CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 193

SEMANA DEL 10 AL 16 DE MARZO 2023

# INFORMACIÓN IMPORTANTE

El CSIRT de Gobierno informa que debido a problemas técnicos no ha sido posible publicar las alertas de seguridad cibernéticas y campañas de concientización en nuestro sitio web.

Por lo tanto, los informes e indicadores de compromiso los podrán encontrar en el repositorio de GitHub del CSIRT de Gobierno: www.github.com/csirtcl

# LA SEMANA EN CIFRAS

## IP INFORMADAS

**21**

IP advertidas en múltiples campañas de phishing y de malware.

## URL ADVERTIDAS

**41**

asociadas a sitios fraudulentos y campañas de phishing y malware

## HASH REPORTADOS

**17**

asociadas a múltiples campañas de phishing con archivos que contienen malware

## PARCHES COMPARTIDOS

**94**

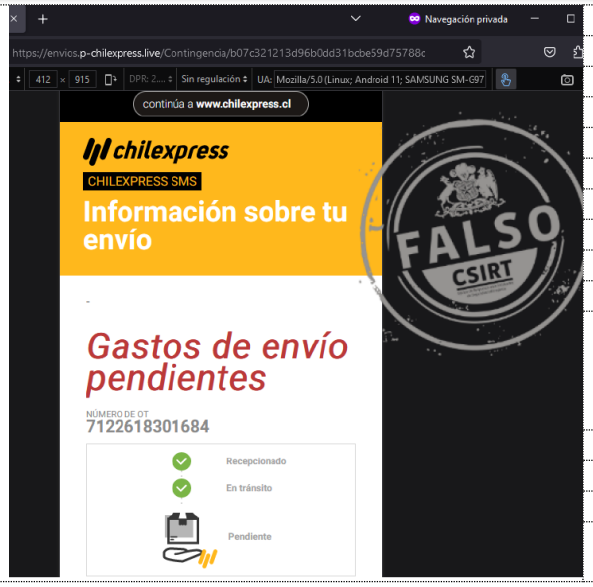
Las mitigaciones son útiles en productos de Microsoft y Fortinet.

# CONTENIDO

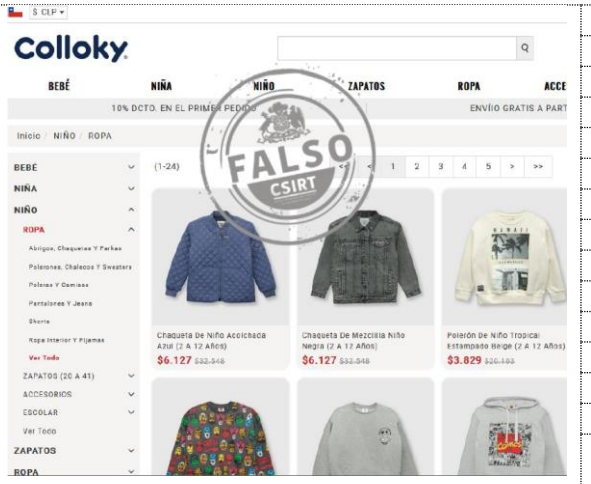

1. Sitios fraudulentos ..... 4
2. Phishing ..... 10
3. Malware ..... 13
4. Vulnerabilidades ..... 15
5. Concientización ..... 20
6. Recomendaciones y buenas prácticas ..... 21
7. Muro de la Fama ..... 22


CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

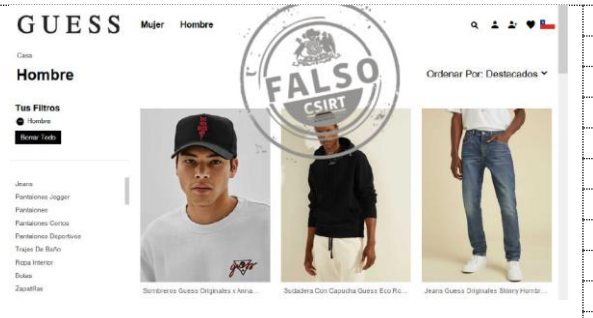
## 1. Sitios fraudulentos




| CSIRT advierte sitio que suplanta a Chilexpress | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01249-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://qsmart[.]cl/chilexpress<br>https://r.p-chilexpress[.]live/r/HjHsN5H<br>https://envios.p-chilexpress[.]live/Contingencia/b07c321213d96b0dd31bcbe59d75788c | |
| **Dirección IP** | |
| [80.78.22.44] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01249-01.txt | |

