



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 243

semana del 23 al 29 de febrero de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

12

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

16

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

1

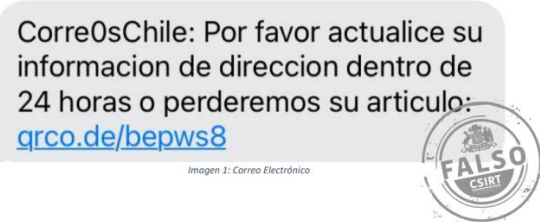
Las mitigaciones son útiles en productos Cisco

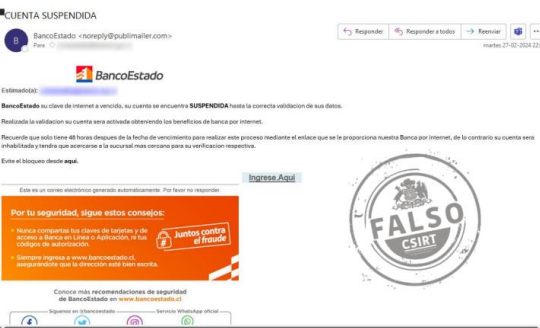


CONTENIDO

| | |
|---|----|
| 1. Phishing | 3 |
| 2. Sitios fraudulentos..... | 4 |
| 3. Vulnerabilidades..... | 8 |
| 4. Malware..... | 9 |
| 5. Noticias y concientización..... | 10 |
| 6. Recomendaciones y buenas prácticas | 12 |
| 7. Muro de la Fama | 13 |

1. Phishing

| Imágenes Relacionadas | CSIRT alerta de campaña de phishing que suplanta a CorreosChile |
|---|--|
|  <p>Corre0sChile: Por favor actualice su informacion de direccion dentro de 24 horas o perderemos su articulo: qrco.de/bepws8</p> <p>Imagen 1: Correo Electrónico</p> | Código de alerta 8FPH24-00933-01 |
| | Clase de alerta Fraude |
| | Tipo de incidente Phishing |
| | Nivel de riesgo Alto |
| | TLP Blanco |
| | Fecha de lanzamiento original 27 febrero, 2024 |
| | Última revisión 27 febrero, 2024 |
| | Indicadores de compromiso |
| | URL del sitio falso https://cl.gouzhang[.]top/slot |
| | URL de redirección qrco.[.]de/bepws8 |
| Dirección IP sitio falso [162.62.53.33] | |
| Enlace para revisar loC: https://csirt.gob.cl/alertas/8fph24-00933-01/ | |

| URL | CSIRT alerta de campaña de phishing que suplanta al BancoEstado |
|---|--|
|  <p>CUENTA SUSPENDIDA</p> <p>BancoEstado</p> <p>Realizada la validación su cuenta será activada obteniendo los beneficios de banco por internet.</p> <p>Recuerde que solo tiene 48 horas después de la fecha de vencimiento para realizar este proceso mediante el enlace que se le proporciona número Banco por internet, de lo contrario su cuenta será inhabilitada y tendrá que acercarse a la sucursal más cercana para su verificación respectiva.</p> <p>Este es el momento de decirle que...</p> <p>Por su seguridad, sigue estos consejos:</p> <p>¡Juntos contra el fraude!</p> | Código de alerta 8FPH24-00935-01 |
| | Clase de alerta Fraude |
| | Tipo de incidente Phishing |
| | Nivel de riesgo Alto |
| | TLP Blanco |
| | Fecha de lanzamiento original 28 febrero, 2024 |
| | Última revisión 28 febrero, 2024 |
| | Indicadores de compromiso |
| | URL del sitio falso https://patito.larissakovalchuk[.]com/1709133127/imagenes/_personas/home/default.asp |
| | URL de redirección https://maximocontaval[.]com/activacion/cuenta-kaoi/ |
| Dirección IP sitio falso [122.201.66.57] | |
| Enlace para revisar loC: https://csirt.gob.cl/alertas/8fph24-00934-01/ | |

CONTACTO Y REDES SOCIALES CSIRT

Imágenes relacionadas



CSIRT alerta de campaña de phishing que suplanta al BancoEstado

| | |
|-------------------------------|------------------|
| Código de alerta | 8FPH24-00935-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 febrero, 2024 |
| Última revisión | 29 febrero, 2024 |

