



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 187

Semana del 27 de enero al 2 de febrero

## **PARCHES COMPARTIDOS**

**3**

Las mitigaciones son útiles en productos de OpenEMR, QNAP y Lexmark.



## **IP INFORMADAS**

**8**



## **URL ADVERTIDAS**

**13**



# CONTENIDO

1. Phishing .....	3
2. Vulnerabilidades .....	8
3. Concientización .....	10
4. Recomendaciones y buenas prácticas .....	12
5. Muro de la Fama .....	13



**CSIRT**

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

## 1. Phishing



### CSIRT alerta de nueva campaña de phishing que suplanta al SII

Alerta de seguridad cibernética	8FPH23-00731-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2023
Última revisión	27 de enero de 2023

#### Indicadores de compromiso

##### URL sitio falso

[https://ppcproyectos\[.\]com/incoming.php?id=TYDWITCABYEVVZMTFEWZXDURJWGKMDLNAJCVVWEKJKAESKALSVXDZSBHXRESJWLREDOOFWCWUYHPKWGBM](https://ppcproyectos[.]com/incoming.php?id=TYDWITCABYEVVZMTFEWZXDURJWGKMDLNAJCVVWEKJKAESKALSVXDZSBHXRESJWLREDOOFWCWUYHPKWGBM)

##### Dirección IP

[198.59.144.138]

##### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph23-00731-01/>

<https://www.csirt.gob.cl/media/2023/01/8FPH23-00731-01.pdf>



### CSIRT alerta de nueva campaña de phishing que suplanta a Impuestos Internos

Alerta de seguridad cibernética	8FPH23-00732-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2023
Última revisión	27 de enero de 2023

#### Indicadores de compromiso

##### Dirección IP

[198.59.144.138]

##### Enlaces para revisar el informe:

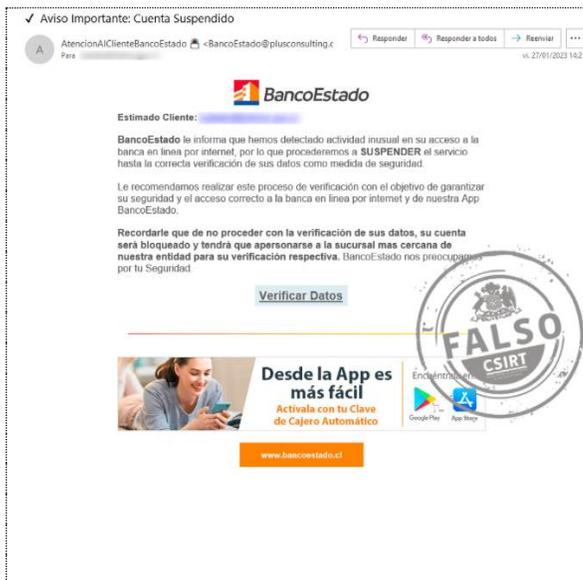
<https://www.csirt.gob.cl/alertas/8fph23-00732-01/>

<https://www.csirt.gob.cl/media/2023/01/8FPH23-00732-01.pdf>

# Boletín de Seguridad Cibernética N° 187

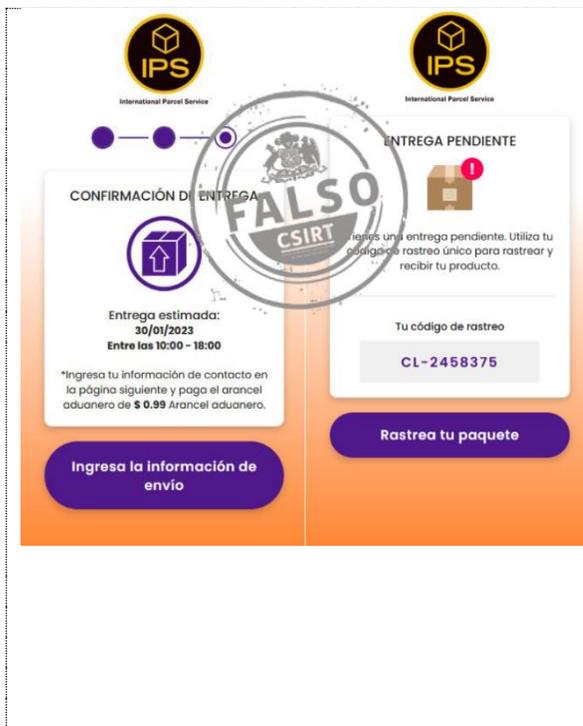
Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno  
Ministerio del Interior y Seguridad Pública  
Gobierno de Chile

