Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

23-07-2021 | Año 3 | N°107

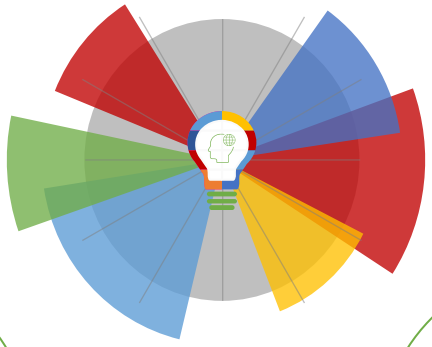
# Boletín de Seguridad Cibernética

Semana del 15 al 22 de julio de 2021

# La semana en cifras

**Hash**
116
**SHA**
Asociadas a múltiples campañas de phishing con archivos que contienen malware

**Se advirtieron**
3
**URL**
Asociadas a sitios fraudulentos y campañas de phishing



**Parches**
339
**para vulnerabilidades**
Las mitigaciones son útiles en productos de Oracle, Citrix, Fortinet, Windows, SonicWall y Google.

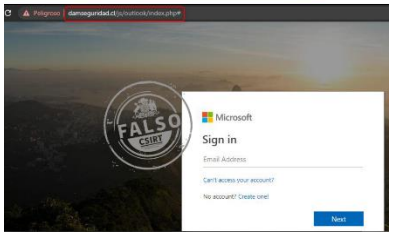
**IP**
80
**Informadas**
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

# Contenido

# Sitios fraudulentos

Imagen del sitio

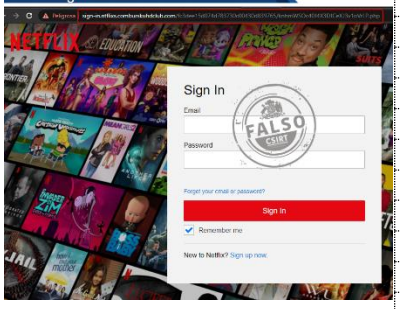



| CSIRT alerta de sitio fraudulento que suplanta a Microsoft | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00991-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 15 de julio de 2021 |
| Última revisión | 15 de julio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://damseguridad[.]cl/js/outlook/index.php# | |
| IP | |
| [186.64.114.60] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00991-01/ | |
| https://www.csirt.gob.cl/media/2021/07/8FFR21-00991-01.pdf | |

Imagen del sitio


| CSIRT alerta ante página fraudulenta que suplanta a Office 365 | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00992-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de julio de 2021 |
| Última revisión | 21 de julio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| http://www.segu[.]cl/templates/beez/ARK/MicrosoftAccount.html | |
| IP | |
| [201.236.101.198] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00992-01/ | |
| https://www.csirt.gob.cl/media/2021/07/8FFR21-00992-01.pdf | |

Imagen del sitio




| CSIRT alerta ante página fraudulenta que suplanta a Netflix | |
|---|---|
| Alerta de seguridad cibernética | 8FFR21-00993-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 21 de julio de 2021 |
| Última revisión | 21 de julio de 2021 |
| **Indicadores de compromiso** | |
| URL sitio falso | |
| https://sign-in.ntflixs.comburskuhdclub[.]com/fc3dee15d074d783730c00430d839765/knhmWSOc40J4X3DJCeXJ3v1oVrLP.php | |
| IP | |
| [104.21.41.67] | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/alertas/8ffr21-00993-01/ | |
| https://www.csirt.gob.cl/media/2021/07/8FFR21-00993-01.pdf | |

# Vulnerabilidades


| CSIRT alerta de vulnerabilidades que afectan a Google Chrome | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00468-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 15 de julio de 2021 |
| Última revisión | 15 de julio de 2021 |
| **CVE** | |
| CVE-2021-30559<br>CVE-2021-30541<br>CVE-2021-30560<br>CVE-2021-30561<br>CVE-2021-30562<br>CVE-2021-30563<br>CVE-2021-30564 | |
| **Fabricante** | |
| Google | |
| **Productos afectados** | |
| Google Chrome a 70.0.3538.67 a 91.0.4472.124. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00468-01 | |
| https://www.csirt.gob.cl/media/2021/07/9VSA21-00468-01.pdf | |


| CSIRT alerta de vulnerabilidad en productos SonicWall | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00469-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de julio de 2021 |
| Última revisión | 19 de julio de 2021 |
| **CVE** | |
| CVE-2019-7481 | |
| **Fabricante** | |
| SonicWall | |
| **Productos afectados** | |
| SonicWall Secure Mobile Access (SMA) 100 series<br>SonicWall Secure Remote Access (SRA) secure VPN appliances | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00469-01 | |
| https://www.csirt.gob.cl/media/2021/07/9VSA21-00469-01.pdf | |


| CSIRT alerta de nueva vulnerabilidad en Windows Print Spooler de Microsoft | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00470-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de julio de 2021 |
| Última revisión | 19 de julio de 2021 |
| **CVE** | |
| CVE-2021-34481 | |
| **Fabricante** | |
| Windows | |
| **Productos afectados** | |
| Microsoft Windows (versiones bajo investigación por el proveedor). | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00470-01 | |
| https://www.csirt.gob.cl/media/2021/07/9VSA21-00470-01.pdf | |


| CSIRT alerta de vulnerabilidad grave en FortiAnalyzer y FortiManager de Fortinet | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00471-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 20 de julio de 2021 |
| Última revisión | 20 de julio de 2021 |
| **CVE** | |
| CVE-2021-32589 | |
| **Fabricante** | |
| Fortinet | |
| **Productos afectados** | |
| FortiManager 5.6.10 y anteriores.<br>FortiManager 6.0.10 y anteriores.<br>FortiManager 6.2.7 y anteriores.<br>FortiManager 6.4.5 y anteriores.<br>FortiManager 7.0.0.<br>FortiManager 5.4.x.<br>FortiAnalyzer 5.6.10 y anteriores.<br>FortiAnalyzer 6.0.10 y anteriores.<br>FortiAnalyzer 6.2.7 y anteriores.<br>FortiAnalyzer 6.4.5 y anteriores.<br>FortiAnalyzer 7.0.0. | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00471-01 | |
| https://www.csirt.gob.cl/media/2021/07/9VSA21-00471-01.pdf | |


| CSIRT alerta de vulnerabilidades en productos de Oracle | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00472-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de julio de 2021 |
| Última revisión | 19 de julio de 2021 |