Indicadores de compromiso

URL del sitio falso
[https://wwwstcursomasxfors\[.\]com/1709230736/imagenes/_personas/home/default.asp](https://wwwstcursomasxfors[.]com/1709230736/imagenes/_personas/home/default.asp)

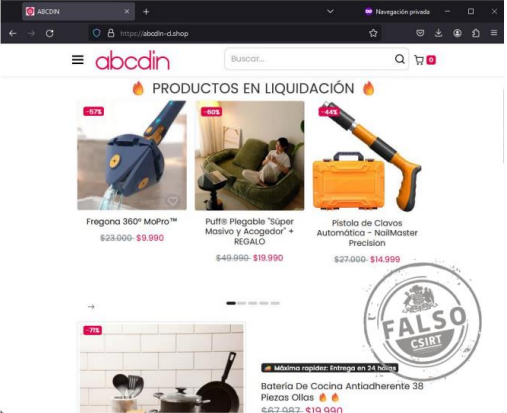
URL redirección
[https://unloackrtmconders\[.\]com/activacion/cuenta-nioj/](https://unloackrtmconders[.]com/activacion/cuenta-nioj/)
[https://bestad0\[.\]cf/personas_bancoestado/](https://bestad0[.]cf/personas_bancoestado/)

Dirección IP sitio falso
 [198.27.78.113]

Enlace para revisar IoC:
<https://csirt.gob.cl/alertas/8fph24-00935-01/>

2. Sitios fraudulentos

Imágenes relacionadas



CSIRT advierte nuevo sitio falso que suplanta a ABCDIN

| | |
|-------------------------------|------------------|
| Código de alerta | 8FFR23-01646-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Fraude |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 26 febrero, 2024 |
| Última revisión | 26 febrero, 2024 |





Indicadores de compromiso

URL del sitio falso
[https://abcdin-cl\[.\]shop/](https://abcdin-cl[.]shop/)

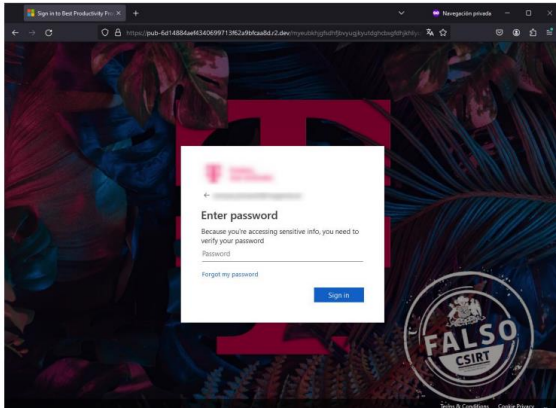
Dirección IP sitio falso
 [23.227.38.73]

Enlace para revisar IoC:
<https://csirt.gob.cl/alertas/8ffr23-01646-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

Imágenes Relacionadas



CSIRT advierte nuevo sitio falso que suplanta a Microsoft

| | |
|-------------------------------|------------------|
| Código de alerta | 8FFR23-01647-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Fraude |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 27 febrero, 2024 |
| Última revisión | 27 febrero, 2024 |

Indicadores de compromiso

URL del sitio falso
[https://2cllc\[.\]cl/hash/mrcashontoday/nkgznkgznkgznkgznkgz/{mail_base64}](https://2cllc[.]cl/hash/mrcashontoday/nkgznkgznkgznkgznkgz/{mail_base64})

URL de redirección
[https://pub-6d14884aef4340699713f62a9bfcaa8d\[.\]r2.dev/myeubkhjgfsdhfjbvyugjkyutdghcbxgfdhjkhllyufgxcfdhgfhjk.html#](https://pub-6d14884aef4340699713f62a9bfcaa8d[.]r2.dev/myeubkhjgfsdhfjbvyugjkyutdghcbxgfdhjkhllyufgxcfdhgfhjk.html#)

Dirección IP sitio falso
 [104.18.3.35]

Enlace para revisar loC:
<https://csirt.gob.cl/alertas/8ffr24-01647-01/>

Imágenes Relacionadas



CSIRT advierte nuevo sitio falso que suplanta a Blue Express

| | |
|-------------------------------|------------------|
| Código de alerta | 8FFR23-01648-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Fraude |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 27 febrero, 2024 |
| Última revisión | 27 febrero, 2024 |