BOLETÍN 13BCS23-00196-01 | SEMANA DEL 27 DE ENERO AL 2 DE FEBRERO DE 2023



## CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado

Alerta de seguridad cibernética	8FPH23-00733-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2023
Última revisión	27 de enero de 2023
<b>Indicadores de compromiso</b>	
<b>URL redirección</b>	
<a href="https://cartoonpuzzl3s[.]com/activacion/cuenta-bpwz/">https://cartoonpuzzl3s[.]com/activacion/cuenta-bpwz/</a>	
<b>URL sitio falso</b>	
<a href="https://xtraillconver[.]com/1674842723/imagenes/_personas/home/default.asp">https://xtraillconver[.]com/1674842723/imagenes/_personas/home/default.asp</a>	
<b>Dirección IP</b>	
[138.128.189.154]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8fph23-00733-01/">https://www.csirt.gob.cl/alertas/8fph23-00733-01/</a>	
<a href="https://www.csirt.gob.cl/media/2023/01/8FPH23-00733-01.pdf">https://www.csirt.gob.cl/media/2023/01/8FPH23-00733-01.pdf</a>	



## CSIRT alerta de campaña de phishing por SMS (smishing) que suplanta a CorreosChile

Alerta de seguridad cibernética	8FPH23-00734-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de enero de 2023
Última revisión	30 de enero de 2023
<b>Indicadores de compromiso</b>	
<b>URL sitio falso</b>	
<a href="https://smartgift[.]live/ips_cl/?cep=ADpcvY4BIMnvUrAW9fx58sqTbjRe25a7RiuOiwXC_-2Y2fTYOJmDp42E-8Htv8msrXSiDuN0bmLZZ5ZWDcUpZCeDoka_1cVJ7OpbjLvJPouTEFc7bd71_Dhsbw-xY61uHCyLqTHq-zeqR6mUD0VfgX4b38enLC1YHiwW008epixUtQfSnEx6FvbYOTVC_miypOqhiaCoUbhLDqVUU sEQlao8IK_cS3Qy98gWLwtglnZfs2irz1qHz-oXXeTHfgSxhosxbT37OxtT-ViuXGUoYRIQe_6B2UbGjYCCsXni3mijBdhc2NdzNyt8qok7lSfw670FxFhsfBDA-9i9XG4uDoFRPVP_v-MuXCpEoEraN9SLZ1_eQJs6u5hQZfchSKHb&amp;lptoken=165974c584b3519f647c">https://smartgift[.]live/ips_cl/?cep=ADpcvY4BIMnvUrAW9fx58sqTbjRe25a7RiuOiwXC_-2Y2fTYOJmDp42E-8Htv8msrXSiDuN0bmLZZ5ZWDcUpZCeDoka_1cVJ7OpbjLvJPouTEFc7bd71_Dhsbw-xY61uHCyLqTHq-zeqR6mUD0VfgX4b38enLC1YHiwW008epixUtQfSnEx6FvbYOTVC_miypOqhiaCoUbhLDqVUU sEQlao8IK_cS3Qy98gWLwtglnZfs2irz1qHz-oXXeTHfgSxhosxbT37OxtT-ViuXGUoYRIQe_6B2UbGjYCCsXni3mijBdhc2NdzNyt8qok7lSfw670FxFhsfBDA-9i9XG4uDoFRPVP_v-MuXCpEoEraN9SLZ1_eQJs6u5hQZfchSKHb&amp;lptoken=165974c584b3519f647c</a>	
<b>Dirección IP</b>	
[84.32.190.20]	
<b>Enlaces para revisar el informe:</b>	
<a href="https://www.csirt.gob.cl/alertas/8fph23-00734-01/">https://www.csirt.gob.cl/alertas/8fph23-00734-01/</a>	
<a href="https://www.csirt.gob.cl/media/2023/01/8FPH23-00734-01.pdf">https://www.csirt.gob.cl/media/2023/01/8FPH23-00734-01.pdf</a>	

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>  
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl  
[@csirtgob](https://twitter.com/csirtgob)  
<https://www.linkedin.com/company/csirt-gob>



## CSIRT alerta de nueva campaña de phishing que suplanta al SII

Alerta de seguridad cibernética	8FPH23-00735-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de enero de 2023
Última revisión	30 de enero de 2023

