostro 5502 1.4.1 | XPS 9550 |
| Latitude 3580 1.15.1 | Vostro 5581 2.9.0 | XPS ONE 2710 |
| Latitude 3590 1.14.1 | Vostro 5590 1.12.0 | |
| Latitude 5175 1.8.1 | Vostro 5591 1.12.0 | |
| Latitude 5179 1.8.1 | Vostro 5880 1.3.0 | |
| | Vostro 5890 1.0.2 | |
| | Vostro 7500 1.5.1 | |
| | Vostro 7590 1.8.0 | |
| | Wyse 5070 1.9.0 | |
| | Wyse 5470 1.6.0 | |
| | Wyse 5470 All-In-One 1.7.0 | |
| | Wyse 7040 Thin Client 1.10.1 | |
| | XPS 12 (9250) 1.9.0 | |
| | XPS 13 (9360) 2.15.0 | |
| | XPS 13 (9370) 1.14.3 | |

| | | |
|---|---|---|
| Latitude 5200 1.14.0<br>Latitude 5280 1.19.3<br>Latitude 5280 mobile thin client 1.19.3<br>Latitude 5285 2-in-1 1.11.2<br>Latitude 5288 1.19.3<br>Latitude 5289 1.22.2<br>Latitude 5290 1.16.3<br>Latitude 5290 2-in-1 1.13.1<br>Latitude 5300 1.14.0<br>Latitude 5300 2-IN-1 1.14.0<br>Latitude 5310 1.5.2<br>Latitude 5310 2-in-1 1.5.2<br>Latitude 5320 1.14.0<br>Latitude 5320 2-in-1 1.14.0<br>Latitude 5400 1.10.1<br>Latitude 5401 1.11.1<br>Latitude 5410 1.5.1<br>Latitude 5411 1.4.3<br>Latitude 5420 1.5.2<br>Latitude 5480 1.19.3<br>Latitude 5488 1.19.3<br>Latitude 5490 1.16.3<br>Latitude 5491 1.14.1<br>Latitude 5495 1.4.0<br>Latitude 5500 1.10.1<br>Latitude 5501 1.11.1<br>Latitude 5510 1.5.1<br>Latitude 5511 1.4.3<br>Latitude 5520 1.5.1<br>Latitude 5580 1.19.3<br>Latitude 5590 1.16.3 | XPS 13 2-in-1 (9365) 2.15.0<br>XPS 13 7390 1.7.0<br>XPS 13 7390 2-in-1 1.7.1<br>XPS 13 9300 1.4.1<br>XPS 13 9305 1.0.5<br>XPS 13 9310 2.2.0<br>XPS 13 9310 2-in-1 2.2.1<br>XPS 13 9380 1.12.0<br>XPS 15 (9560) 1.22.0<br>XPS 15 2-in-1 (9575) 1.14.1<br>XPS 15 9500 1.7.1<br>XPS 15 9570 1.18.1<br>XPS 17 9700 1.7.2<br>XPS 27 AIO (7760) 2.8.1<br>XPS 7590 1.9.1<br>XPS 8900 2.9.1<br>XPS 8940 2.0.11<br>Dell Dock WD15 N/A<br>Dell Dock WD19 N/A<br>Dell Thunderbolt Dock TB16<br>Dell Thunderbolt Dock TB18DC | |
| **Enlaces para revisar el informe:** | | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00439-01 | | |
| https://www.csirt.gob.cl/media/2021/05/9VSA21-00439-01.pdf | | |


| CSIRT alerta de vulnerabilidad grave en IBM QRadar | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00440-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 6 de mayo de 2021 |
| Última revisión | 6 de mayo de 2021 |
| **CVE** | |
| CVE-2020-5013 | |
| **Fabricante** | |
| IBM | |
| **Productos afectados** | |
| IBM QRadar SIEM 7.3 y 7.4. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00440-01 | |
| https://www.csirt.gob.cl/media/2021/05/9VSA21-00440-01.pdf | |


| CSIRT alerta de vulnerabilidades en distintos productos de Cisco | | |
|---|---|---|
| Alerta de seguridad cibernética | 9VSA21-00441-01 | |
| Clase de alerta | Vulnerabilidad | |
| Tipo de incidente | Sistema y/o Software Abierto | |
| Nivel de riesgo | Alto | |
| TLP | Blanco | |
| Fecha de lanzamiento original | 6 de mayo de 2021 | |
| Última revisión | 6 de mayo de 2021 | |
| **CVE** | | |
| CVE-2021-1497 | CVE-2021-1284 | CVE-2021-1447 |
| CVE-2021-1498 | CVE-2021-1421 | CVE-2021-1234 |
| CVE-2021-1275 | CVE-2021-1400 | CVE-2021-1535 |
| CVE-2021-1468 | CVE-2021-1401 | CVE-2021-1514 |
| CVE-2021-1505 | CVE-2021-1509 | CVE-2021-1512 |
| CVE-2021-1506 | CVE-2021-1510 | CVE-2021-1515 |
| CVE-2021-1508 | CVE-2021-1511 | CVE-2021-1520 |
| CVE-2021-1426 | CVE-2021-1513 | CVE-2021-1521 |
| CVE-2021-1427 | CVE-2021-1490 | CVE-2021-1499 |
| CVE-2021-1428 | CVE-2021-1438 | CVE-2021-1516 |
| CVE-2021-1429 | CVE-2021-1507 | CVE-2021-1530 |
| CVE-2021-1430 | CVE-2021-1486 | CVE-2021-1519 |
| CVE-2021-1496 | CVE-2021-1478 | CVE-2020-3347 |
| CVE-2021-1363 | CVE-2021-1532 | CVE-2021-1493 |
| CVE-2021-1365 | | |
| **Fabricante** | | |
| Cisco | | |
| **Productos afectados** | | |
| Cisco HyperFlex HX | | |
| Cisco AnyConnect Secure Mobility Client for Windows | | |