| CVE | | | |
|---|---|---|---|
| CVE-2012-0881 | CVE-2020-1967 | CVE-2021-22884 | oCVE-2021-2400 |
| CVE-2015-0254 | CVE-2020-1968 | CVE-2021-22890 | CVE-2021-2401 |
| CVE-2016-0762 | CVE-2020-1971 | CVE-2021-22897 | CVE-2021-2402 |
| CVE-2016-4429 | CVE-2020-24553 | CVE-2021-22898 | CVE-2021-2403 |
| CVE-2017-14735 | CVE-2020-24616 | CVE-2021-22901 | CVE-2021-2404 |
| CVE-2017-16931 | CVE-2020-24750 | CVE-2021-2323 | CVE-2021-2405 |
| CVE-2017-3735 | CVE-2020-2555 | CVE-2021-2324 | CVE-2021-2406 |
| CVE-2017-5461 | CVE-2020-25638 | CVE-2021-2326 | CVE-2021-2407 |
| CVE-2017-5637 | CVE-2020-25648 | CVE-2021-2328 | CVE-2021-2408 |
| CVE-2017-7656 | CVE-2020-25649 | CVE-2021-2329 | CVE-2021-2409 |
| CVE-2017-7657 | CVE-2020-2604 | CVE-2021-2330 | CVE-2021-2410 |
| CVE-2017-7658 | CVE-2020-26217 | CVE-2021-2333 | CVE-2021-2411 |
| CVE-2017-9735 | CVE-2020-26870 | CVE-2021-23336 | CVE-2021-2412 |
| CVE-2018-0737 | CVE-2020-27193 | CVE-2021-2334 | CVE-2021-24122 |
| CVE-2018-0739 | CVE-2020-27216 | CVE-2021-2335 | CVE-2021-2415 |
| CVE-2018-15686 | CVE-2020-27218 | CVE-2021-2336 | CVE-2021-2417 |
| CVE-2018-21010 | CVE-2020-27783 | CVE-2021-2337 | CVE-2021-2418 |
| CVE-2018-7160 | CVE-2020-27814 | CVE-2021-2338 | CVE-2021-2419 |
| CVE-2018-7183 | CVE-2020-27841 | CVE-2021-2339 | CVE-2021-2420 |
| CVE-2019-0190 | CVE-2020-27842 | CVE-2021-2340 | CVE-2021-2421 |
| CVE-2019-0201 | CVE-2020-27843 | CVE-2021-2341 | CVE-2021-2422 |
| CVE-2019-0205 | CVE-2020-27844 | CVE-2021-2342 | CVE-2021-2423 |
| CVE-2019-0210 | CVE-2020-27845 | CVE-2021-2343 | CVE-2021-2424 |
| CVE-2019-0219 | CVE-2020-28052 | CVE-2021-2344 | CVE-2021-2425 |
| CVE-2019-0228 | CVE-2020-28196 | CVE-2021-2345 | CVE-2021-2426 |
| CVE-2019-10086 | CVE-2020-28928 | CVE-2021-2346 | CVE-2021-2427 |
| CVE-2019-10173 | CVE-2020-29582 | CVE-2021-2347 | CVE-2021-2428 |
| CVE-2019-10746 | CVE-2020-35490 | CVE-2021-2348 | CVE-2021-2429 |
| CVE-2019-11358 | CVE-2020-35491 | CVE-2021-2349 | CVE-2021-2430 |
| CVE-2019-12260 | CVE-2020-35728 | CVE-2021-2350 | CVE-2021-2431 |
| CVE-2019-12399 | CVE-2020-36179 | CVE-2021-2351 | CVE-2021-2432 |
| CVE-2019-12402 | CVE-2020-36180 | CVE-2021-2352 | CVE-2021-2433 |
| CVE-2019-12415 | CVE-2020-36181 | CVE-2021-2353 | CVE-2021-2434 |
| CVE-2019-12973 | CVE-2020-36182 | CVE-2021-2354 | CVE-2021-2435 |
| CVE-2019-13990 | CVE-2020-36183 | CVE-2021-2355 | CVE-2021-2436 |
| CVE-2019-15604 | CVE-2020-36184 | CVE-2021-2356 | CVE-2021-2437 |
| CVE-2019-15605 | CVE-2020-36185 | CVE-2021-2357 | CVE-2021-2438 |
| CVE-2019-15606 | CVE-2020-36186 | CVE-2021-2358 | CVE-2021-2439 |
| CVE-2019-16942 | CVE-2020-36187 | CVE-2021-2359 | CVE-2021-2440 |
| CVE-2019-16943 | CVE-2020-36188 | CVE-2021-2360 | CVE-2021-2441 |
| CVE-2019-17195 | CVE-2020-36189 | CVE-2021-2361 | CVE-2021-2442 |