### Indicadores de compromiso

#### URL sitio falso

[https://tequilamisorpresa\[.\]com/ytweshdg.php?id=wkwxifybauwrkeqzgapwyjkgypdfwqpuqkfmkewdounxwysesjljrxcbgledjfbctzpjhejk](https://tequilamisorpresa[.]com/ytweshdg.php?id=wkwxifybauwrkeqzgapwyjkgypdfwqpuqkfmkewdounxwysesjljrxcbgledjfbctzpjhejk)

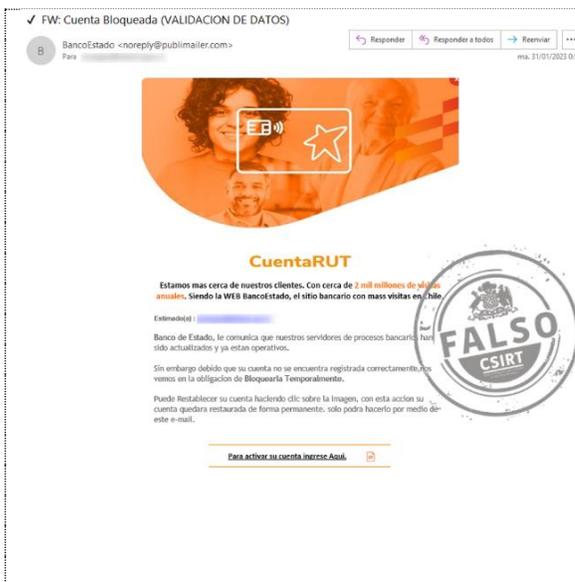
#### Dirección IP

[65.99.252.243]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph23-00735-01/>

<https://www.csirt.gob.cl/media/2023/01/8FPH23-00735-01.pdf>



## CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH23-00736-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 de enero de 2023

### Indicadores de compromiso

#### URL sitio redirección

[https://ucmstudio\[.\]info/activacion/cuenta-aotq/](https://ucmstudio[.]info/activacion/cuenta-aotq/)

#### URL sitio falso

[https://prestamoonlineibk\[.\]net/1675171907/imagenes/\\_personas/home/default.asp](https://prestamoonlineibk[.]net/1675171907/imagenes/_personas/home/default.asp)

#### Dirección IP

[186.64.119.85]

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/alertas/8fph23-00736-01/>

<https://www.csirt.gob.cl/media/2023/01/8FPH23-00736-01.pdf>

<p>✓ Aviso Importante: Cuenta Suspendido</p> <p>AtencionClienteBancoEstado &lt;BancoEstado@plusconsulting.cl&gt;</p> <p>Para</p> <p>ma. 31/01/2023 13:08</p> 	<p><b>CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado</b></p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00737-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Phishing</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>31 de enero de 2023</td> </tr> <tr> <td>Última revisión</td> <td>31 de enero de 2023</td> </tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b> https://cartoonpuzzl3s[.]com/activacion/cuenta-htna/</p> <p><b>URL sitio falso</b> https://xtrailconver[.]com/1675189288/imagenes/_personas/home/default.asp</p> <p><b>Dirección IP</b> [138.128.189.154]</p> <p><b>Enlaces para revisar el informe:</b> https://www.csirt.gob.cl/alertas/8fph23-00737-01/ https://www.csirt.gob.cl/media/2023/01/8FPH23-00737-01.pdf</p>	Alerta de seguridad cibernética	8FPH23-00737-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	31 de enero de 2023	Última revisión	31 de enero de 2023
Alerta de seguridad cibernética	8FPH23-00737-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	31 de enero de 2023														
Última revisión	31 de enero de 2023														

<p>✓ Fw: Actividad Inusual (Cuenta Deshabilitada)</p> <p>BancoEstado &lt;bancostado@plusconsulting.cl&gt;</p> <p>Para</p> <p>Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.</p> 	<p><b>CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado</b></p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00738-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Phishing</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>31 de enero de 2023</td> </tr> <tr> <td>Última revisión</td> <td>31 de enero de 2023</td> </tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b> https://nwmmayorsa[.]com/activacion/cuenta-igzs/</p> <p><b>URL sitio falso</b> https://nmhportal[.]click/1675190214/imagenes/_personas/home/default.asp</p> <p><b>Dirección IP</b> [104.21.21.215]</p> <p><b>Enlaces para revisar el informe:</b> https://www.csirt.gob.cl/alertas/8fph23-00738-01/ https://www.csirt.gob.cl/media/2023/01/8FPH23-00738-01.pdf</p>	Alerta de seguridad cibernética	8FPH23-00738-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	31 de enero de 2023	Última revisión	31 de enero de 2023
Alerta de seguridad cibernética	8FPH23-00738-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	31 de enero de 2023														
Última revisión	31 de enero de 2023														