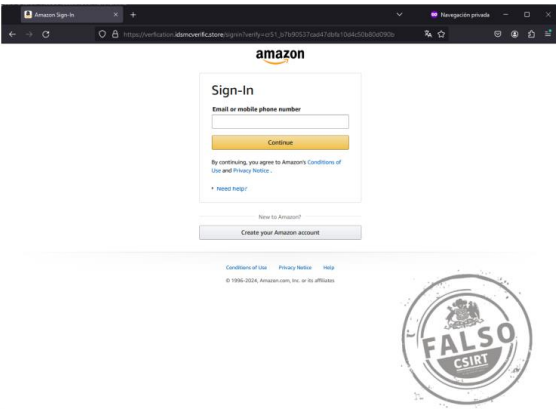
Indicadores de compromiso

URL del sitio falso
[https://bluexpres.inparx\[.\]top/slot](https://bluexpres.inparx[.]top/slot)

Dirección IP sitio falso
 [162.62.53.33]

Enlace para revisar loC:
<https://csirt.gob.cl/alertas/8ffr24-01648-01/>

Imágenes relacionadas



CSIRT advierte nuevo sitio falso que suplanta a Amazon

| | |
|-------------------------------|------------------|
| Código de alerta | 8FFR23-01649-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Fraude |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 febrero, 2024 |
| Última revisión | 28 febrero, 2024 |

Indicadores de compromiso

URL del sitio falso
[https://verification.idsmcverific\[.\]store/signin?verify=cr51_b7b90537cad47dbfa10d4c50b80d090b](https://verification.idsmcverific[.]store/signin?verify=cr51_b7b90537cad47dbfa10d4c50b80d090b)

Dirección IP sitio falso
 162.240.170.105

Enlace para revisar loC:
<https://csirt.gob.cl/alertas/8ffr24-01649-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

| | | |
|---|--|-------------------------|
| <p>Imágenes relacionadas</p>  | <p>CSIRT advierte nuevo sitio falso que suplanta al Banco de Chile</p> | |
| | <p>Código de alerta</p> | <p>8FFR23-01650-01</p> |
| | <p>Clase de alerta</p> | <p>Fraude</p> |
| | <p>Tipo de incidente</p> | <p>Fraude</p> |
| | <p>Nivel de riesgo</p> | <p>Alto</p> |
| | <p>TLP</p> | <p>Blanco</p> |
| | <p>Fecha de lanzamiento original</p> | <p>28 febrero, 2024</p> |
| | <p>Última revisión</p> | <p>28 febrero, 2024</p> |
| | <p>Indicadores de compromiso</p> | |
| | <p>URL del sitio falso</p> | |
| | <p>https://portal-mlbanncochile.skillio[.]online/1709123716/bchile-web/persona/login/index.html/login</p> | |
| | <p>Dirección IP sitio falso</p> | |
| | <p>[162.241.85.202]</p> | |
| | <p>Enlace para revisar IoC:</p> | |
| | <p>https://csirt.gob.cl/alertas/8ffr24-01650-01/</p> | |

| | | |
|--|--|-------------------------|
| <p>Imágenes relacionadas</p>  | <p>CSIRT advierte nuevo sitio falso que suplanta al Banco de Chile</p> | |
| | <p>Código de alerta</p> | <p>8FFR23-01651-01</p> |
| | <p>Clase de alerta</p> | <p>Fraude</p> |
| | <p>Tipo de incidente</p> | <p>Fraude</p> |
| | <p>Nivel de riesgo</p> | <p>Alto</p> |
| | <p>TLP</p> | <p>Blanco</p> |
| | <p>Fecha de lanzamiento original</p> | <p>28 febrero, 2024</p> |
| | <p>Última revisión</p> | <p>28 febrero, 2024</p> |
| | <p>Indicadores de compromiso</p> | |
| | <p>URL del sitio falso</p> | |
| | <p>https://wwwsoporte-mlbancochile-cl.downtownarena[.]in/1709124826/bchile-web/persona/login/index.html/login</p> | |
| | <p>Dirección IP sitio falso</p> | |
| | <p>[216.137.176.69]</p> | |
| | <p>Enlace para revisar IoC:</p> | |
| | <p>https://csirt.gob.cl/alertas/8ffr24-01651-01/</p> | |