| | | | |
|---|---|---|---|
| CVE-2019-17531 | CVE-2020-5258 | CVE-2021-2362 | CVE-2021-2443 |
| CVE-2019-17543 | CVE-2020-5397 | CVE-2021-2363 | CVE-2021-2444 |
| CVE-2019-17545 | CVE-2020-5398 | CVE-2021-2364 | CVE-2021-2445 |
| CVE-2019-17566 | CVE-2020-5413 | CVE-2021-2365 | CVE-2021-2446 |
| CVE-2019-2030 | CVE-2020-5421 | CVE-2021-2366 | CVE-2021-2447 |
| CVE-2019-2725 | CVE-2020-7016 | CVE-2021-2367 | CVE-2021-2448 |
| CVE-2019-2729 | CVE-2020-7017 | CVE-2021-2368 | CVE-2021-2449 |
| CVE-2019-2897 | CVE-2020-7712 | CVE-2021-2369 | CVE-2021-2450 |
| CVE-2019-3738 | CVE-2020-7733 | CVE-2021-2370 | CVE-2021-2451 |
| CVE-2019-3739 | CVE-2020-7760 | CVE-2021-2371 | CVE-2021-2452 |
| CVE-2019-3740 | CVE-2020-8174 | CVE-2021-2372 | CVE-2021-2453 |
| CVE-2019-5063 | CVE-2020-8203 | CVE-2021-2373 | CVE-2021-2454 |
| CVE-2019-5064 | CVE-2020-8277 | CVE-2021-2374 | CVE-2021-2455 |
| CVE-2020-10543 | CVE-2020-8284 | CVE-2021-2375 | CVE-2021-2456 |
| CVE-2020-10683 | CVE-2020-8285 | CVE-2021-2376 | CVE-2021-2457 |
| CVE-2020-10878 | CVE-2020-8286 | CVE-2021-2377 | CVE-2021-2458 |
| CVE-2020-11022 | CVE-2020-8554 | CVE-2021-2378 | CVE-2021-2460 |
| CVE-2020-11023 | CVE-2020-8908 | CVE-2021-2380 | CVE-2021-2462 |
| CVE-2020-11612 | CVE-2020-9484 | CVE-2021-2381 | CVE-2021-2463 |
| CVE-2020-11868 | CVE-2020-9489 | CVE-2021-2382 | CVE-2021-25122 |
| CVE-2020-11973 | CVE-2021-20190 | CVE-2021-2383 | CVE-2021-25329 |
| CVE-2020-11979 | CVE-2021-20227 | CVE-2021-23839 | CVE-2021-26117 |
| CVE-2020-11987 | CVE-2021-21275 | CVE-2021-2384 | CVE-2021-26271 |
| CVE-2020-11988 | CVE-2021-21290 | CVE-2021-23840 | CVE-2021-26272 |
| CVE-2020-11998 | CVE-2021-2131 | CVE-2021-23841 | CVE-2021-27568 |
| CVE-2020-12723 | CVE-2021-2134 | CVE-2021-2385 | CVE-2021-27807 |
| CVE-2020-13934 | CVE-2021-21343 | CVE-2021-2386 | CVE-2021-27906 |
| CVE-2020-13935 | CVE-2021-21344 | CVE-2021-2387 | CVE-2021-28041 |
| CVE-2020-13949 | CVE-2021-21345 | CVE-2021-2388 | CVE-2021-29921 |
| CVE-2020-13956 | CVE-2021-21346 | CVE-2021-2389 | CVE-2021-30369 |
| CVE-2020-14060 | CVE-2021-21347 | CVE-2021-2390 | CVE-2021-30640 |
| CVE-2020-14061 | CVE-2021-21348 | CVE-2021-2391 | CVE-2021-3156 |
| CVE-2020-14062 | CVE-2021-21349 | CVE-2021-2392 | CVE-2021-3177 |
| CVE-2020-14195 | CVE-2021-21350 | CVE-2021-2393 | CVE-2021-31811 |
| CVE-2020-14756 | CVE-2021-21351 | CVE-2021-2394 | CVE-2021-33037 |
| CVE-2020-15389 | CVE-2021-21409 | CVE-2021-2395 | CVE-2021-3345 |
| CVE-2020-17521 | CVE-2021-22112 | CVE-2021-2396 | CVE-2021-3449 |
| CVE-2020-17527 | CVE-2021-22118 | CVE-2021-2397 | CVE-2021-3450 |
| CVE-2020-17530 | CVE-2021-2244 | CVE-2021-2398 | CVE-2021-3520 |
| CVE-2020-1941 | CVE-2021-22876 | CVE-2021-2399 | CVE-2021-3560 |
| CVE-2020-1945 | CVE-2021-22883 | | |

**Fabricante**

Oracle

**Productos afectados**

Enterprise Manager Base Platform [1370]
Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers [10656]
Hyperion Financial Reporting [8776]
Hyperion Infrastructure Technology [4392]
Identity Manager [1980]
Instantis EnterpriseTrack [10563]
Java SE [856]

Java SE, Oracle GraalVM Enterprise Edition [856]
JD Edwards EnterpriseOne Orchestrator [11681]
JD Edwards EnterpriseOne Tools [4781]
MICROS Compact Workstation 3 [13794]
MICROS ES400 Series [14212]
MICROS Kitchen Display System Hardware [11641]
MICROS Workstation 5A [11636]
MICROS Workstation 6 [11628]
MySQL Cluster [8479]
MySQL Connectors [8576]
MySQL Enterprise Monitor [8480]
MySQL Server [8478]
Oracle Access Manager [5565]
Oracle Advanced Inbound Telephony [265]
Oracle Advanced Outbound Telephony [785]
Oracle Agile Engineering Data Management [4436]
Oracle Agile PLM [4461]
Oracle Application Testing Suite [4622]
Oracle Applications Framework [1472]
Oracle Approvals Management [1168]
Oracle BAM (Business Activity Monitoring) [1675]
Oracle Banking Enterprise Default Management [13390]
Oracle Banking Liquidity Management [13304]
Oracle Banking Party Management [13929]
Oracle Banking Platform [9178]
Oracle Banking Treasury Management [14133]
Oracle BI Publisher [1479]
Oracle Business Intelligence Enterprise Edition [2025]
Oracle Coherence [2545]
Oracle Collaborative Planning [1037]
Oracle Commerce Guided Search / Oracle Commerce Experience Manager
Oracle Commerce Guided Search [9633]
Oracle Commerce Merchandising [9349]
Oracle Commerce Platform [9348]
Oracle Commerce Service Center [9351]
Oracle Common Applications [1198]
Oracle Communications Application Session Controller [10769]
Oracle Communications Billing and Revenue Management [2136]
Oracle Communications BRM – Elastic Charging Engine [9742]
Oracle Communications Cloud Native Core Console [14250]
Oracle Communications Cloud Native Core Network Function Cloud Native Environment [14125]
Oracle Communications Cloud Native Core Network Slice Selection Function
Oracle Communications Cloud Native Core Policy [14277]
Oracle Communications Cloud Native Core Security Edge Protection Proxy
Oracle Communications Cloud Native Core Service Communication Proxy
Oracle Communications Cloud Native Core Unified Data Repository [14119]
Oracle Communications Convergent Charging Controller [12985]
Oracle Communications Design Studio [2283]
Oracle Communications Diameter Signaling Router (DSR) [10899]
Oracle Communications EAGLE Software [10768]

Oracle Communications Evolved Communications Application Server [10994]
Oracle Communications Instant Messaging Server [8495]
Oracle Communications Network Charging and Control [4623]
Oracle Communications Offline Mediation Controller [2269]
Oracle Communications Pricing Design Center [9437]
Oracle Communications Services Gatekeeper [5381]
Oracle Communications Unified Inventory Management [4516]
Oracle Configuration Manager [1967]
Oracle Data Integrator [2196]
Oracle Database (Advanced Networking Option) [219]
Oracle Database (Big Data Spatial and Graph) [11528]
Oracle Database (Essbase Analytic Provider Services) [4349]
Oracle Database (Essbase) [4379]
Oracle Database (Hyperion Essbase Administration Services) [4380]
Oracle Database (MapViewer) [619]
Oracle Database (Oracle Application Express Application Builder) [1348]
Oracle Database (Oracle Application Express Data Reporter) [1348]
Oracle Database (Oracle Application Express) [1348]
Oracle Database (Oracle Spatial and Graph MapViewer) [619]
Oracle Database (Oracle Spatial and Graph Network Data Model) [619]
Oracle Database (Oracle Spatial and Graph) [619]
Oracle Database (Oracle Text) [211]
Oracle Database (RDBMS) [662]
Oracle Database Enterprise Edition [5]
Oracle Engineering [532]
Oracle Enterprise Data Quality [9464]
Oracle Enterprise Repository [5326]
Oracle E-Records [1325]
Oracle Field Service [747]
Oracle Financial Services Analytical Applications Infrastructure [5680]
Oracle Financial Services Crime and Compliance Investigation Hub [13964]
Oracle Financial Services Regulatory Reporting with AgileREPORTER [13077]
Oracle Financial Services Revenue Management and Billing Analytics [11527]
Oracle FLEXCUBE Private Banking [9110]
Oracle FLEXCUBE Universal Banking [9052]
Oracle Fusion Middleware MapViewer [1215]
Oracle GoldenGate Application Adapters [5760]
Oracle GraalVM Enterprise Edition [13497]
Oracle Hospitality Reporting and Analytics [11599]
Oracle Hospitality Suite8 [12614]
Oracle Human Resources [507]
Oracle Hyperion BI+ [4361]
Oracle Insurance Policy Administration [5279]
Oracle Insurance Policy Administration J2EE [5279]
Oracle Insurance Rules Palette [5288]
Oracle iSupplier Portal [208]
Oracle JDeveloper [807]
Oracle JDeveloper and ADF [807]
Oracle Managed File Transfer [10198]
Oracle Marketing [229]
Oracle Outside In Technology [2276]

