



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 196

semana del 31 de marzo al 6 de abril de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

6

IP advertidas en múltiples campañas de phishing y de malware.



URL ADVERTIDAS

7

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

52

Las mitigaciones son útiles en productos de Cisco, IBM y Apple.



CONTENIDO

1.	Sitios fraudulentos	3
2.	Phishing	5
3.	Vulnerabilidades	6
4.	Concientización	10
5.	Recomendaciones y buenas prácticas	12
6.	Muro de la Fama	13



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

1. Sitios fraudulentos

CSIRT alerta de sitio fraudulento que suplanta a Merrell

Alerta de seguridad cibernética	8FFR23-01271-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2023
Última revisión	5 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.moveoutlets[.]shop/	
Dirección IP	
[167.160.0.229]	
Enlace para revisar loC:	
https://www.csirt.gob.cl/alertas/8ffr23-01271-01	

CSIRT alerta de sitio fraudulento que suplanta a H&M

Alerta de seguridad cibernética	8FFR23-01272-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2023
Última revisión	5 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.hcmropa[.]online/	
Dirección IP	
[162.218.176.46]	
Enlace para revisar loC:	
https://www.csirt.gob.cl/alertas/8ffr23-01272-01	

CSIRT alerta página web que suplanta a Converse

Alerta de seguridad cibernética	8FFR23-01273-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2023
Última revisión	5 de abril de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.converse-chile[.]com/	
Dirección IP	
[172.67.213.29]	
Enlace para revisar loC:	
https://www.csirt.gob.cl/alertas/8ffr23-01273-01	

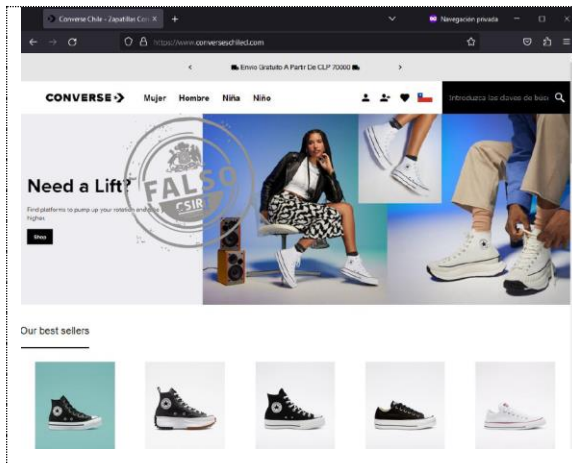
CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

Boletín de Seguridad Cibernética N° 196

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

BOLETÍN 13BCS23-00205-01 | Semana del 31 de marzo al 6 de abril de 2023



CSIRT alerta página web que suplanta a Converse

Alerta de seguridad cibernética	8FFR23-01274-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de abril de 2023
Última revisión	6 de abril de 2023

Indicadores de compromiso

URL sitio falso

[https\[:\]//www.converseschilecl\[.\]com/](https[:]//www.converseschilecl[.]com/)

Dirección IP

[196.247.29.14]

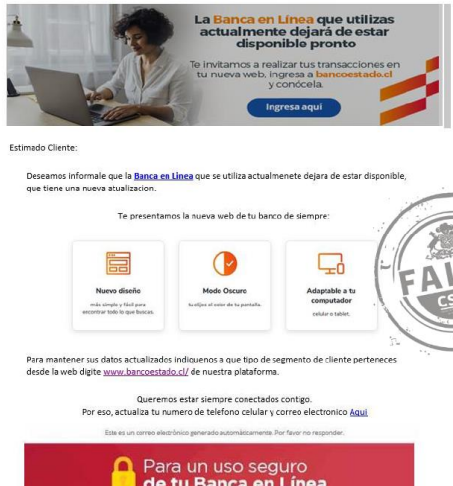
Enlace para revisar IoC:

<https://www.csirt.gob.cl/alertas/8ffr23-01274-01>

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

2. Phishing



Estimado Cliente:

Deseamos informarle que la **Banca en Línea** que se utiliza actualmente dejará de estar disponible, que tiene una nueva actualización.