| | | |
|---|--|-------------------------|
| <p>Imágenes Relacionadas</p>  | <p>CSIRT advierte nuevo sitio falso que suplanta a Microsoft Outlook</p> | |
| | <p>Código de alerta</p> | <p>8FFR23-01652-01</p> |
| | <p>Clase de alerta</p> | <p>Fraude</p> |
| | <p>Tipo de incidente</p> | <p>Fraude</p> |
| | <p>Nivel de riesgo</p> | <p>Alto</p> |
| | <p>TLP</p> | <p>Blanco</p> |
| | <p>Fecha de lanzamiento original</p> | <p>29 febrero, 2024</p> |
| | <p>Última revisión</p> | <p>29 febrero, 2024</p> |
| | <p>Indicadores de compromiso</p> | |
| | <p>URL del sitio falso</p> | |
| | <p>https://gestampcom[.]weebly.com/</p> | |
| | <p>Dirección IP sitio falso</p> | |
| | <p>[199.34.228.53]</p> | |
| | <p>Enlace para revisar IoC:</p> | |
| | <p>https://csirt.gob.cl/alertas/8ffr24-01652-01/</p> | |

CONTACTO Y REDES SOCIALES CSIRT

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

Imágenes Relacionadas



CSIRT advierte nuevo sitio falso que suplanta a Termas Los Pozones

| | |
|-------------------------------|------------------|
| Código de alerta | 8FFR23-01653-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Fraude |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 febrero, 2024 |
| Última revisión | 29 febrero, 2024 |

Indicadores de compromiso

URL del sitio falso

[https://termaslospozones\[.\]com/](https://termaslospozones[.]com/)

Dirección IP sitio falso

[162.241.61.159]

Enlace para revisar loC:

<https://csirt.gob.cl/alertas/8ffr24-01653-01/>

Imágenes Relacionadas



CSIRT advierte nuevo sitio falso que suplanta a la Universidad de Chile

| | |
|-------------------------------|------------------|
| Código de alerta | 8FFR23-01654-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Fraude |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 febrero, 2024 |
| Última revisión | 29 febrero, 2024 |

Indicadores de compromiso

URL del sitio falso

[https://uchilecl.weebly\[.\]com/](https://uchilecl.weebly[.]com/)

Dirección IP sitio falso

[199.34.228.53]

Enlace para revisar loC:

<https://csirt.gob.cl/alertas/8ffr24-01654-01/>

3. Vulnerabilidades



CSIRT comparte información de vulnerabilidades en Cisco NX-OS

| | |
|-------------------------------|------------------------------|
| Código de alerta | 9VSA24-00980-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 29 febrero, 2024 |
| Última revisión | 29 febrero, 2024 |

CVE

CVE-2024-20321

Fabricante

Cisco

Productos afectados





Conmutadores Cisco Nexus serie 3600 y a las tarjetas de línea Cisco Nexus 9500 serie R si ejecutan una versión vulnerable del software Cisco NX-OS y tienen funcionalidad BGP con al menos un vecino BGP (par) configurado con un Valor del sistema autónomo (AS) y tienen uno de los siguientes ID de producto de Cisco:

N3K-C36180YC-R
N3K-C3636C-R
N9K-X9624D-R2
N9K-X9636C-R
N9K-X9636C-RX
N9K-X9636Q-R
N9K-X96136YC-R


Enlaces para revisar el informe:

<https://csirt.gob.cl/vulnerabilidades/9vsa24-00980-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

4. Malware

| Imagen del Mensaje | CSIRT advierte phishing con malware en falsa factura | |
|--|--|------------------|
|  | Código de alerta | 2CMV24-00447-01 |
| | Clase de alerta | Fraude |
| | Tipo de incidente | Malware |
| | Nivel de riesgo | Alto |
| | TLP | Blanco |
| | Fecha de lanzamiento original | 28 febrero, 2024 |
| | Última revisión | 28 febrero, 2024 |
| | Indicadores de compromiso | |
| | SHA256 | |
| | c1e0f5185a2efc13b4e821ee1a2d445634e87fb380306315c482c05ae26fbd5517a6f57be6897d2a7456ad9b0f5bc798b951c6c41b2511886706edee16c5c14c8ecc1fea5ca3169d8c6269ae0f1a13e3b1e7e9c415c6df4a77af08bd4a2dba11913bbaede66f7c2f00b92916d5cad558067b589bca0b782409e96cb6bf48106e | |

CONTACTO Y REDES SOCIALES CSIRT

5. Noticias y concientización

CSIRT tuvo destacada participación en el Digital Security Challenge

La competencia de tipo Capture The Flag se llevó a cabo en Filipinas entre el 19 y 23 de febrero. El CSIRT de Gobierno representó a Chile, obteniendo el primer lugar en la competencia.