| |
|---|
| Oracle Policy Automation [5624] |
| Oracle Public Sector Financials (International) [26] |
| Oracle Retail Back Office [2013] |
| Oracle Retail Central Office [2016] |
| Oracle Retail Customer Engagement [11518] |
| Oracle Retail Customer Management and Segmentation Foundation [13388] |
| Oracle Retail Financial Integration [10722] |
| Oracle Retail Integration Bus [1807] |
| Oracle Retail Merchandising System [1816] |
| Oracle Retail Order Broker [11520] |
| Oracle Retail Order Management System Cloud Service [11519] |
| Oracle Retail Point-of-Service [2017] |
| Oracle Retail Price Management [1824] |
| Oracle Retail Returns Management [2020] |
| Oracle Retail Service Backbone [10867] |
| Oracle Retail Xstore Point of Service [11513] |
| Oracle SD-WAN Aware [13941] |
| Oracle SD-WAN Edge [13940] |
| Oracle Secure Global Desktop [8539] |
| Oracle Solaris [10006] |
| Oracle Solaris Cluster [10005] |
| Oracle Time and Labor [311] |
| Oracle Transportation Management [1991] |
| Oracle VM VirtualBox [8370] |
| Oracle Web Applications Desktop Integrator [1171] |
| Oracle WebCenter Portal [1696] |
| Oracle WebLogic Server [5242] |
| Oracle Workflow [174] |
| Oracle ZFS Storage Appliance Kit [10026] |
| OSS Support Tools [1330] |
| PeopleSoft Enterprise CS Campus Community [5183] |
| PeopleSoft Enterprise HCM Candidate Gateway [5043] |
| PeopleSoft Enterprise HCM Shared Components [8943] |
| PeopleSoft Enterprise PeopleTools [5085] |
| PeopleSoft Enterprise PT PeopleTools [5085] |
| Primavera Gateway [10605] |
| Primavera P6 Enterprise Project Portfolio Management [5579] |
| Primavera Unifier [10354] |
| Real-Time Decisions (RTD) Solutions [4509] |
| Siebel Apps – Marketing [8974] |
| Siebel Core – Automation [8988] |
| Siebel Core – Server Framework [9001] |
| Siebel CRM [9001] |
| StorageTek Tape Analytics SW Tool [10085] |
| **Enlaces para revisar el informe:** |
| https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00472-01 |
| https://www.csirt.gob.cl/media/2021/07/9VSA21-00472-01.pdf |


| CSIRT alerta de vulnerabilidades en productos de Citrix | |
|---|---|
| Alerta de seguridad cibernética | 9VSA21-00473-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 22 de julio de 2021 |
| Última revisión | 22 de julio de 2021 |
| **CVE** | |
| CVE-2021-22919<br>CVE-2021-22920<br>CVE-2021-22927 | |
| **Fabricante** | |
| Citrix | |
| **Productos afectados** | |
| Citrix ADC<br>Citrix Gateway<br>Citrix SD-WAN WANOP Edition | |
| **Enlaces para revisar el informe:** | |
| https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00473-01 | |
| https://www.csirt.gob.cl/media/2021/07/9VSA21-00473-01.pdf | |

# IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el CSIRT de Gobierno.

Recomendamos a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

| Hash de archivos maliciosos | Tipo de malware | Documento web |
|---|---|---|
| 85bf932b3b1d6dfdd4a88990127d3506f66dc1291fa219e899e45d5b7e301984 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| f2d084daef2879143ef4fbb13b95ceaa502a6a10ddbbb6f8f5aa240e7975493d | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 07dd4ee1df8e68ee3db8f40d229a67f7c2bc6c84f7771811b874eaef52f52308 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 3ae1e49f9ed22a71e3cbe361ddf8069ea4bb0cd97f007f3ece0371bdcd8f3a8a | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 54d72f13cbc428b63bf447f27d311d47dca8b3ea66db6ea40a97a3c1efe7b553 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 40973413af67edf20103934ded7d79f027b4c03ae1feef37cf4cce125a71836a | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 046acc091e1295057af4873d1270eba61b09be7ad145827b1757f4042b753d81 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 8fb73c6a027c5e515ac227d7f069dfeff04c94073a83e81eb69253c8c75cf0d0 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| c01dedbc746a16a56712536bf571c32f93a2931a6fa107a6b59c01cf0dbf8546 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 40f6bb24a2a8429d407b46580685a3b7d0283c18d1315b1e0f3e44381c8794e5 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 0ddc217fad3c587462e43829f94a5aec4e4079ddf6ab088423129615accff04e | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| e9f631f88fa84f86a467b734ca186a3f6c0a00c65c072a7b3d62501b53ca424d | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| c76acd788320030e85aaa925870a770217352f34a86b9de625f00db6d14298ee | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 17f87a0422c08443f627bfba6ebd143c0c62c0cf70431cecdd040f619946c57e | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 0af2fe0136bea931e762112d811f9aabbdf733afa2f4aea816bfc66af2974ded | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 305e0fb98c52c99b7e5541a0ef2ab832b047dd6281c8dfadd284a8004afabc16 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 027686cab112ebd16edb28f71379b69d310636d671b90b41a5dca7004b992b77 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| f847ea36df2d40d1700ef099b244afb05c960e11c44e22cfc12b44b22bf993df | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 8fd8fb4df74fa886589a6e13e08769e70c0d576171369a767ba78a69b8b26634 | HTML/Fisher.295!tr | 2CMV21-00203-01 |