Te presentamos la nueva web de tu banco de siempre:



Nuevo diseño
más simple y fácil para
navegar todo lo que necesitas.



Modo Oscuro
Navega al color de tu preferencia.



**Adaptable a tu
computador**
veloz y seguro.

Para mantener sus datos actualizados indiquenos a que tipo de segmento de cliente perteneces desde la web digite www.bancoestado.cl de nuestra plataforma.

Queremos estar siempre conectados contigo.
Por eso, actualiza tu número de teléfono celular y correo electrónico [aquí](mailto:tuinfo@bce.cl).

Este es un correo electrónico generado automáticamente. Por favor no responder.

 **Para un uso seguro de tu Banca en Línea**

CSIRT alerta de campaña de phishing que suplanta a BancoEstado

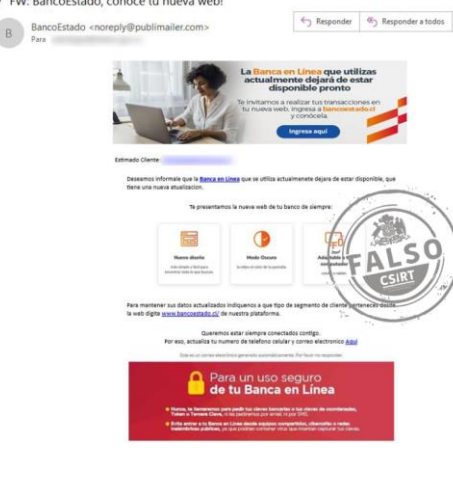
Alerta de seguridad cibernética	8FPH23-00778-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de abril de 2023
Última revisión	3 de abril de 2023

Indicadores de compromiso

URL sitio falso
[https://fogapehomeunder\[.\]info/1680556894/imagenes/_personas/home/default.asp](https://fogapehomeunder[.]info/1680556894/imagenes/_personas/home/default.asp)

Dirección IP
[172.67.146.96]

Enlace para revisar loC:
<https://www.csirt.gob.cl/alertas/8fph23-00778-01/>



✓ FW: BancoEstado, conoce tu nueva web!

BancoEstado <noreply@publmail.com>
Para [redacted] mi: 05/04/2023 21:16

Estimado Cliente:

Deseamos informarle que la **Banca en Línea** que se utiliza actualmente dejará de estar disponible, que tiene una nueva actualización.

Te presentamos la nueva web de tu banco de siempre:



Nuevo diseño
más simple y fácil para
navegar todo lo que necesitas.



Modo Oscuro
Navega al color de tu preferencia.



**Adaptable a tu
computador**
veloz y seguro.

Para mantener sus datos actualizados indiquenos a que tipo de segmento de cliente perteneces desde la web digite www.bancoestado.cl de nuestra plataforma.

Queremos estar siempre conectados contigo.
Por eso, actualiza tu número de teléfono celular y correo electrónico [aquí](mailto:tuinfo@bce.cl).

Este es un correo electrónico generado automáticamente. Por favor no responder.

 **Para un uso seguro de tu Banca en Línea**

CSIRT alerta de campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH23-00779-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de abril de 2023
Última revisión	6 de abril de 2023

Indicadores de compromiso

URL redirección
[https://www.ideaprisma\[.\]it/online/activacion/cuenta-kzho/](https://www.ideaprisma[.]it/online/activacion/cuenta-kzho/)

URL sitio falso
[https://fogapehomeunder\[.\]info/1680789160/imagenes/_personas/home/default.asp](https://fogapehomeunder[.]info/1680789160/imagenes/_personas/home/default.asp)

Dirección IP
[104.21.47.92]

Enlace para revisar loC:
<https://www.csirt.gob.cl/alertas/8fph23-00779-01/>

3. Vulnerabilidades



INFORME DE Vulnerabilidad

9VSA23-00808-01
CSIRT comparte vulnerabilidad actualmente explotada en IBM Aspera Faspex

