



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 213

semana del 28 de julio al 3 de agosto de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

6

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

11

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

20

Las mitigaciones son útiles en productos de Mozilla, Atlassian, Ubuntu y Zimbra.



CONTENIDO

1.	Sitios fraudulentos	3
2.	Phishing	5
3.	Vulnerabilidades	7
4.	Concientización	9
5.	Recomendaciones y buenas prácticas	13
6.	Muro de la Fama	14

1. Sitios fraudulentos



CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile

Alerta de seguridad cibernética	8FFR23-01479-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 agosto, 2023
Última revisión	1 agosto, 2023

Indicadores de compromiso

URL redirección

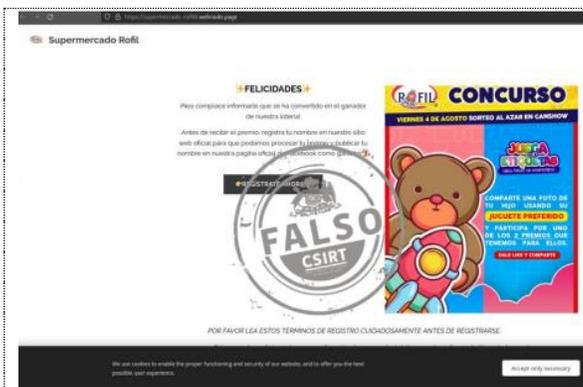
[https://is\[.\]gd/CYkDn3](https://is[.]gd/CYkDn3)

URL sitio falso

[https://cl.correosaddress\[.\]top/](https://cl.correosaddress[.]top/)

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01479-01/>



CSIRT alerta de sitio fraudulento que suplanta al Supermercado Rofil

Alerta de seguridad cibernética	8FFR23-01480-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 agosto, 2023
Última revisión	3 agosto, 2023

Indicadores de compromiso

URL sitio falso

[https://supermercado-rofil.webnode\[.\]page/](https://supermercado-rofil.webnode[.]page/)

[https://supermercado-rofil6.webnode\[.\]page/](https://supermercado-rofil6.webnode[.]page/)

Dirección IP

[217.16.182.250]

[85.132.152.223]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01480-01/>

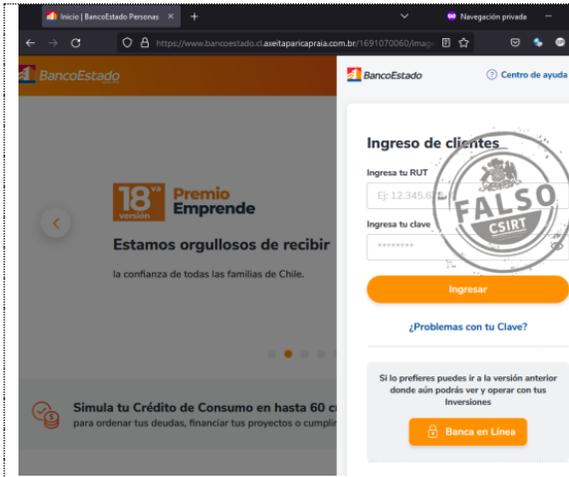
CONTACTO Y REDES SOCIALES CSIRT

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

Boletín de Seguridad Cibernética N° 213

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

BOLETÍN 13BCS23-00222-01 | Semana del 28 de julio al 3 de agosto de 2023



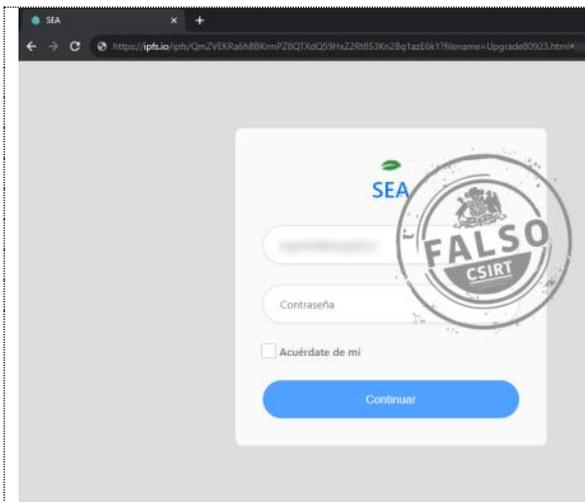
CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado

Alerta de seguridad cibernética	8FFR23-01481-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 agosto, 2023
Última revisión	3 agosto, 2023
Indicadores de compromiso	
URL sitio falso	https://www.bancoestado.cl.axeitaparicpraia[.]com.br/1691070060/imagenes/_personas/home/default.asp
Dirección IP	[192.185.131.48]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01481-01/

CONTACTO Y REDES SOCIALES CSIRT

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

2. Phishing



CSIRT alerta de nueva campaña de phishing que suplanta un inicio de sesión de correo electrónico

Alerta de seguridad cibernética	8FPH23-00864-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 julio, 2023
Última revisión	28 julio, 2023

URL redirección

https://ipfs.io/ipfs/QmZVEKR6hBBKrmPZ8QTXdQ59HxZ2Rt853Kn2Bq1azE6k1?filename=Upgrade80923.html#test@csirt.gob.cl&c=E,1,EK11F056kt_IPddersxFilDwKxMHbt4os81NGAlDJrc5hfbRRFXAFzEjzLL3StRBgkdvH4VoNwDs8PhzFR2ZBQo1eaj5TAb3pb3ykjHEM,&typo=1&data=05|01|test@csirt.gob.cl|77121cea35cf4f45d9880db8f58edd2|b71dc67ef57148469db81264f14ea88b|1|0|638261384379089655|Unknown|TWFpbGZsb3d8eyJWljoimC4wLjAwMDAilCJQljoiv2luMzliLCJBTil6Ik1haWwlcjXVCl6Mn0=|0||&sdata=FK3QQdHosLaKTfJqJE7eXB58a10CrkFnCiKkhUhdMvQ=&reserved=0

URL sitio falso

<https://ipfs.io/ipfs/QmZVEKR6hBBKrmPZ8QTXdQ59HxZ2Rt853Kn2Bq1azE6k1?filename=Upgrade80923.html#test@csirt.gob.cl>

Dirección IP

[162.240.110.92]

Enlace para revisar IoC:

<https://www.csirt.gob.cl/alertas/8fph23-00864-01/>



CSIRT alerta de nueva campaña de smishing que suplanta a CorreosChile

Alerta de seguridad cibernética	8FPH23-00865-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 agosto, 2023
Última revisión	1 agosto, 2023

Indicadores de compromiso

URL redirección

[https://correoscl1\[.\]icu/?token=GnmnOKuf5PVfJezf](https://correoscl1[.]icu/?token=GnmnOKuf5PVfJezf)

URL sitio falso

[https://cutt\[.\]ly/fwsn4r2G](https://cutt[.]ly/fwsn4r2G)

Dirección IP sitio falso

[43.135.156.208]

Enlace para revisar IoC:

<https://www.csirt.gob.cl/alertas/8fph23-00865-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

Boletín de Seguridad Cibernética N° 213

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

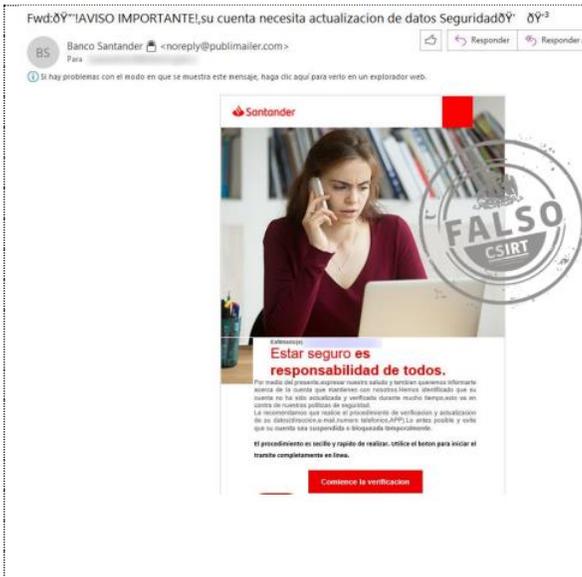


BOLETÍN 13BCS23-00222-01 | Semana del 28 de julio al 3 de agosto de 2023



CSIRT alerta de nueva campaña de phishing, que amenaza falsamente con revelar datos personales del usuario