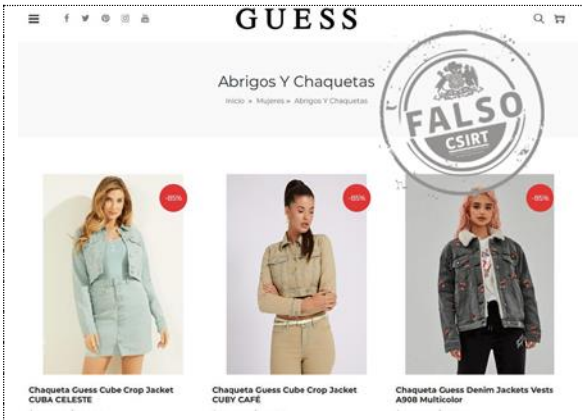



| CSIRT alerta página web que suplanta a Colloky | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01250-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://www.clothespromo[.]online/ | |
| **Dirección IP** | |
| [23.252.71.142] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01250-01.txt | |

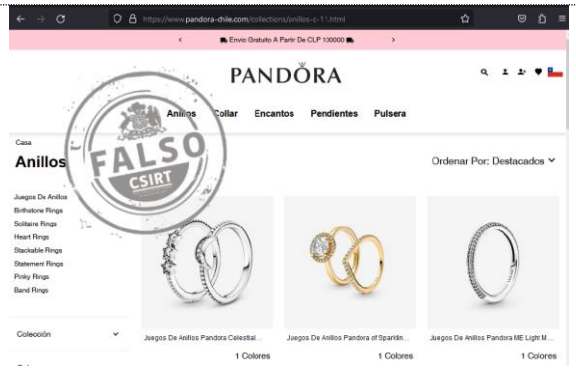



| CSIRT alerta página web que suplanta a Guess | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01251-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://www.guesschileoutlet[.]com | |
| **Dirección IP** | |
| [196.196.231.198] | |

| | |
|---|---|
| | **Enlace para revisar IoC:** |
| | https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01251-01.txt |



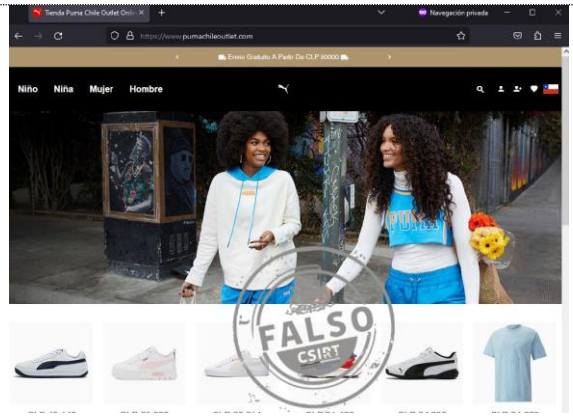

| | |
|---|---|
| **CSIRT advierte sitio que suplanta a Guess** | |
| Alerta de seguridad cibernética | 8FFR23-01252-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://www.cl-guess[.]shop/ | |
| **Dirección IP** | |
| [172.67.205.186] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01252-01.txt | |



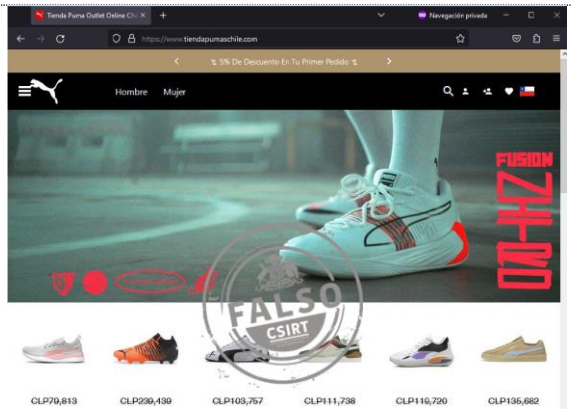

| | |
|---|---|
| **CSIRT alerta de página web que suplanta a Pandora** | |
| Alerta de seguridad cibernética | 8FFR23-01253-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://www.pandora-chile[.]com/ | |
| **Dirección IP** | |
| [196.196.101.105] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01253-01.txt | |


| | |
|---|---|
| **CSIRT alerta sitio web falso de Pandora** | |
| Alerta de seguridad cibernética | 8FFR23-01254-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://www.pandora-chile[.]com/ | |
| **Dirección IP** | |
| [196.196.154.254] | |
| **Enlace para revisar IoC:** | |

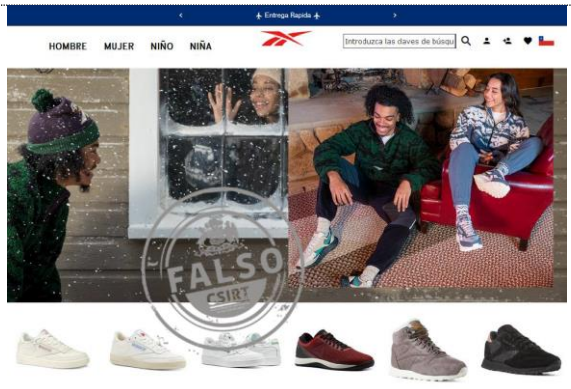
| | |
|---|---|
| | https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01254-01.txt |




| CSIRT advierte página web que suplanta a Puma | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01255-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://www.pumachileoutlet[.]com/ | |
| **Dirección IP** | |
| [165.231.154.176] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01255-01.txt | |