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT alerta de vulnerabilidad actualmente explotada en IBM Aspera Faspex

Alerta de seguridad cibernética	9VSA23-00808-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	3 de abril de 2023
Última revisión	3 de abril de 2023

CVE

CVE-2022-47986

Fabricantes

IBM

Productos afectados

IBM Aspera Faspex 4.4.2 Patch Level 1 y anteriores.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00808-01/>



INFORME DE Vulnerabilidad

9VSA23-00809-01
CSIRT comparte vulnerabilidades parchadas por Apple en iOS 15.7.4 y iPadOS 15.7.4

PARA REGISTRAR | 1510
UN INCIDENTE | www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte vulnerabilidades parchadas por Apple en iOS15.7.4 y iPadOS 15.7.4

Alerta de seguridad cibernética	9VSA23-00809-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	4 de abril de 2023
Última revisión	4 de abril de 2023

CVE

CVE-2023-27961	CVE-2023-27928	CVE-2023-27949
CVE-2023-23541	CVE-2023-27946	CVE-2023-28182
CVE-2023-23543	CVE-2023-23535	CVE-2023-27963
CVE-2023-27936	CVE-2023-27941	CVE-2023-27954
CVE-2023-23537	CVE-2023-27969	CVE-2023-23529
CVE-2023-27956		

Fabricantes

IBM

Productos afectados

La actualización que mitiga estas vulnerabilidades está disponible para iPhone 6s (todos los modelos), iPhone 7 (todos los modelos), iPhone SE (primera generación), iPad Air 2, iPad mini (cuarta generación), and iPod touch (séptima generación).

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00809-01/>

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<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° 196

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

BOLETÍN 13BCS23-00205-01 | Semana del 31 de marzo al 6 de abril de 2023



CSIRT comparte información de vulnerabilidades parchadas por Cisco

Alerta de seguridad cibernética	9VSA23-00810-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2023
Última revisión	5 de abril de 2023

CVE

CVE-2022-20812	CVE-2022-20967	CVE-2023-20113
CVE-2022-20959	CVE-2023-20029	CVE-2023-20029
CVE-2022-20813	CVE-2023-20016	CVE-2023-20016
CVE-2023-20064	CVE-2023-20027	CVE-2023-20027
CVE-2022-20797	CVE-2023-20065	CVE-2023-20065
CVE-2022-20952	CVE-2023-20035	CVE-2023-20035
CVE-2023-20113	CVE-2023-20072	CVE-2023-20072
CVE-2023-20099	CVE-2023-20080	CVE-2023-20080
CVE-2022-20956	CVE-2023-20067	CVE-2023-20067
CVE-2022-20964	CVE-2023-20055	CVE-2023-20055
CVE-2022-20965	CVE-2023-20082	CVE-2023-20082
CVE-2022-20966	CVE-2023-20011	

Fabricantes

Cisco

Productos afectados

Software Cisco Expressway Series y Cisco TelePresence VCS en configuración por defecto.

Si utilizan software Cisco IOS XR:

ASR 9000 Series Aggregation Services Routers (64-bit) (CSCwd35552)
IOS XR White box (IOSXRWBD) (CSCwd35552)
IOS XRV 9000 Routers (CSCwd35552)
Network Convergence System (NCS) 540 Series Routers (CSCwd35552)
NCS 560 Series Routers (CSCwd35552)
NCS 1001 Series Routers (CSCwd35552)
NCS 1002 Series Routers (CSCwd35552)
NCS 1004 Series Routers (CSCwd35552)
NCS 4000 Series Routers (CSCwc97333)
NCS 5000 Series Routers (CSCwd35552)
NCS 5500 Series Routers (CSCwd35552)
NCS 5700 Series Routers (CSCwd35552)
NCS 6000 Series Routers (CSCwc97332)

Cisco Secure Network Analytics.
Cisco Secure Web Appliance, virtual y hardware.
Cisco Identity Services Engine (ISE).
Cisco APIC.
Cisco Cloud Network Controller.
Cisco SD-WAN vManage Software.