Alerta de seguridad cibernética	8FPH23-00866-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 agosto, 2023
Última revisión	1 agosto, 2023
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00866-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a Banco Santander

Alerta de seguridad cibernética	8FPH23-00867-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 agosto, 2023
Última revisión	3 agosto, 2023
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3OE47RK?l=www.santander.cl	
https://www.nationaltreasures.co[.]nz/bancosantander/cuenta-daiu/	
URL sitio falso	
https://banco.santander-cl.infenso[.]hr/1691069564/portada/personas/home.asp	
Dirección IP sitio falso	
[185.58.73.179]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00867-01/	

CONTACTO Y REDES SOCIALES CSIRT

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

3. Vulnerabilidades



INFORME DE Vulnerabilidad

9VSA23-00873-01
 CSIRT informa de vulnerabilidad de día cero parchada en Zimbra Collaboration Suite

PARA REGISTRAR | 15 10
 UN INCIDENTE | www.csirt.gob.cl

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

CSIRT comparte información de vulnerabilidad día cero parchada en Zimbra Collaboration Suite (ZCS)

Alerta de seguridad cibernética	9VSA23-00873-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 julio, 2023
Última revisión	28 julio, 2023

CVE

CVE-2023-38750

Fabricante

Oracle

Productos afectados

Zimbra Collaboration Suite (ZCS) anteriores a ZCS 10.0.2.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00873-01/>



INFORME DE Vulnerabilidad

9VSA23-00874-01
 CSIRT informa de vulnerabilidades de alto riesgo parchadas en productos Atlassian

PARA REGISTRAR | 15 10
 UN INCIDENTE | www.csirt.gob.cl

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

CSIRT comparte nuevas vulnerabilidades parchadas por Atlassian

Alerta de seguridad cibernética	9VSA23-00874-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 julio, 2023
Última revisión	28 julio, 2023

CVE

CVE-2023-22505

CVE-2023-22506

CVE-2023-22508

Fabricante

Atlassian

Productos afectados

Confluence Data Center and Server

Bamboo

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00874-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

Boletín de Seguridad Cibernética N° 213

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



BOLETÍN 13BCS23-00222-01 | Semana del 28 de julio al 3 de agosto de 2023

Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00875-01
CSIRT informa de vulnerabilidades de alto riesgo parchadas en Ubuntu

PARA REGISTRAR | 15 10
UN INCIDENTE | www.csirt.gob.cl

CSIRT comparte información de dos vulnerabilidades parchadas por Ubuntu

Alerta de seguridad cibernética	9VSA23-00875-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 agosto, 2023
Última revisión	1 agosto, 2023

CVE

CVE-2023-2640
CVE-2023-32629

Fabricante

Ubuntu

Productos afectados

Ubuntu

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00875-01/>

Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00876-01
CSIRT informa de vulnerabilidades de alto riesgo parchadas en Firefox 116

PARA REGISTRAR | 15 10
UN INCIDENTE | www.csirt.gob.cl

CSIRT comparte vulnerabilidades parchadas en Google Chrome 115

Alerta de seguridad cibernética	9VSA23-00876-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 agosto, 2023
Última revisión	2 agosto, 2023

CVE

CVE-2023-4045	CVE-2023-4050	CVE-2023-4055
CVE-2023-4046	CVE-2023-4051	CVE-2023-4056
CVE-2023-4047	CVE-2023-4052	CVE-2023-4057
CVE-2023-4048	CVE-2023-4053	CVE-2023-4058
CVE-2023-4049	CVE-2023-4054	

Fabricante

Mozilla

Productos afectados

Firefox, Firefox ESR.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00876-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

4. Concientización

CSIRT participa de Seminario de Ciberseguridad del Ministerio de Salud

La mañana de este martes, el CSIRT de Gobierno participó del Seminario de Ciberseguridad en Salud, organizado por el Ministerio de Salud y que tuvo lugar en el Auditorio del Edificio Moneda Bicentenario, Teatinos 92.

La presentación del CSIRT fue realizada por su actual jefe, Cristián Bravo Lillo, quien explicó los principales elementos de la propuesta de nueva Política Nacional de Ciberseguridad, y del proyecto de Ley Marco de Ciberseguridad, concentrándose en la institucionalidad de ciberseguridad que espera pueda ser implementada al aprobarse ambos textos. Más información de la jornada: csirt.gob.cl/noticias/csirt-seminario-minsal/.