| | | |
|---|---|---|
| 111238fb60b05d919e550d0ab4e95e2dc2e8e75ecd233a7c73be9678aa396805 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 332eda8c68cec9356a1ed39e53cc79e8ac8467053628002b3c5d6a7fec1812f9 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 7a7c7295a28e8866f20255156cec71b1f32908924c1b39fe35b3eb93a39a23be | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 10eb56cf79b33e82d8300cbe0b5e71072410028f14d0c7c721947b58bb8054a3 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 6c35a6510a269c3a8b44cb58ed84a23b421cc6eaa739ca0fdc8838c8d18240e9 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 2ebba28b582188214a3acf2860feae608e773a4a12e1ff0b761d4811d50c1bdd | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 608681de369640df3ebceeb3401feb364b97909273c93af0424230e881e0cfb1 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 24ec6085094a95a0edba39ffb97dd51b875eed029bad9251889ba5af22d76d99 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 7ef68c356fd0a898a11f94dd46da3f24e82a4de30b08d49254d9ef15e8efa37b | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 9a25bf4863a58000431b48d9e342e31cf2766a2de4ac38c2169773a4b89d1998 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 10ca4aa8fdbd2f71339c90a26fc148368ae7fa950aa52dce1dfa2fdadc76b133 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| e253c023459dce97c95ca9c63446633eafbca1dd83c762c5cb4c3d24986eba3f | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| d0e193d278f6605cd4a032035216b7223e92ea3ac8bf3efa8ac17e5a5b001cbb | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| fdfd6757c110bf486c550c212a4bf1aa9869235b9f5a690c29a70ae51112466c | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 684756755a0fc568b7034d87ed9ecd32ea36e2eb8fc164f0c3cc52476968d717 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| dbbec7a08ef6286e974cb910f493e1255e8bb25d001762bef9aa3ecd18249cd1 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| f534c9ec6fcb77fe9dea3e354b2140dbb2227808294803228bf962799094ff84 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| c76483aecab8ee54042e55e37da2a93c900082c8235e40f5b480b000a15f9b60 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 8191a837bda3274522c8dc26a56d2fcdf1ed7973267d191606ea787253127ea1 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 2fcefd048932aaaa187e94eee172a866ae24328a936590713eabf1145c50befa | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 95318a67672f8aeed29449cdb7b2ac8fc8376ad220a3dcfb0dbafca9c9b7106e | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| baf481f753c8d140374c7fab2d4c8eff4b11041f152fc3c2dd02aab7427fe2e5 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 7d449af0446e44e8aaf70bb6a72e53997de835c29957ac1c81d9b493a65ce1b1 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| e7c3aa587409d80ff83af0e03783264464e261072660956dc0520a8d5d778e48 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 6ad401f8f4e3d398aa71edfb2f70ccf46b05264039487ce89e87a5c88261e137 | HTML/Fisher.295!tr | 2CMV21-00203-01 |

| | | |
|---|---|---|
| 35d68f509bf318ae37607c8ec3e6761b3ee8393b0a5d7c19e74c0fcd4c8ce099 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 5fe8e07025b43b9d033f39db2a7270e1d08818347b6fcd3116bb08e02d529552 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 49142234dad2247b501caaa3733bf35adc75e5c4d88eca66902135c624eeefcd | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 2c39f0e9c19ed13e35cc2b8a45816b08809fb9b352fbb41fa7d5e71587b65d0b | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| c2cdb4b408859f1071b0689321a90c11d18319e1c074a5dfc578fe766fdc0cb4 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| f9c5c7ecb93e07b2c3cf0d70ef954271b9c1638d49aeabdd8957442935614f29 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| ecd13939c43d1ab838198696196b5090c6128b2ad9f2ff96d2b85081e68ae697 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 3a49559073969cfff64fa093e2090a2e92fb5a345122d018260390a33fd6d6ad | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 708a91b1746b7d240defefa2c5c3e46aec524d802089bac20558eb359f190d09 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| c0a2c9590ddec8b91a2d5f41016bf3bc49071b61a308605ea966b31c7acda1b5 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 401e27db43fb18ee0badd90ebfedff42bd721f0f82b78aeb427d0d6227f10dba | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 0a7a628f83780df70e68d932a0de5f97ab34e9f622dc686b7e3386c86a1a0a51 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 8a03904b6fc1fbb8559a42bdd4df2fdc78c98d7e767cf0b0f7870c2ce7f9a6a0 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| faa617b50c35b31ecbdeb2904ef52138d3829f3cea06488cef4313a629d24d75 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 5fde1e91d2d79179e9349ed2e037af30cf808636bf446fbcf16a7ee8c17e8214 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| c6bf627c961f219ad2a2bdb2024bd6c498fcbad0d6252ad0d4719eaf4fc44995 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 41b8563391eeb3c26f39ab9484a694dc332ef95990e9f680721271ad513166c2 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 742d411e53be4a81a450648d104415a8441c78ccd6127a2902ba3c589f6ea953 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 4cfaa3d19bea873b693b3f939af328d4577c5234c8a9342d9c7cd96f70d7ab94 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 441f7c39078e978334d200e765e21626a792d7d9adeb283431daf0ba7dab1dfe | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 264f08f041d0d6d265425189bfd853351bf5445bd72d4eda2383d475b857a4b3 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 0c7c9e7ad2e0b4abacfef83623316ad978a97a3db192e263a6976f30ac8286a8 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 577122608f35d15f6993191ef795bdf80ab3ffa6d2540f3bccf0bbeeaac7570d | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 73d30b360b8f72a5e45e48d92b353d703db9e6caf2fea17ba940553f430ea1a1 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| fd7bb3f9d20db4a16d0c12e4c330d8bb6c23883c33fa13f0505ce2eab3f665cf | HTML/Fisher.295!tr | 2CMV21-00203-01 |