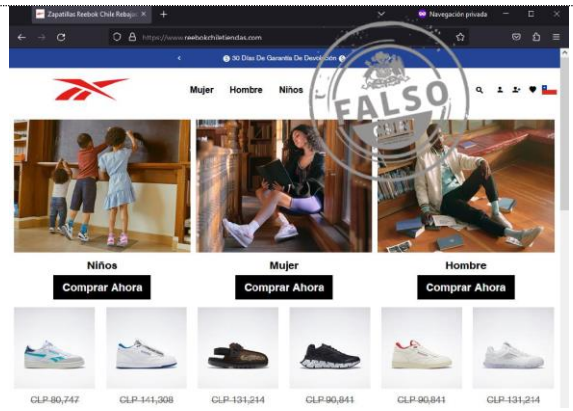



| CSIRT alerta de sitio web falso de Puma | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01256-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://www.tiendapumaschile[.]com/ | |
| **Dirección IP** | |
| [5.157.59.45] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01256-01.txt | |




| CSIRT informa de página web que suplanta a Reebok | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01257-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://www.reebok-chile[.]com/ | |
| **Dirección IP** | |
| [165.231.154.138] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Regis | |

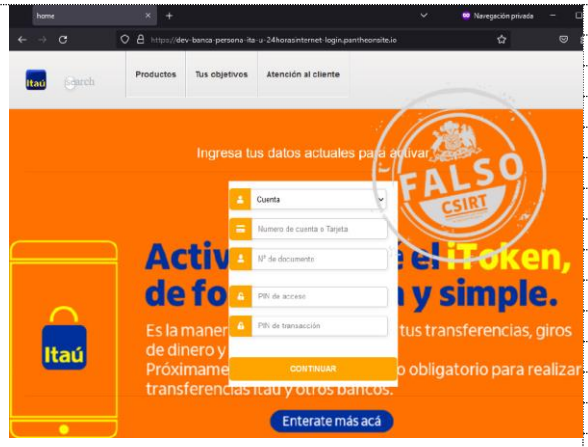
| | |
|---|---|
| | tros%20o%20Identidad_8FFR23-01257-01.txt |



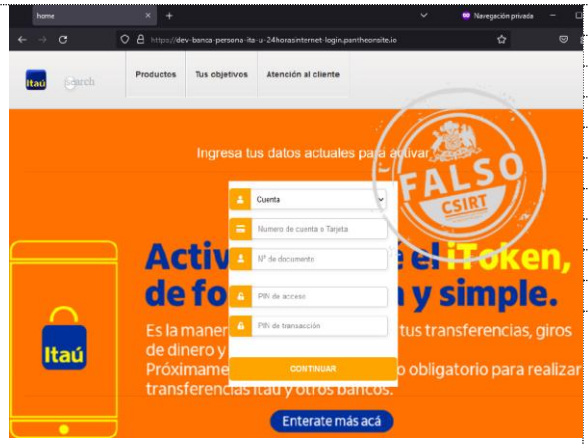

| CSIRT advierte sitio web falso que suplanta a Reebok | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01258-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://www.reebok-chile[.]com/ | |
| **Dirección IP** | |
| [196.196.101.113] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01258-01.txt | |


| CSIRT advierte sitio web falso que suplanta a Banco Itaú | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01259-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 14 de marzo de 2023 |
| Última revisión | 14 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://dev-alertpyitau.pantheonsite[.]io/ | |
| **Dirección IP** | |
| [23.185.0.3] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01259-01.txt | |

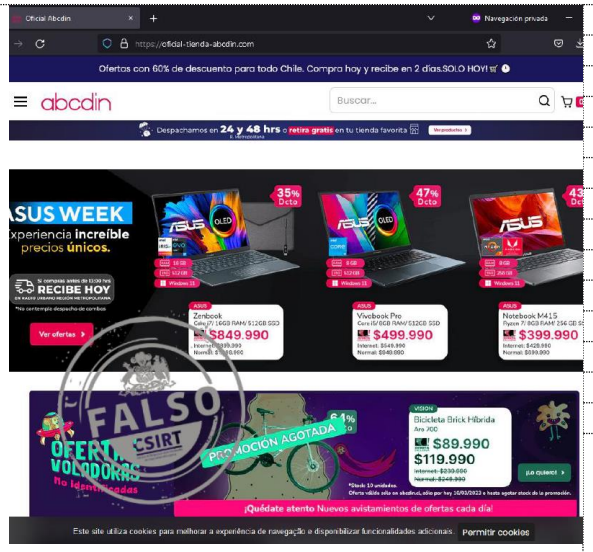

| CSIRT advierte sitio web falso que suplanta a Banco Itaú | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01260-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 14 de marzo de 2023 |
| Última revisión | 14 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://dev-login-seguridad-homeitau.pantheonsite[.]io/ | |
| **Dirección IP** | |
| [23.185.0.2] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01260-01.txt | |