<p>✓ Fw: Actividad Inusual (Cuenta Deshabilitada)</p> <p>BancoEstado &lt;bancoestado@plusconsulting.cl&gt; Para [Redacted]</p> <p>Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.</p> 	<p><b>CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado</b></p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00739-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Phishing</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>1 de febrero de 2023</td> </tr> <tr> <td>Última revisión</td> <td>1 de febrero de 2023</td> </tr> </table> <p><b>Indicadores de compromiso</b></p> <p><b>URL redirección</b>  <a href="https://ucmstudio[.]info/activacion/cuenta-vbvq/">https://ucmstudio[.]info/activacion/cuenta-vbvq/</a></p> <p><b>URL sitio falso</b>  <a href="https://prestamoonlineibk[.]net/1675256303/imagenes/_personas/home/default.asp">https://prestamoonlineibk[.]net/1675256303/imagenes/_personas/home/default.asp</a></p> <p><b>Dirección IP</b>          [186.64.119.85]</p> <p><b>Enlaces para revisar el informe:</b>  <a href="https://www.csirt.gob.cl/alertas/8fph23-00739-01/">https://www.csirt.gob.cl/alertas/8fph23-00739-01/</a>  <a href="https://www.csirt.gob.cl/media/2023/02/8FPH23-00739-01.pdf">https://www.csirt.gob.cl/media/2023/02/8FPH23-00739-01.pdf</a></p>	Alerta de seguridad cibernética	8FPH23-00739-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	1 de febrero de 2023	Última revisión	1 de febrero de 2023
Alerta de seguridad cibernética	8FPH23-00739-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	1 de febrero de 2023														
Última revisión	1 de febrero de 2023														

## 2. Vulnerabilidades



Ministerio del Interior y Seguridad Pública

**INFORME DE Vulnerabilidad**

**9VSA23-00778-01**  
CSIRT comparte vulnerabilidad crítica en impresoras Lexmark

PARA REGISTRAR | 1510  
UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)

**CSIRT**  
Equipo de Respuesta ante Incidentes de Seguridad Informática

### CSIRT alerta de vulnerabilidad crítica que afecta a productos Lexmark

Alerta de seguridad cibernética	9VSA23-00778-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 de enero de 2023

#### CVE

CVE-2023-23560

#### Fabricantes

Lexmark

#### Productos afectados

Múltiples aparatos Lexmark, los que aparecen listados en su comunicado oficial (<https://publications.lexmark.com/publications/security-alerts/CVE-2023-23560.pdf>).

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00778-01/>

<https://www.csirt.gob.cl/media/2023/01/9VSA22-00778-01.pdf>



Ministerio del Interior y Seguridad Pública

**INFORME DE Vulnerabilidad**

**9VSA23-00779-01**  
CSIRT comparte vulnerabilidad crítica en QNAP NAS

PARA REGISTRAR | 1510  
UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)

**CSIRT**  
Equipo de Respuesta ante Incidentes de Seguridad Informática

### CSIRT comparte información de vulnerabilidad crítica en QNAP NAS

Alerta de seguridad cibernética	9VSA23-00779-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2023
Última revisión	31 de enero de 2023

#### CVE

CVE-2022-27596

#### Fabricantes

QNAP

#### Productos afectados

QTS 5.0.1 y QuTS hero h5.0.1

#### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00779-01/>

<https://www.csirt.gob.cl/media/2023/01/9VSA23-00779-01.pdf>

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>  
Teléfonos: 1510 | + (562) 24863850 | Correo: [soc-csirt@interior.gob.cl](mailto:soc-csirt@interior.gob.cl)  
[@csirtgob](https://twitter.com/csirtgob)  
<https://www.linkedin.com/company/csirt-gob>



## CSIRT alerta de vulnerabilidades críticas en OpenEMR

Alerta de seguridad cibernética	9VSA23-00780-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	2 de febrero de 2023
Última revisión	2 de febrero de 2023

### CVE

CVE-2022-27596

### Fabricantes

OpenEMR

### Productos afectados

CVE no disponible

CVE no disponible

CVE no disponible

### Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00780-01/>

<https://www.csirt.gob.cl/media/2023/02/9VSA23-00780-01.pdf>

## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>  
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl  
 @csirtgob  
 <https://www.linkedin.com/company/csirt-gob>

## 3. Concientización

### Ciberconsejos | Cómo crear una clave segura

Esta semana queremos recordarles la importancia de contar con contraseñas únicas y difíciles de adivinar para los ciberdelincuentes, con los siguientes ciberconsejos. Y es que definir contraseñas que sean fáciles de recordar, pero difíciles de adivinar, es el desafío que tienen los usuarios de internet.