| | | |
|---|---|---|
| 8c1e5736331e9c875ea1ae532dcd58bd40eb80819ef2f3a2d5080bb723ed5f4c | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 4bd248fe22ac9d611889b6e6c8a9d093832f69f17100db06b069c1e69bc1c271 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| f34221c5b56c76435638a0ce9354fce51b27f27eea773b3f6e7781770dd99767 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 034199c0abf2d787c9778a08591dda826ec9a887f4337b372b217d153133ddab | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 8be0bfabd0131293651ec5acfde25ef78773dd3ba4eb898b4cc0cc836512e7d3 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| b79bcbe51e73fd483469b7b63e19d3a1971d6a9c05b77a7dc7b45dc068f77be5 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 498c6a657325b8306cdd5ca5b61edcdd2074dc69ac7c3d53eb4a5848a8a23cf3 | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 8f7e3a87c2fe8ddbbf84b011f49e3a243b33637761c82eaeb3495bb1164908fe | HTML/Fisher.295!tr | 2CMV21-00203-01 |
| 5ce36ce85184945d5f30a8d9081105723297c0650aa929e9e53801414bb68fea | HTML/GenericKDZ.1174!tr | 2CMV21-00203-01 |
| 4eb8af783f0a5ee33275f4f875fe69408c61b5ca77df8a399c70d682afef06a2 | HTML/GenericKDZ.1174!tr | 2CMV21-00203-01 |
| 90c8ae15aec66d5c11ad5cc0bfc0e80deec11b2a04f0ab2bff3182de5300fe2e | HTML/GenericKDZ.1174!tr | 2CMV21-00203-01 |
| 3e187fbe81b364327180fc1ca695ad251c09f918b1a147d1ea28104bf6f4cbe9 | HTML/Phish.397C!tr | 2CMV21-00203-01 |
| 08ebcff7243587fccd12c49ea2f2933be00bdc6546cc6c5fd0239aa4bf815342 | HTML/Phish.BF41!tr | 2CMV21-00203-01 |
| 41e48d3cadcccaccc4ad6260384779b11d8c0bd63c18ee7ae12de6dafd53213d | HTML/Phish.BF41!tr | 2CMV21-00203-01 |
| 692cb027c375a5309c7bd30e7cef0204c60eacfafd35889e59c530636f8ade70 | Malicious_Behavior.SB | 2CMV21-00203-01 |
| 8b6152f4163a83ba3eef961d44115feb19e8f916c887af6b85fe9541c1f97fd7 | Malicious_Behavior.SB | 2CMV21-00203-01 |
| 461a101eda112b3565d7f8ee961a2a066bc059333b7f85715872634cc1f081ac | Malicious_Behavior.SB | 2CMV21-00203-01 |
| bc25a7d43fc1da6677d62e5f9573b259f8b4ec6ab32f5aed8102d57948517bae | Malicious_Behavior.SB | 2CMV21-00203-01 |
| 439b1755be21ad2c8eefd63531e8bbbacdc7b1c07057d83dd9066358b4402661 | Malware_Generic.P0 | 2CMV21-00203-01 |
| 9b34ded1cfa18860eed4e7f6fa5043db044fa0eb6a81eb911a408304b05aefa7 | MSIL/Kryptik.ABRY!tr | 2CMV21-00203-01 |
| afcba9ee59b8d6972e414ffd93556389ee378a4139453acf70be522e91a69c95 | MSIL/Kryptik.DLO!tr | 2CMV21-00203-01 |
| 8e026969ac083cb90e1ece1b2a13353eb9facd2c5cfde7d73ae0c52bf828f88a | W32/Malicious_Behavior.SBX | 2CMV21-00203-01 |
| 2b4219e8a06702279e71778d097bcd122766a44d07827c5834768ac9463c7b65 | W32/Taskun!tr | 2CMV21-00203-01 |
| f9930198476d841f38ec234cfbc8ea3796efb4bafd157fe6f51330cf940290b4 | W32/Taskun.ABVW!tr | 2CMV21-00203-01 |
| 8d25f321f961251a7286688aa3379f493fdb5eaffe439131c0425a7a12e1feab | HTML/AccPhish.A!tr | 2CMV21-00204-01 |

| | | |
|---|---|---|
| b4a2526963ed9fb511a6ef6d45e454688fa97f6e0b6b70f01c9e89ece2c3a55c | HTML/AccPhish.A!tr | 2CMV21-00204-01 |
| f51dfa36793decdd634ecdccc169d68795b33a105a2d2801a0b6beeed1ae338e | HTML/AccPhish.A!tr | 2CMV21-00204-01 |
| fb71a3dfe9ead054b0532f09bec284da5966ed1f1a284be0fbe303457057bac4 | Malicious_Behavior.SB | 2CMV21-00204-01 |
| 3e61ed3c8e9fcdc2cbc9cfa733c2819d06c68e4db6609526fed67e0e1af2675d | Malware_Generic.P0 | 2CMV21-00204-01 |
| b03f50b5fc47b8433f9b5b4be5a972d18a8e59d6923715017fe71a20c5012431 | Malware_Generic.P0 | 2CMV21-00204-01 |
| ed855e00bc8c7ffeb19d2f854c630e1dcae61c14cd402290dce71170c44c328c | Malware_Generic.P0 | 2CMV21-00204-01 |
| b725eb4f491ac6f877a31a0877a648b5b486e905c6a356049ee44126bda2854f | MSExcel/CVE_2017_11882!exploit | 2CMV21-00204-01 |
| 135894c83ce3c3b86098831bd8ea6908750ed64df951118540402847c782584c | MSIL/GenKryptik.EYTI!tr | 2CMV21-00204-01 |
| f0212164481dbc5204645f14e6fd604178e2a1bbc7064e021f459b3aa49abacf | MSIL/GenKryptik.FHQY!tr | 2CMV21-00204-01 |
| 069048269a726715a5b39c9735a0aa7c4f19ce4b6efea4a8dc13adda4f84420c | MSIL/GenKryptik.FHSB!tr | 2CMV21-00204-01 |
| 107834af78735ee81662a252fa57946ef11750bdd3dbbe32e87e5f150970baed | MSIL/GenKryptik.FHSB!tr | 2CMV21-00204-01 |
| d639b760a935bfbb5168606f6c7b11aa87a44893ea0bf0f1e344775333d3715d | MSIL/GenKryptik.FHSB!tr | 2CMV21-00204-01 |
| 3c7eb9f8247f14ae0f2b4f9cd50e0e6e73da2fd22e6a916c26e5bf9b3da9eaa3 | MSIL/Kryptik.ACAH!tr | 2CMV21-00204-01 |
| 343573a841f9a28bfe7eb58ae4ac084c714abfc0ca3484466b879a92eea4a975 | MSIL/Kryptik.ACAN!tr | 2CMV21-00204-01 |
| 4a9cb8738125e9b209c25af9319c5fd8cbcfbbd8e55036789459fe76928df70f | MSIL/Kryptik.ACAN!tr | 2CMV21-00204-01 |
| acb6756f7955bd09c092eb8b9e53dc4e97f96dde294d41681ffdd1ff0f56e7ea | MSIL/Kryptik.ACAN!tr | 2CMV21-00204-01 |
| 63241bbcdda9b9030690adcc937f3e0b0a88bac2403aeafb4842c8a062357326 | MSIL/Kryptik.DLO!tr | 2CMV21-00204-01 |
| 13406dbb5a4e23808961b84a71e59ff774affd421e1ffa2364dc22c9582912fb | MSIL/Kryptik.ZXG!tr | 2CMV21-00204-01 |
| bdb9857496e50544537e1a1d7b9baf6fb8c8ba9ce51f98dc8cdcabb04ce8776f | MSIL/Kryptik.ZXG!tr | 2CMV21-00204-01 |
| 38473a7da74c7513b8b26550778e6c10337bfa0c8037a5ec1040200c324dcc5b | VBA/Agent.1873!tr.dldr | 2CMV21-00204-01 |
| 46aa81e194997d9f71e52292acaedbf2d269143f112aaf2f582e504ba75ee90a | W32/Injector.EPUC!tr | 2CMV21-00204-01 |