| CSIRT advierte sitio web falso que suplanta a Banco Itaú | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01261-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 14 de marzo de 2023 |
| Última revisión | 14 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://dev-banca-persona-ita-u-24horasinternet-login.pantheonsite[.]io/ | |
| **Dirección IP** | |
| [23.185.0.4] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01261-01.txt | |

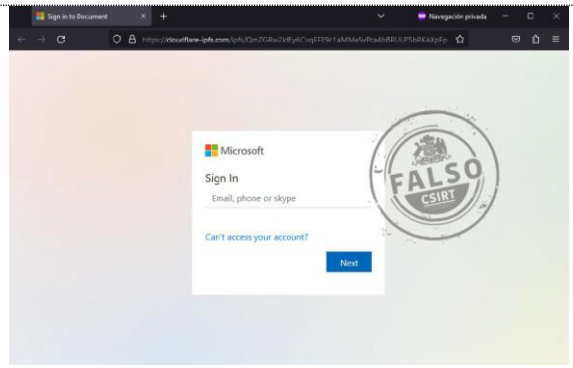



| CSIRT advierte sitio web falso que suplanta a Banco Itaú | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01262-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 14 de marzo de 2023 |
| Última revisión | 14 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://dev-ingresar-portal-de-seguridad-itau.pantheonsite.io/<br>https://dev-00989.pantheonsite.io/<br>http://dev-glmane2s.pantheonsite.io<br>https://dev-seguridadenlinea-homeitaupy.pantheonsite.io/<br>https://dev-itaupyrj.pantheonsite.io/<br>https://dev-seguridadenlinea-homeitau.pantheonsite.io/<br>https://dev-iayuloginsecurpy.pantheonsite.io/<br>https://dev-itaupycli.pantheonsite.io/<br>https://dev-ltaupyequipo.pantheonsite.io/<br>https://dev-verifiaccountnewww.pantheonsite.io/<br>https://dev-glmane2s.pantheonsite.io/<br>https://dev-alertpyitau.pantheonsite.io/<br>https://dev-autenticar-datoscuenta-itaupy.pantheonsite.io/ | |
| **Dirección IP** | |
| [23.185.0.2-3-4] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01262-01.txt | |




| CSIRT advierte sitio web falso que suplanta a ABCDin | |
|---|---|
| Alerta de seguridad cibernética | 8FFR23-01263-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 15 de marzo de 2023 |
| Última revisión | 15 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL sitio falso** | |
| https://oficial-tienda-abcdin[.]com/ | |
| **Dirección IP** | |
| [23.227.38.67] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Falsificaci%C3%B3n%20de%20Registros%20o%20Identidad_8FFR23-01263-01.txt | |

## 2. Phishing

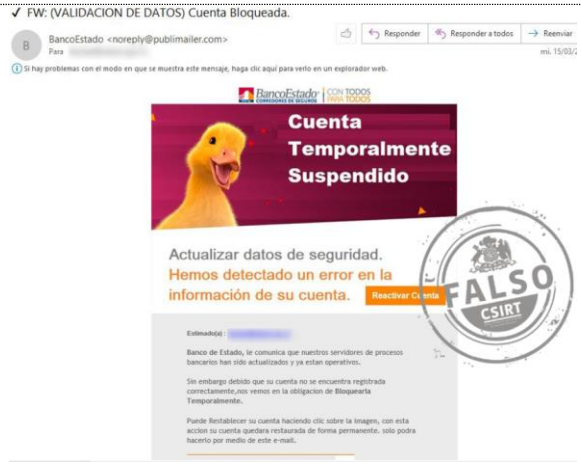



| CSIRT alerta de campaña de phishing que suplanta a Microsoft | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00769-02 (actualización) |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 16 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| falcon-calliope-83ry.squarespace[.]com | |
| **URL sitio falso** | |
| https[:]//cloudflare-ipfs[.]com/ipfs/QmZGRw2kfEy6CvqFFE9c1aMMeSvPca4bBRULP5bRKAXpFp | |
| **Dirección IP** | |
| [104.17.96.13] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00769-02.txt | |


| CSIRT alerta campaña de phishing que suplanta a BancoEstado | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00770-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| https://containd3structible[.]com/activacion/cuenta-ffca/ | |
| **URL sitio falso** | |
| https://nwmepsonpatito[.]club/1678739215/imagenes/_personas/home/default.asp | |
| **Dirección IP** | |
| [172.67.131.190] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00770-01.txt | |