CONTACTO Y REDES SOCIALES CSIRT

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

Ciberconsejos | Precauciones ante el uso de dominios .zip

Recientemente empezaron a ser registrados muchos dominios web que terminan en .zip, los que pueden ser usados por ciberdelincuentes para hacer parecer a sus víctimas que un enlaces malicioso es en realidad un archivo comprimido, facilitando la infección de sus equipos con malware.

Por eso es que en estos nuevos Ciberconsejos hacemos un llamado a ser extra cuidadosos al recibir un correo electrónico o mensaje de cualquier aplicación con lo que parece un descargable .zip, siguiendo estas recomendaciones. Pueden encontrarlo también aquí (incluyendo su versión en PDF): csirt.gob.cl/recomendaciones/ciberconsejos-precauciones-dominios-zip/

 <h3>CIBERCONSEJOS CUÍDATE DE LOS DOMINIOS .ZIP</h3> 	 <h3>¿Qué son los dominios .zip?</h3> <p>En mayo de este año comenzó el registro de numerosos nuevos dominios web ".zip".</p> <p>La terminación .zip es conocida popularmente por corresponder a un tipo de compresión de archivos, disminuyendo su tamaño.</p> <p>Pero también puede referirse a un tipo de dominio web, como son .cl o .com</p> 
 <h3>El problema</h3> <p>Los ciberdelincuentes están aprovechando de utilizar el dominio .zip en campañas de phishing, con tal de instalar malware en el dispositivo del usuario.</p> <p>Así, buscan engañar a los usuarios que creen que descargan un archivo comprimido en .zip, cuando realmente hacen clic en un sitio web malicioso.</p>  <p>Lo mismo ocurre con otros dominios como .mov, que permite enviar a una persona a un link malicioso haciéndolo pasar por un video.</p>	 <h3>Recomendaciones</h3> <ul style="list-style-type: none">◆ Ten extrema precaución si te mandan lo que parece ser un archivo comprimido en .zip o un video .mov. Puede ser un archivo malicioso, o ser un enlace a contenido peligroso.◆ No hagas nunca clic en links sospechosos.◆ Mantén actualizado el software de tu dispositivo, y sólo consíguelo en sitios oficiales.◆ En empresas y otras organizaciones, es importante reforzar la concientización para protegernos del phishing.

CONTACTO Y REDES SOCIALES CSIRT

Ciberconsejos para una navegación segura con tus hijos

Esta semana publicamos ciberconsejos extra con motivo del Día del Niño. Se los puede revisar completos (son 6 láminas e incluyendo una versión en PDF) en nuestro sitio web dedicado a la campaña: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-navegacion-segura-con-tus-hijos-2/>.



The infographic consists of six panels arranged in a 2x3 grid, each with the CSIRT logo and the title 'CIBERCONSEJOS PARA UNA NAVEGACIÓN SEGURA CON TUS HIJOS'. The panels are:

- Top Left:** 'Niños y RRSS: ¿Para qué las usan?' (Children and RRSS: Why do they use them?). It lists: 'Chatean con sus amigos y buscan ser reconocidos socialmente.' (They chat with their friends and seek social recognition), 'Refuerzan sus lazos con los grupos que tienen en común.' (They strengthen their ties with groups they have in common), 'Juegan en línea y ven videos.' (They play online and watch videos), 'Publican fotos o estados para compartir su día.' (They post photos or statuses to share their day), and 'Siguen a personas relevantes (influencer).' (They follow relevant people (influencers)).
- Top Right:** '¿Cuáles son los riesgos en internet para nuestros hijos?' (What are the risks on the internet for our children?). It lists: 1. GROOMING: Acoso y abuso sexual online. 2. CIBERACOSO: Abuso sostenido entre escolares a través de las redes sociales. 3. SUPLANTACIÓN DE IDENTIDAD: Una persona se hace pasar por el menor en redes sociales. 4. COMUNIDADES PELIGROSAS Y CONTENIDO INAPROPIADO: En ocasiones, se comparte contenido violento, sentimientos de odio o potencian la autolesión y/o suicidio. 5. PÉRDIDA DE PRIVACIDAD: Al publicar mucha información, alguien la puede utilizar en contra de ellos mismos u otras personas. A note at the bottom says: 'Los juegos en línea son la plataforma más utilizada para cometer "grooming".' (Online games are the most used platform to commit "grooming").
- Middle Left:** '¿Cómo usar las redes sociales con responsabilidad?' (How to use social media responsibly?). It says: 'Antes de que tus hijos se registren en una red social, asegúrate que sea acorde a su edad y madurez.' (Before your children register on a social network, make sure it is appropriate to their age and maturity). It lists 'CONFIGURACIÓN SEGURA:' (SAFE CONFIGURATION): 1. Perfil privado. 2. Sólo los contactos deben ver las publicaciones. 3. Configura su perfil para recibir mensajes y comentarios sólo de sus contactos. A note at the bottom says: 'Cuida la IDENTIDAD DIGITAL. Todo lo que se comparten debe respetar la imagen de los menores.' (Protect digital IDENTITY. Everything shared must respect the image of minors).
- Middle Right:** 'Niños y RRSS: ¿Por qué les gusta conectarse?' (Children and RRSS: Why do they like to connect?). It lists: 1. LES SIRVE como un lugar de encuentro. 2. COMPARTEN fotos y videos de forma rápida y fácil. 3. PUEDEN hacer sus post más entretenidos con filtros, efectos, stickers u otros. 4. REAFIRMAN que son aceptados, a través de la cantidad de seguidores y likes en sus publicaciones. 5. PUEDEN etiquetar a personas y temáticas en sus post, gracias a los # (hashtags). A note at the bottom says: 'Sabías que... El 40% de los niños entre 8 y 14 años están conectados más de 3 horas al día.' (Did you know... 40% of children between 8 and 14 years are connected for more than 3 hours a day).

CONTACTO Y REDES SOCIALES CSIRT

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

Ciberdiccionario Volumen 42

Una nueva edición del ciberdiccionario del CSIRT, en esta ocasión con las definiciones para domótica, M2M, ciberresiliencia y machine learning. También los pueden encontrar acá, incluyendo una versión en PDF: <https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-42/>.

 <h3>Ciberdiccionario</h3> <h4>M2M</h4> <p>Se refiere a la comunicación directa y automática entre dispositivos, sistemas o máquinas sin la intervención humana (por eso el nombre, "machine to machine"). Al interactuar de esta forma, los dispositivos inteligentes pueden compartir datos y ejecutar acciones de manera autónoma.</p> <p>La comunicación M2M es parte fundamental del Internet de las Cosas (IoT)</p> 	 <h3>Ciberdiccionario</h3> <h4>Domótica</h4> <p>Automatización y control de sistemas y dispositivos electrónicos en el hogar, como la seguridad, la limpieza y el uso de la energía, por medio de redes de comunicación, generalmente a través de Internet. Comprende tecnologías que vienen creciendo de la mano del llamado "internet de las cosas" (IoT). Su control se realiza utilizando aplicaciones móviles o por medios web.</p> 
 <h3>Ciberdiccionario</h3> <h4>Ciberresiliencia</h4> <p>Capacidad de una organización para resistir y recuperarse de ataques, permitiendo así mantener la operatividad y la continuidad del negocio al sufrir un incidente de ciberseguridad. Para contar con ciberresiliencia es necesario haber diseñado y comunicado una estrategia que defina activos esenciales de información, roles y procesos de recuperación, contando con las capacidades necesarias para retomar rápidamente la continuidad operativa.</p> 	 <h3>Ciberdiccionario</h3> <h4>Machine learning</h4> <p>En castellano aprendizaje de máquinas, es un subconjunto de la inteligencia artificial, que combina el uso de distintas tecnologías (como deep learning, redes neuronales y procesamiento de lenguaje) para que los computadores puedan aprender a partir de grandes cantidades de datos, desarrollando algoritmos que no han sido programados explícitamente por humanos.</p> 

CONTACTO Y REDES SOCIALES CSIRT

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

5. 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 CSIRT

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

6. 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.

- Francisco Contreras
- Héctor Jesús Concha Vera
- César Labbé
- Sugy Nam
- Jair Palma
- Natalia Ninoska Riva Barraza
- Pablo Ignacio Pizarro Cortínez

CONTACTO Y REDES SOCIALES CSIRT

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