**Direcciones IP de servidor SMTP** donde es enviado el correo malicioso: Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

| IP | Etiqueta de sistema autónomo | Documento web |
|---|---|---|
| 45.7.230.78 | OPEN CLOUD SpA | 2CMV21-00203-01 |
| 141.226.3.28 | RIPE Network Coordination Centre | 2CMV21-00203-01 |
| 184.176.134.58 | Cox Communications Inc. | 2CMV21-00203-01 |
| 162.245.182.137 | Reedsburg Utility Commission | 2CMV21-00203-01 |
| 181.58.189.228 | Telmex Colombia S.A. | 2CMV21-00203-01 |
| 174.115.233.87 | Rogers Communications Canada Inc. | 2CMV21-00203-01 |
| 166.157.4.235 | Service Provider Corporation | 2CMV21-00203-01 |
| 54.160.161.235 | Amazon Technologies Inc. | 2CMV21-00203-01 |
| 190.4.213.174 | TELEFONICA MOVIL DE CHILE S.A. | 2CMV21-00203-01 |
| 120.158.130.252 | Telstra Corporation | 2CMV21-00203-01 |
| 51.210.20.90 | System Ltd BDM | 2CMV21-00203-01 |
| 178.32.76.155 | Gross Alan | 2CMV21-00203-01 |
| 136.144.41.79 | RIPE Network Coordination Centre | 2CMV21-00203-01 |
| 136.144.41.208 | RIPE Network Coordination Centre | 2CMV21-00203-01 |
| 37.0.11.104 | Serverion BV | 2CMV21-00203-01 |
| 37.0.11.253 | Serverion BV | 2CMV21-00203-01 |
| 2.56.59.91 | Serverion BV | 2CMV21-00203-01 |
| 103.115.67.133 | MIXTELECOMLLC | 2CMV21-00203-01 |
| 118.42.185.245 | Korea Telecom | 2CMV21-00203-01 |
| 103.24.0.199 | Hong Kong RedTone Telecomunications Limited | 2CMV21-00203-01 |
| 77.76.155.50 | INTERCITY | 2CMV21-00203-01 |
| 95.225.50.112 | Telecom Italia S.p.A. | 2CMV21-00203-01 |
| 80.35.82.110 | Red de servicios IP | 2CMV21-00203-01 |
| 103.82.27.232 | Phong Thuy media joint stock company | 2CMV21-00203-01 |
| 103.139.44.229 | Trung Hieu Services Trading Investment Company Limited | 2CMV21-00203-01 |
| 103.28.70.171 | Transferred to the ARIN region on 2016-06-20T22:38:28Z. | 2CMV21-00203-01 |
| 103.28.70.138 | Transferred to the ARIN region on 2016-06-20T22:38:28Z. | 2CMV21-00203-01 |
| 108.62.118.59 | Lease web USA Inc. | 2CMV21-00203-01 |
| 68.42.145.159 | Comcast Cable Communications LLC | 2CMV21-00203-01 |
| 138.197.147.173 | DigitalOcean LLC | 2CMV21-00203-01 |
| 151.84.151.179 | Wind Tre S.p.A. | 2CMV21-00203-01 |

| | | |
|---|---|---|
| 43.129.181.214 | Tencent Building, Kejizhongyi Avenue | 2CMV21-00203-01 |
| 217.155.205.10 | Zen Internet Ltd | 2CMV21-00203-01 |
| 177.200.80.201 | SOBRALNET SERVICOS E TELECOMUNICACOES LTDA - ME | 2CMV21-00203-01 |
| 87.240.208.54 | POST Luxembourg | 2CMV21-00203-01 |
| 43.133.33.18 | Tencent Building, Kejizhongyi Avenue | 2CMV21-00203-01 |
| 43.132.149.219 | Tencent Building, Kejizhongyi Avenue | 2CMV21-00203-01 |
| 43.133.33.102 | Tencent Building, Kejizhongyi Avenue | 2CMV21-00203-01 |
| 179.192.99.253 | Telemar Norte Leste S.A. | 2CMV21-00203-01 |
| 51.195.227.148 | OVH SAS | 2CMV21-00203-01 |
| 92.222.24.222 | OVH SAS | 2CMV21-00204-01 |
| 103.155.82.198 | VIETSPEED SERVICE COMPANY LIMITED | 2CMV21-00204-01 |
| 185.222.57.93 | bd-rootlayer-1-mnt | 2CMV21-00204-01 |
| 101.99.64.166 | Shinjiru Technology Sdn. Bhd. | 2CMV21-00204-01 |
| 107.175.156.137 | ColoCrossing | 2CMV21-00204-01 |
| 185.222.57.170 | bd-rootlayer-1-mnt | 2CMV21-00204-01 |
| 103.167.93.90 | VNNETWORK NETWORK SOLUTION COMPANY LIMITED | 2CMV21-00204-01 |
| 191.101.130.79 | Digital Energy Technologies Chile SpA | 2CMV21-00204-01 |
| 103.133.108.70 | Vcloud service limited company | 2CMV21-00204-01 |
| 45.137.22.132 | RootLayer Web Services Ltd. | 2CMV21-00204-01 |
| 185.222.58.158 | bd-rootlayer-1-mnt | 2CMV21-00204-01 |
| 198.16.95.5 | FDCservers.net | 2CMV21-00204-01 |
| 185.222.57.149 | bd-rootlayer-1-mnt | 2CMV21-00204-01 |
| 103.207.38.69 | VietServer Services technology company limited | 2CMV21-00204-01 |
| 87.240.72.14 | KERTEL SAS | 2CMV21-00204-01 |
| 138.68.253.26 | DigitalOcean LLC | 2CMV21-00204-01 |
| 200.10.184.121 | Corporacion Administrativa del Poder Judicial de C | 2CMV21-00204-01 |
| 209.85.166.49 | Google LLC | 2CMV21-00204-01 |
| 209.85.166.50 | Google LLC | 2CMV21-00204-01 |
| 200.91.27.106 | Ingenieria  Servicios y Comunicaciones S.A. | 2CMV21-00204-01 |
| 104.47.33.59 | Microsoft Corporation | 2CMV21-00204-01 |
| 167.89.57.99 | SendGrid Inc. | 2CMV21-00204-01 |
| 104.47.40.54 | Microsoft Corporation | 2CMV21-00204-01 |
| 190.160.0.176 | VTR BANDA ANCHA S.A. | 2CMV21-00204-01 |
| 40.92.22.54 | Microsoft Corporation | 2CMV21-00204-01 |
| 52.100.166.207 | Microsoft Corporation | 2CMV21-00204-01 |
| 104.47.33.51 | Microsoft Corporation | 2CMV21-00204-01 |
| 200.68.36.201 | Distribuidora y Servicio D&S S.A. | 2CMV21-00204-01 |
| 209.85.216.71 | Google LLC | 2CMV21-00204-01 |