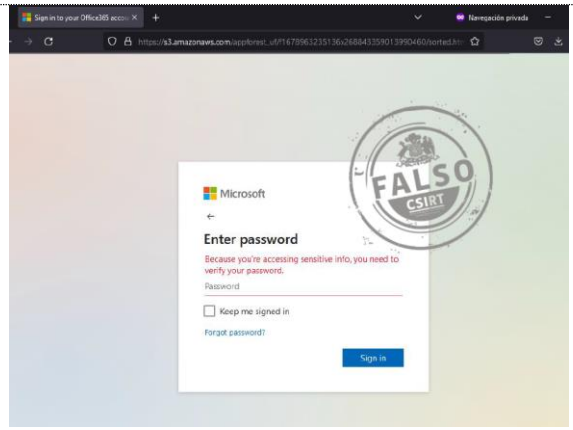

| CSIRT advierte campaña de phishing que suplanta a BancoEstado | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00771-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 13 de marzo de 2023 |
| Última revisión | 13 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| https://bit[.]ly/3BohsH2<br>http://139.59.82[.]7/cdabdc4669e50f6d9288b990cf8fccea/64229fbd812b67cfd4 | |

| | |
|---|---|
| | fcf98f57b6c1ea/1c3861b1d9e4fd3c0b2849b30964cb99YY?p=rip |
| | **URL sitio falso** |
| | https://cuenta-banestado.web[.]app/7SBCJUUEF6SYBGT/cad?source=rja&node=gqcbqqc2ejgaa |
| | **Dirección IP** |
| | [172.64.171.15] |
| | **Enlace para revisar IoC:** |
| | https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00771-01.txt |




| | |
|---|---|
| **CSIRT informa campaña de phishing que suplanta a BancoEstado** | |
| Alerta de seguridad cibernética | 8FPH23-00772-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 15 de marzo de 2023 |
| Última revisión | 15 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| https://fogapehomeunder[.]info/Solicitud_Aprobada/cuenta-rsqg/ | |
| **URL sitio falso** | |
| https://underzonaportal[.]info/1678886730/imagenes/_personas/home/default.asp | |
| **Dirección IP** | |
| [213.136.93.171] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00772-01.txt | |


| | |
|---|---|
| **CSIRT alerta campaña de phishing que suplanta a BancoEstado** | |
| Alerta de seguridad cibernética | 8FPH23-00773-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 15 de marzo de 2023 |
| Última revisión | 15 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| https://fogapehomeunder[.]info/Solicitud_Aprobada/cuenta-rsqg/ | |
| **URL sitio falso** | |
| https://underzonaportal[.]info/1678975232/imagenes/_personas/home/default.asp | |
| **Dirección IP** | |
| [213.136.93.171] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00773-01.txt | |




| CSIRT alerta campaña de phishing que suplanta a Microsoft | |
|---|---|
| Alerta de seguridad cibernética | 8FPH23-00774-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 15 de marzo de 2023 |
| Última revisión | 15 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **URL redirección** | |
| http://it.fashionnetwork[.]com/nl/?nl=241666&uc=4073310&link=https%3A%2F%2Fkhapang.com%2Fnew%2Fauth%2F/2gznpt%2F%2F%2F%2Ftest@csirt.gob.cl | |
| **URL sitio falso** | |
| https://s3.amazonaws[.]com/appforest_uf/f1678963235136x268843359013990460/sorted.html?email=test@csirt.gob.cl | |
| **Dirección IP** | |
| [52.217.92.246] | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/Fraude/blob/main/Phishing_8FPH23-00774-01.txt | |

## 3. Malware

| Imagen del mensaje | CSIRT advierte campaña de phishing con malware con falsa factura pendiente de pago | |
|---|---|---|
|  | Alerta de seguridad cibernética | 2CMV23-00404-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Malware |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 10 de marzo de 2023 |
| | Última revisión | 10 de marzo de 2023 |
| | **Indicadores de compromiso** | |
| | **Asunto** | |
| | Reciba su Factura digital. Pago pendiente. | |
| | **Correo de Salida** | |
| | facturaenlinea@network.org | |
| | **SHA256** | |
| | 74f711b89d63666185c0ec841257d297b3b250fffa70b7f19adc9ac673feeb28<br>cd38912cfb9229fb7edd3dd0fa109e727903c20445385b2d15749d2ab95d6309<br>806c48155540240aa973980549f0a96a989369be8fc5255d4dbc03f8e11a2fd4<br>eac572bed2d66ffc1f3f5c5372d53fe0bc3fab76599b5aea6fb013ea1adbcbab<br>4be77b79f83d9af63b7cf9b3e0ef1072ac0768260491c161fef118ce9618d8fe<br>98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b<br>1b4fb02896577539225fdc43508db518064796e045753d6c7b1d9e1a9f49a3f3 | |
| | **Enlace para revisar IoC:** | |
| | https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00404-01.txt | |