Si usan el Cisco IOS XE Software:

Catalyst 9200 Series Switches
Catalyst 9300 Series Switches

Si usan Cisco FXOS or Cisco UCS Manager Software:
Firepower 4100 Series

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

Boletín de Seguridad Cibernética N° 196

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



BOLETÍN 13BCS23-00205-01 | Semana del 31 de marzo al 6 de abril de 2023

Firepower 9300 Security Appliances
UCS 6200 Series Fabric Interconnects
UCS 6300 Series Fabric Interconnects
UCS 6400 Series Fabric Interconnects
UCS 6500 Series Fabric Interconnects

Si usan Cisco IOS XE Software con la función VFR activada:

1000 Series Integrated Services Routers
4000 Series Integrated Services Routers
Catalyst 8000V Edge Software Routers
Catalyst 8200 Series Edge Platforms
Catalyst 8300 Series Edge Platforms
Catalyst 8500L Series Edge Platforms
Cloud Services Router 1000V Series

Productos Cisco corriendo Cisco IOS XE Software releases 17.9.1, 17.9.1a, o 17.9.1w con la tunnel interface configurada.

Aparatos Cisco que se encuentren ejecutando versiones vulnerables de software Cisco IOS o IOS XE y tienen IPv6 y la función servidor o relay DHCPv6 activada.

Los siguientes productos de Cisco si corren una versión vulnerable del software Cisco IOS XE para WLC y tienen la función de perfilamiento de cliente basado en HTTP:

Catalyst 9800 Embedded Wireless Controllers for Catalyst 9300, 9400, and 9500 Series Switches
Catalyst 9800 Series Wireless Controllers
Catalyst 9800-CL Wireless Controllers for Cloud
Embedded Wireless Controllers on Catalyst Access Points

Cisco DNA Center en la configuración por defecto.

Switches Cisco Catalyst 9300 Series si corren software Cisco IOS XE con una versión de Cisco IOS XE ROM Monitor (ROMMON) anterior a las 17.3.7r, 17.6.5r o 17.8.1r.

Cisco SD-WAN vManage Software.

Si corren una versión vulnerable de Cisco IOS XE Software:

Catalyst 9200 Series Switches
Catalyst 9300 Series Switches

Si corren una versión vulnerable de Cisco FXOS or Cisco UCS Manager Software:

Firepower 4100 Series
Firepower 9300 Security Appliances
UCS 6200 Series Fabric Interconnects
UCS 6300 Series Fabric Interconnects
UCS 6400 Series Fabric Interconnects
UCS 6500 Series Fabric Interconnects

Si corren una versión vulnerable de Cisco IOS XE Software con la función VFR activada:

1000 Series Integrated Services Routers
4000 Series Integrated Services Routers
Catalyst 8000V Edge Software Routers

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

Boletín de Seguridad Cibernética N° 196

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



BOLETÍN 13BCS23-00205-01 | Semana del 31 de marzo al 6 de abril de 2023

Catalyst 8200 Series Edge Platforms
Catalyst 8300 Series Edge Platforms
Catalyst 8500L Series Edge Platforms
Cloud Services Router 1000V Series

Productos Cisco si corren Cisco IOS XE Software, tienen la función Cisco IOx de hosting configurada y la aplicación está corriendo.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00810-01/>

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

4. Concientización

Ciberconsejos | Operación Renta 2023

Protégete del phishing durante la Operación Renta 2023 teniendo en cuenta los siguientes indicios de contenido malicioso. Si ves cualquiera de estas situaciones en correos electrónicos que recibas, ¡no hagas clic!, no descargues archivos adjuntos o abras enlaces incluidos en los mensajes: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-operacion-renta-2023/>.

#Ciberconsejos Operación Renta 2023

El phishing es un tipo de ataque que se hace pasar por instituciones o personas de confianza para infectar nuestros equipos o robar información

Factura No Pagada. Segundo Aviso.