| | | |
|---|---|---|
| 186.148.42.78 | CTC Transmisiones Regionales S.A. | 2CMV21-00204-01 |
| 104.47.56.44 | Microsoft Corporation | 2CMV21-00204-01 |
| 209.85.219.182 | Google LLC | 2CMV21-00204-01 |
| 209.85.221.45 | Google LLC | 2CMV21-00204-01 |
| 209.85.222.51 | Google LLC | 2CMV21-00204-01 |

# Actualidad

## Presidente Piñera envía proyecto de ley contra amenazas, coacción y hostigamiento

En una ceremonia en el Palacio de la Moneda, el Presidente de la República, Sebastián Piñera, presentó el proyecto de ley elaborado por el Gobierno para combatir de mejor forma las amenazas, el hostigamiento y la coacción.

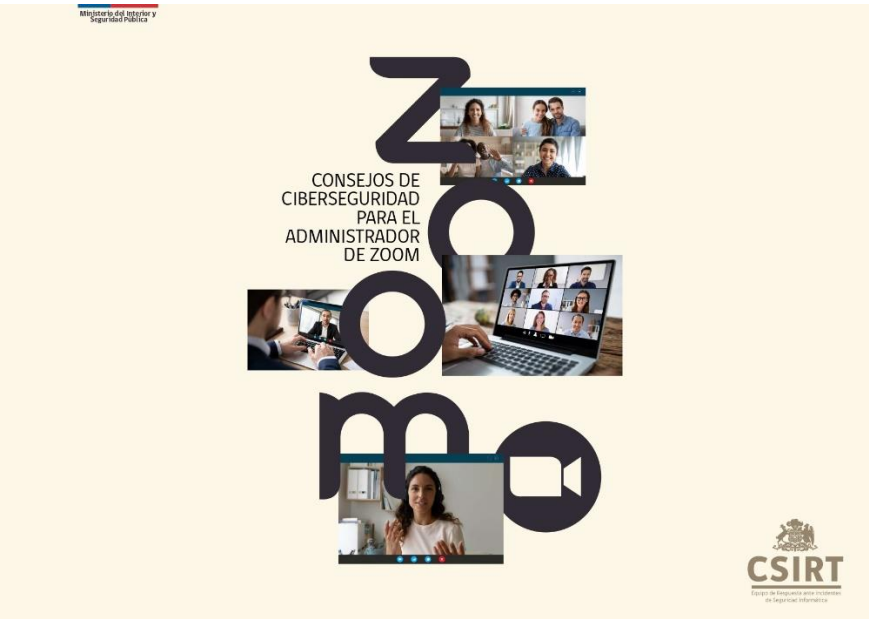
La ceremonia contó con la participación de padres de víctimas de acoso escolar, como Evanyely Zamorano y Emanuel Pacheco, padres de Katy Summer y creadores de la fundación del mismo nombre, que lucha por combatir este tipo de hostigamiento.

Más información sobre el proyecto, aquí: https://www.csirt.gob.cl/noticias/presidente-pinera-envia-proyecto-de-ley-contra-amenazas-coaccion-y-hostigamiento-leyantiamenazas/

## Ciberguías | Consejos de ciberseguridad para el administrador de Zoom

Hace rato quedó claro que el trabajo mantendrá una cuota importante de labores remotas. Y para la coordinación de actividades en este contexto de teletrabajo es esencial realizar reuniones virtuales, siendo la plataforma más popular para ello Zoom.

Por eso queremos entregar, en una de nuestras tradicionales ciberguías, las principales recomendaciones para hacer más seguras las reuniones que se administren en este programa. La guía completa, en formato PDF para descargar y compartir, aquí: https://www.csirt.gob.cl/recomendaciones/ciberguias-consejos-de-ciberseguridad-para-el-administrador-de-zoom/.



## Director del CSIRT de Gobierno inaugura segunda reunión de Cybersecurity Innovation Councils, organizada por la OEA y Cisco

La Organización de los Estados Americanos (OEA) y Cisco organizaron este martes la segunda reunión en Chile de los Cybersecurity Innovation Councils (CIC), espacio de discusión para la promoción de la innovación y las buenas prácticas en ciberseguridad.

Teniendo un foco de ciberseguridad, el CSIRT de Gobierno no podía estar ausente, y así es como su Director Nacional, Carlos Landeros, participó del evento junto a otros actores relevantes del rubro en nuestro país, como el senador Kenneth Pugh, permanente impulsor de la ciberseguridad y la transformación digital en el Congreso; Carlos Ávila, responsable de Inteligencia Artificial del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación (un área clave en el avance de la transformación digital a todo nivel), Katherina Canales, Directora Operacional del CSIRT de Gobierno y Claudio Ortiz, gerente general en Chile de Cisco, importante empresa tecnológica que organizó la reunión junto a la OEA.

Más información: https://www.csirt.gob.cl/noticias/director-del-csirt-de-gobierno-inaugura-segunda-reunion-de-cybersecurity-innovation-councils-organizada-por-la-oea-y-cisco/.

## El Comando de la Semana | No. 9 Comandos para hacer u test de stress

El Comando de la Semana trajo en esta ocasión un pack de comandos para realizar pruebas de stress. Las herramientas de las que haremos una descripción de su uso básico en esta oportunidad son: IPERF, TOMAHAWK, HPING3, HTTPERF, SIEGE y AB.

Se puede encontrar aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-8/.

## El Control de la Semana | No. 4 Inventarios de Activos

El documento de esta semana tuvo como objetivo ilustrar sobre los diferentes controles normativos que se estima son prioritarios para todo Sistema de Gestión de Seguridad de la Información. Esta cuarta ficha, sobre cómo realizar Inventarios de Activos, aquí: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-3.

# 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 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.

- Patricio Pérez Cárcamo
- Nicolás Matías
- Jair Palma
- Romel Rivas
- Roberto Iván Sapiaín Caro
- Andrés Aldana F.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.23 14:07:46 -04'00'