| Imagen del mensaje | CSIRT advierte campaña de phishing con malware que suplanta a Western Union | |
|---|---|---|
|  | Alerta de seguridad cibernética | 2CMV23-00405-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Malware |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 14 de marzo de 2023 |
| | Última revisión | 14 de marzo de 2023 |
| | **Indicadores de compromiso** | |
| | **Asunto** | |
| | (sin asunto) | |
| | **Correo de Salida** | |
| | azzwestbr@hotmail.com | |
| | **SHA256** | |
| | ef4affb6a91e67cd7b1ee492589e18cf700653e6d6b32a66d5b1747ab861ef56<br>9472d7a4e6028ef04c5b1a1a57844a3198229bd209b68c1d3534123e4fad8fb2<br>3349be17dc030f34b0d2a9067897b91b45d87d585531fc108463be9174aab3c8<br>af3ebfddb7d9356ba8272014df8a10fed3c0ce25f17d0958e34daee4bef90b77<br>fd133ec88368b5125c6e886efc0f30e345eec49a887169a904601fb3c5e50dcf | |
| | **Enlace para revisar IoC:** | |
| | https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00405-01.txt | |


| CSIRT advierte campaña de phishing con malware que suplanta a Western Union | |
|---|---|
| Alerta de seguridad cibernética | 2CMV23-00406-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Malware |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 16 de marzo de 2023 |
| Última revisión | 16 de marzo de 2023 |
| **Indicadores de compromiso** | |
| **Asunto** | |
| 3-Tercera_Notificación_Del_Proceso_Llevado_En_Contra_Referencia_Nro°_29873893_21_Radicado_#93903030-32 | |
| **Correo de Salida** | |
| luisa.9117.sierra@gmail.com | |
| **SHA256** | |
| ef4affb6a91e67cd7b1ee492589e18cf700653e6d6b32a66d5b1747ab861ef569472d7a4e6028ef04c5b1a1a57844a3198229bd209b68c1d3534123e4fad8fb23349be17dc030f34b0d2a9067897b91b45d87d585531fc108463be9174aab3c8af3ebfddb7d9356ba8272014df8a10fed3c0ce25f17d0958e34daee4bef90b77fd133ec88368b5125c6e886efc0f30e345eec49a887169a904601fb3c5e50dcf | |
| **Enlace para revisar IoC:** | |
| https://github.com/csirtcl/CodigoMalicioso/blob/main/Phishing-Malware_2CMV23-00406-01.txt | |

## 4. Vulnerabilidades


| CSIRT alerta de vulnerabilidad crítica en Atlassian Jira Service Management | |
|---|---|
| Alerta de seguridad cibernética | 9VSA23-00802-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Crítico |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de marzo de 2023 |
| Última revisión | 10 de marzo de 2023 |

**CVE**

| | | |
|---|---|---|
| CVE-2022-45861 | CVE-2023-25611 | CVE-2022-41328 |
| CVE-2022-42476 | CVE-2022-39951 | CVE-2022-40676 |
| CVE-2022-29056 | CVE-2022-41333 | CVE-2022-39953 |
| CVE-2022-41329 | CVE-2023-23776 | CVE-2022-27490 |
| CVE-2023-25605 | CVE-2022-22297 | |

**Fabricantes**

Fortinet

**Productos afectados**

Al menos FortiAnalyzer versión 6.0.0 a 6.0.4
Al menos FortiManager versión 6.0.0 a 6.0.4
Al menos FortiPortal 4.1 todas las versiones
FortiPortal 4.2 todas las versiones
FortiAnalyzer 6.4 todas las versiones
FortiAnalyzer versión 6.4.0 a 6.4.10
FortiAnalyzer versión 7.0.0 a 7.0.5
FortiAnalyzer versión 7.2.0 a 7.2.1
FortiAuthenticator versión 5.4 todas las versiones
FortiAuthenticator versión 5.5 todas las versiones
FortiAuthenticator versión 6.0 todas las versiones
FortiAuthenticator versión 6.1 todas las versiones
FortiAuthenticator versión 6.2 todas las versiones
FortiAuthenticator versión 6.3 todas las versiones
FortiAuthenticator versión 6.4 todas las versiones
FortiDeceptor versión 1.0 todas las versiones
FortiDeceptor versión 1.1 todas las versiones
FortiDeceptor versión 2.0 todas las versiones
FortiDeceptor versión 2.1 todas las versiones
FortiDeceptor versión 3.0 todas las versiones
FortiDeceptor versión 3.1 todas las versiones
FortiMail versión 6.0.0 a 6.0.9
FortiMail versión 6.2.1 a 6.2.4
FortiMail versión 6.4.0
Ministerio del Interior y Seguridad Pública Página 4 de 5
FortiNAC todas las versiones 8.8, 8.7, 8.6, 8.5, 8.3
FortiNAC versión 9.1.0 a 9.1.8
FortiNAC versión 9.2.0 a 9.2.6
FortiNAC versión 9.4.0 a 9.4.1
FortiOS 6.0 todas las versiones
FortiOS 6.2 todas las versiones
FortiOS versión 6.4.0 a 6.4.11
FortiOS versión 7.0.0 a 7.0.9
FortiOS versión 7.2.0 a 7.2.3