Pueden encontrar la campaña y todas las anteriores que hemos hecho, en nuestro sitio web oficial: [https://www.csirt.gob.cl/recomendaciones/ciberconsejos-clave-segura\\_2023/](https://www.csirt.gob.cl/recomendaciones/ciberconsejos-clave-segura_2023/).



**#Ciberconsejos**  
**Cómo crear una contraseña segura**

**Ejemplo de construcción de una clave robusta**

1. Empieza con una frase fácil de recordar, por ejemplo: CREANDO MI CLAVE SEGURA
2. Cambia algunas letras por números: CR3ANDO\_M1\_CL4V3\_S3GUR4
3. Intercala mayúsculas y minúsculas e incorpora símbolos: Cr3AndO\_M1\_CL4V3\_S3guR4!



**#Ciberconsejos**  
**Cómo crear una contraseña segura**

**Otro ejemplo que empieza de una frase fácil de recordar**

"Chile salió campeón de América en julio de 2015"

Utilizando sólo las letras iniciales, combinadas entre mayúsculas y minúsculas, se podría usar CsCdAe7/15 como contraseña.



**#Ciberconsejos**  
**Cómo crear una contraseña segura**

**Al construir una clave:**

- NUNCA uses datos personales como RUT, teléfono o dirección.
- NO USES cumpleaños, datos o nombres de familiares o mascotas
- NUNCA repitas la misma contraseña en distintas cuentas.



**#Ciberconsejos**  
**Cómo crear una contraseña segura**

- Para tu frase de partida puedes usar la letra de alguna canción, nombres de películas o pasajes de libros.
- Recuerda: entre más usada y frecuente sea una clave, menos segura es. En Chile algunas de las contraseñas más utilizadas, y que no recomendamos utilizar son "123456789" y "colocolo", que está dentro de las 10 claves más repetidas en el país.

## Ciberdiccionario Volumen 28

Los conceptos definidos en el ciberdiccionario del CSIRT de Gobierno esta semana: TIC, actores estatales, sistemas heredados o legacy y OSINT. Pueden encontrar todos los números del ciberdiccionario, junto a nuestros ciberconsejos y otras guías de concientización siempre en <https://www.csirt.gob.cl/recomendaciones/>.

Enlace: <https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-28/>



**OSINT**

Sigla que viene del inglés y significa inteligencia de fuentes abiertas, aquellas de las cuales se obtienen datos de una persona u organización de forma libre. La OSINT es usada tanto por criminales, para hallar puntos débiles en sus víctimas, como en seguridad, para, por ejemplo, identificar datos robados e informarse de amenazas y proteger sus sistemas.



**Sistemas heredados o legacy**

Tecnologías antiguas que siguen en uso y que las organizaciones no quieren o no pueden reemplazar, lo que generalmente conlleva problemas de compatibilidad con sistemas más recientes, además de exponer los recursos de la organización, ya que los sistemas heredados suelen carecer de actualizaciones de seguridad, dejándolos vulnerables a ser explotados.



**TIC**

Como TIC se agrupa y destaca la interacción de varias tecnologías de la información y la comunicación, como la telefonía, la televisión, la computación y la ciberseguridad, destacando su interacción. Con el avance tecnológico, la definición de las TIC cambia permanentemente, y sus tecnologías se interrelacionan cada vez más.



**Actores estatales**

Actores de amenaza apoyados por un gobierno o pertenecientes a ellos, lo que les entrega mayores recursos para realizar campañas maliciosas más dañinas que el común de las bandas de ciberdelincuentes. Sus objetivos suelen ser principalmente políticos, con operaciones de sabotaje e inteligencia, en lugar de financieros.



## CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>  
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl  
@csirtgob  
<https://www.linkedin.com/company/csirt-gob>

## 4. 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.

### CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

## 5. 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.

- Didye Paolo Orellana Ponce
- Julian Leou
- Javier Ignacio Candia Tapia
- Miguel Morales Saravia

### CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>  
 Teléfonos: 1510 | + (562) 24863850 | Correo: [soc-csirt@interior.gob.cl](mailto:soc-csirt@interior.gob.cl)  
 [@csirtgob](https://twitter.com/csirtgob)  
 <https://www.linkedin.com/company/csirt-gob>