| |
|---|
| Cisco SD-WAN vManage<br>Cisco SD-WAN vEdge<br>Cisco SD-WAN vBond Orchestrator Software<br>Cisco SD-WAN vEdge Cloud Routers<br>Cisco SD-WAN vEdge Routers<br>Cisco SD-WAN vManage Software<br>Cisco SD-WAN vSmart Controller Software<br>Cisco Unified Communications Manager IM & Presence Service<br>Cisco Unified Communications Manager (Unified CM)<br>Cisco Unified Communications Manager Session Management Edition (Unified CM SME)<br>Cisco Enterprise NFV Infrastructure<br>Cisco Small Business 100, 300 y 500 Series Wireless Access<br>Cisco Web Security Appliance<br>Cisco Wide Area Application Services<br>Cisco TelePresence Collaboration Endpoint (CE) Software<br>Cisco RoomOS Software<br>Cisco AsyncOS for Cisco Content Security Management Appliance (SMA)<br>Routers Cisco RV340, RV340W, RV345, y RV345P Dual WAN Gigabit VPN<br>Cisco Video Surveillance 8000 Series<br>Cisco Integrated Management Controller (IMC)<br>Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA)<br>Cisco Email Security Appliance (ESA)<br>Cisco Web Security Appliance (WSA)<br>Cisco BroadWorks Messaging Server Software<br>Cisco AnyConnect Secure Mobility Client para Windows, MacOS, y Linux anteriores al 4.10.00093<br>Cisco Webex Meetings Desktop App for Windows<br>Cisco Adaptive Security Appliance (ASA) Software<br>Cisco Firepower Threat Defense (FTD) |
| **Enlaces para revisar el informe:** |
| https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00441-01 |
| https://www.csirt.gob.cl/media/2021/05/9VSA21-00441-01.pdf |

# Actualidad

## Este 13 de mayo tiene lugar 8.8 Gobierno, con grandes invitados de Estonia, Israel, España y Latinoamérica e inscripción gratuita


En la primera 8.8 dedicada al trabajo de ciberseguridad y ciberinteligencia de los gobiernos e instituciones de carácter nacional, participarán representantes de algunos de los países más avanzados del mundo, tendrá lugar un potente panel protagonizado únicamente por mujeres en los más altos cargos de la materia en Latinoamérica, y una charla-taller a cargo del CCN de España.

**Las inscripciones ya se encuentran abiertas y son gratuitas**. Pueden hacerla en este enlace: https://www.passline.com/landing/88-computer-security-conference.

La apertura la hará el Ministro del Interior y Seguridad Pública, **Rodrigo Delgado**, además de contar con la participación de **Gabriel Bergel**, famoso hacker white hat y cofundador y CEO de 8.8. Participan con charlas el director del **CERT de Estonia, Tõnu Tammer**, representantes del **CERT de Israel** y del **Centro Criptológico Nacional (CCN) de España**, además del director nacional del CSIRT de Gobierno, **Carlos Landeros**.

También se presentará un panel con cinco mujeres líderes de la ciberseguridad latinoamericana: la secretaria ejecutiva del Comité Interamericano contra el Terrorismo de la OEA, **Alison Treppel**; la especialista líder en Modernización del BID, **María José Jarquín**; la directora general de Ciberseguridad y Protección de la Información de Paraguay, **Gabriela Ratti** y la directora del CERT Panamá, **Silvia Batista**. Además, **Mateo Martinez**, director de Krav Maga Hacking, analizará las

últimas fugas de datos en Latinoamérica, y el desarrollador argentino **Javier Smaldone** revisará las perspectivas del voto electrónico. Ambas charlas son parte del Call For Papers (CFP) de este evento.

El cierre del evento estará a cargo del Subsecretario del Interior, **Juan Francisco Galli**. Aquí pueden ver la agenda completa, con los invitados y los horarios de sus exposiciones:

## Ciberconsejos para no caer en estafas en este nuevo retiro de tu 10%

Ante la aprobación del tercer retiro del 10% de los ahorros previsionales, y el comienzo del trámite respectivo ante las AFP, compartimos estos útiles consejos para evitar las estafas tipo phishing que abundan en estas instancias: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-no-caer-en-estafas-en-este-nuevo-retiro-de-tu-10/.

## Ciberguía | Fake news: los peligros de la desinformación


Se aproxima una jornada eleccionaria que conmina a los chilenos a votar en cuatro sufragios diferentes. Ante esta definición clave, decidimos recordar a la población los peligros de las "fake news" y cómo reconocer ejemplos de mensajes de desinformación, con una didáctica ciberguía.

Lea y descargue la guía completa aquí: https://www.csirt.gob.cl/recomendaciones/ciberguia-fake-news-los-peligros-de-la-desinformacion/

# Recomendaciones y buenas prácticas

## Recomendaciones generales de seguridad

- 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 públicos 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 (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Jorge Muñoz
- Rosario Brovarone

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.07 13:23:38 -04'00'