| | |
|---|---|
| | FortiPortal 5.0 todas las versiones<br>FortiPortal 5.1 todas las versiones<br>FortiPortal 5.2 todas las versiones<br>FortiPortal 5.3 todas las versiones<br>FortiPortal versión 6.0.0 a 6.0.9 al menos<br>FortiProxy 1.1 todas las versiones<br>FortiProxy 1.1 todas las versiones.<br>FortiProxy 1.2 todas las versiones<br>FortiProxy 1.2 todas las versiones.<br>FortiProxy 7.0.x, 2.0.x, 1.2.x, 1.1.x: Impacto es pequeño, ya que no tienen VDOM.<br>FortiProxy versión 1.1.0 a 1.1.6<br>FortiProxy versión 1.2.0 a 1.2.13<br>FortiProxy versión 2.0.0 a 2.0.11<br>FortiProxy versión 7.0.0 a 7.0.7<br>FortiProxy versión 7.0.0 a 7.0.8<br>FortiProxy versión 7.2.0 a 7.2.1<br>FortiProxy versión 7.2.0 a 7.2.2<br>FortiRecorder 6.0.11 a 6.0.0<br>FortiRecorder 6.4.3 y anteriores.<br>FortiRecorder todas las versiones 2.7<br>FortiRecorder todas las versiones 6.0<br>FortiRecorder versión 6.4.0 a 6.4.3<br>FortiSOAR versión 7.3.0 a 7.3.1<br>FortiSwitch versión 6.0.0 a 6.0.7<br>FortiSwitch versión 6.2.0 a 6.2.7<br>FortiSwitch versión 6.4.0 a 6.4.10<br>FortiSwitch versión 7.0.0 a 7.0.4<br>FortiWeb 6.4 todas las versiones<br>FortiWeb todas las versiones 6.0<br>FortiWeb todas las versiones 6.1<br>FortiWeb todas las versiones 6.2<br>FortiWeb versión 6.3.0 a 6.3.17<br>FortiWeb versión 6.3.6 a 6.3.20<br>FortiWeb versión 6.4.0 a 6.4.1<br>FortiWeb versión 7.0.0 a 7.0.2 |
| | **Enlaces para revisar el informe:** |
| | https://github.com/csirtcl/Vulnerabilidades/blob/main/9VSA23-00802-01.pdf |


| CSIRT alerta de vulnerabilidades del Update Tuesday de Microsoft marzo 2023 | |
|---|---|
| Alerta de seguridad cibernética | 9VSA23-00803-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Crítico |
| TLP | Blanco |
| Fecha de lanzamiento original | 10 de marzo de 2023 |
| Última revisión | 10 de marzo de 2023 |

**CVE**

| | | |
|---|---|---|
| CVE-2023-1017 | CVE-2023-23409 | CVE-2023-24867 |
| CVE-2023-1018 | CVE-2023-23410 | CVE-2023-24868 |
| CVE-2023-21708 | CVE-2023-23411 | CVE-2023-24869 |
| CVE-2023-22490 | CVE-2023-23412 | CVE-2023-24870 |
| CVE-2023-22743 | CVE-2023-23413 | CVE-2023-24871 |
| CVE-2023-23383 | CVE-2023-23414 | CVE-2023-24872 |
| CVE-2023-23385 | CVE-2023-23415 | CVE-2023-24876 |
| CVE-2023-23388 | CVE-2023-23416 | CVE-2023-24879 |