Servicio de Impuestos Internos de Chile <zap@webmail.zap.co.ao>

Para [Redacted]

Le informamos mediante este medio que hay una factura que se encuentra en estado de NO PAGADA. Le del siguiente enlace.

Por favor realice el pago lo mas pronto posible, a fin de evitar las molestias de un cobro judicial, que pue definitiva depende el caso.

Puede consultar el estado

ENLACE DE DESCARGA MALICIOSO

¡SI VES ESTOS ELEMENTOS, NO HAGAS CLIC NI DESCARGUES ARCHIVOS!

REVISEMOS ALGUNOS DE SUS ELEMENTOS MALICIOSOS

ASUNTO ALARMANTE

EL REMITENTE NO ES EL SII

MENSAJE ALARMANTE

#Ciberconsejos Operación Renta 2023

Otro ejemplo: suplantación a la Tesorería (TGR)

✓ Fw: Información TGR - Protocolo - (594407610129)

16087577 @servicio al TGR <Servicio-TGR@tgr.cl>

19 de octubre de 2022, 15:32

EL REMITENTE NO ES LA TGR

FALSO COMPROBANTE

Comprobante de Pago en Línea

Tesorería General de la República.

Informamos que su pago electrónico realizado con exito! 18/10/2022 - N° de transacción 36556314

ENLACE DE DESCARGA MALICIOSO

SI TIENES DUDAS, INGRESA A SII.CL O TGR.CL Y LLAMA A SUS NÚMEROS DE CONTACTO

#Ciberconsejos Operación Renta 2023

Recuerda

- Ni el SII ni la TGR te enviarán emails con enlaces directos.
- Desconfía de correos o mensajes de texto o WhatsApp con mensajes alarmantes o que te llaman a actuar inmediatamente.
- Si crees que un mensaje alarmante puede ser real, verificalo llamando directamente a la organización o persona involucrada. No hagas clic en enlaces incluidos en el mismo mensaje.



CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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

Ciberconsejos | Operación Renta 2023

Protégete del phishing durante la Operación Renta 2023 teniendo en cuenta los siguientes indicios de contenido malicioso. Si ves cualquiera de estas situaciones en correos electrónicos que recibas, ¡no hagas clic!, no descargues archivos adjuntos o abras enlaces incluidos en los mensajes: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-operacion-renta-2023/>.

 Ciber diccionario Chatbot Los chatbots son programas computacionales diseñados para simular la forma en que conversaría un humano, ya sea por texto o voz. Son principalmente usados en la atención al cliente, aunque se expande el uso de chatbots que aseguran implementar mecanismos de inteligencia artificial, como ChatGPT, para otros usos, como la generación de todo tipo de textos. 	 Ciber diccionario Metadatos Datos contenidos en un archivo, incluyendo fotos y videos, pero ocultos a simple vista. Registran elementos como la ubicación o la hora en que se creó o modificó el archivo y qué usuario lo hizo. Pueden resultar un riesgo para la privacidad de las personas. Versiones recientes de aplicaciones de Office y Acrobat, ofrecen la opción de eliminar algunos metadatos de sus archivos. 
 Ciber diccionario NFC / tecnología contactless Se conoce como NFC, sigla en inglés de "comunicación de campo cercano", es la tecnología que permite el accionar sin contacto (o "contactless") de las tarjetas de crédito y débito actuales, y también otras como la Bip!, además de smart-phones y etiquetas inteligentes ("tags") equipadas con esta tecnología. 	 Ciber diccionario Bloatware Programas de software no deseados y que vienen incluidos de fábrica en un dispositivos. Solo ocupan espacio y, cuando se ejecutan, gastan recursos del aparato, ralentizando los demás programas. Además, pueden contener vulnerabilidades. Su nombre viene de "bloat", o "hinchar", en inglés, ya que solo constituyen un relleno sin utilidad. 

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

 <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 DEL CSIRT DE GOBIERNO

 <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.

- Felipe Cortés
- Carlos Escalona
- María Gabriela
- Martín Cruzat Varela
- Jorge Ignacio Molina Martinez

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

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