| | | |
|---|---|---|
| CVE-2023-23389 | CVE-2023-23417 | CVE-2023-24880 |
| CVE-2023-23391 | CVE-2023-23418 | CVE-2023-24882 |
| CVE-2023-23392 | CVE-2023-23419 | CVE-2023-24890 |
| CVE-2023-23393 | CVE-2023-23420 | CVE-2023-24891 |
| CVE-2023-23394 | CVE-2023-23421 | CVE-2023-24892 |
| CVE-2023-23395 | CVE-2023-23422 | CVE-2023-24906 |
| CVE-2023-23396 | CVE-2023-23423 | CVE-2023-24907 |
| CVE-2023-23397 | CVE-2023-23618 | CVE-2023-24908 |
| CVE-2023-23398 | CVE-2023-23946 | CVE-2023-24909 |
| CVE-2023-23399 | CVE-2023-24856 | CVE-2023-24910 |
| CVE-2023-23400 | CVE-2023-24857 | CVE-2023-24911 |
| CVE-2023-23401 | CVE-2023-24858 | CVE-2023-24913 |
| CVE-2023-23402 | CVE-2023-24859 | CVE-2023-24919 |
| CVE-2023-23403 | CVE-2023-24861 | CVE-2023-24920 |
| CVE-2023-23404 | CVE-2023-24862 | CVE-2023-24921 |
| CVE-2023-23405 | CVE-2023-24863 | CVE-2023-24922 |
| CVE-2023-23406 | CVE-2023-24864 | CVE-2023-24923 |
| CVE-2023-23407 | CVE-2023-24865 | CVE-2023-24930 |
| CVE-2023-23408 | CVE-2023-24866 | |

**Fabricantes**

Fortinet

**Productos afectados**

Azure HDInsights
Azure Service Fabric 9.1 for Ubuntu
Azure Service Fabric 9.1 for Windows
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Dynamics 365 (on-premises) version 9.1
Ministerio del Interior y Seguridad Pública Página 3 de 6
Microsoft Edge (Chromium-based)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Malware Protection Engine
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office for Android
Microsoft Office for Universal
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)

| | |
|---|---|
| | Microsoft Outlook 2016 (32-bit edition)<br>Microsoft Outlook 2016 (64-bit edition)<br>Microsoft SharePoint Enterprise Server 2013 Service Pack 1<br>Microsoft SharePoint Enterprise Server 2016<br>Microsoft SharePoint Foundation 2013 Service Pack 1<br>Microsoft SharePoint Server 2019<br>Microsoft SharePoint Server Subscription Edition<br>Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)<br>Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)<br>Microsoft Visual Studio 2022 version 17.0<br>Microsoft Visual Studio 2022 version 17.2<br>Microsoft Visual Studio 2022 version 17.4<br>Microsoft Visual Studio 2022 version 17.5<br>OneDrive for Android<br>OneDrive for iOS<br>OneDrive for MacOS Installer<br>Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Ministerio del Interior y Seguridad Pública Página 4 de 6<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 20H2 for 32-bit Systems<br>Windows 10 Version 20H2 for ARM64-based Systems<br>Windows 10 Version 20H2 for x64-based Systems<br>Windows 10 Version 21H2 for 32-bit Systems<br>Windows 10 Version 21H2 for ARM64-based Systems<br>Windows 10 Version 21H2 for x64-based Systems<br>Windows 10 Version 22H2 for 32-bit Systems<br>Windows 10 Version 22H2 for ARM64-based Systems<br>Windows 10 Version 22H2 for x64-based Systems<br>Windows 11 version 21H2 for ARM64-based Systems<br>Windows 11 version 21H2 for x64-based Systems<br>Windows 11 Version 22H2 for ARM64-based Systems<br>Windows 11 Version 22H2 for x64-based Systems<br>Windows Server 2008 for 32-bit Systems Service Pack 2<br>Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 for x64-based Systems Service Pack 2<br>Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2019 (Server Core installation)<br>Windows Server 2022<br>Windows Server 2022 (Server Core installation) |

| | |
|---|---|
| | Enlaces para revisar el informe:<br>https://github.com/csirtcl/Vulnerabilidades/blob/main/9VSA23-00803-01.pdf |

## 5. Concientización

### Charla virtual: Cómo identificar el ciberacoso y cómo abordarlo

Este martes el CSIRT de Gobierno, junto a la Fundación Katy Summer y la Unidad de Ciberseguridad del Ministerio del Interior llevaron a cabo una charla online sobre formas para identificar el ciberacoso en nuestros niños, y también sobre cómo lidiar con él. Pueden ver el video con la grabación de la instancia aquí: https://www.youtube.com/watch?v=0tec0FhH3O4.

## 6. Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar que los sitios web a los que se ingrese sean los oficiales.

## 7. Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar campañas de phishing, malware y/o sitios fraudulentos.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono 1510), siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Emilia Vergara
- Juan Sebastián Henríquez Iturra
- Juan Rodrigo Sepúlveda Romo
- Francisco Javier Gutiérrez
- Bárbara Nicol Hills Lira
- Marcelo Pizarro
- Marcelo Patricio Corales Barrera
- Antonia Espinoza
- Jhonel Santiago García Roa
- Francisco Leonel Herrera Goñía
- Tomás Pablo Crespo Guzmán
- Fernando Flores Tobar
- Tiare Escarlett Lantadilla González
- Jorge Ignacio Molina Martínez
- Sandra Elizabeth Olivares Araya