Más de 50 desafíos tuvieron que enfrentar los participantes de diferentes países en la 6ta edición del Digital Security Challenge, Filipinas, evento organizado por la Interpol y financiada por el proyecto GLACY+ del Concilio de Europa.





Durante cinco días, los representantes y especialistas de ciberseguridad y policías de Latinoamérica, África, Asia y Europa, debieron resolver problemas del tipo Capture The Flag (CTF), entre ellos criptografía, ingeniería reversa, escalamientos de privilegios, OSINT, esteganografía, redes, bases de datos y aplicaciones web.

Fueron 50 participantes, divididos en 7 grupos, según la especialidad. El equipo con el que Chile participó estuvo cointegrado por Costa Rica, Letonia, Isla Mauricio, Filipinas y Maldivas, siendo el único en finalizar el desafío principal.

Eduardo Riveros, arquitecto de seguridad del CSIRT, quien participó en la competencia aseguró: “El objetivo principal del evento era compartir entre especialistas de distintos países. Fue una experiencia muy provechosa para aprender y establecer contactos entre especialistas de ciberseguridad de gobiernos y policías de las regiones participantes”. Además, agregó: “Es una instancia muy importante para que Chile pueda mostrar al mundo que contamos con profesionales con altas capacidades y dispuestos a colaborar para hacer frente a las amenazas cibernéticas que afectan a todos los países, como así también para actualizar y perfeccionar nuestros conocimientos”.



CONTACTO Y REDES SOCIALES CSIRT

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

¿Qué hacer frente a un incidente de ciberseguridad

Para prepararte con anticipación, el CSIRT de Gobierno entrega las siguientes recomendaciones:

- **Determina qué ocurre.** ¿Tienes un sitio web o un sistema interno caído? ¿Tus usuarios no tienen acceso a algún sistema importante? ¿Salió publicada información de tu servicio en la prensa? Recopila la mayor cantidad de datos posibles y que sean relevantes para presentarlos de forma ordenada a tu jefatura o (si existe) al comité de emergencia.
- **Responde a la emergencia.** Una vez identificado el problema, actúa rápido y toma las medidas necesarias para resolver el problema. Así, en el caso de un sitio web afectado por un defacement, o una aplicación expuesta a Internet caída, redirígela a una página estática que diga, por ejemplo, “en mantención”. Si existen máquinas en tu red interna que estén infectadas y atacando a otras, desconéctalas físicamente de la red y retira los aparatos para que los usuarios no los sigan usando.
- **Avisa a la jefatura y a los usuarios o clientes oportunamente.** Prepara un par de párrafos que expliquen brevemente qué ocurrió, que se está haciendo para solucionar el problema y qué se hará dentro de los próximos minutos u horas. Recuerda que además debes notificar al CSIRT de Gobierno, según lo establecido en el decreto 273.
- **información.** Si la emergencia está controlada, continúa reuniendo información para realizar una investigación forense. Esto incluye: copias de los filesystems afectados, logs de las aplicaciones, listas de procesos en las máquinas infectadas, etc. Crea copias de la información afectada, calcula hashes de la información y guarda todo en un medio de almacenamiento permanente.
- **Resuelve el problema.** Por ejemplo, si hay actualizaciones de seguridad no aplicadas, instálalas inmediatamente en las máquinas comprometidas; si hay servidores infectados, reinstala el SO y las aplicaciones necesarias; ¿hay usuarios desconocidos o permisos en exceso otorgados a usuarios existentes?, arregla los permisos según las políticas oficiales.
- **Recupera la operación de los sistemas afectados.** Levanta una máquina limpia desde el último backup disponible y asegúrate que esté limpio. Una vez que el sistema esté disponible de nuevo, recupera la información faltante por el período en que el sistema estuvo caído o atacado. Cuando tengas una copia “limpia” y actualizada del sistema, redirige (e.g., DNS) el sitio público a la copia limpia.
- **Avisa nuevamente.** Infórmale a la jefatura y los usuarios que la operación volvió a la normalidad. Construye un relato breve sobre qué ocurrió y las medidas que se tomaron para solucionar el problema (post-mortem del incidente).
- **Respira hondo** y distribuye el post-mortem a la jefatura y los usuarios que corresponda. Vuelve a contactar al CSIRT para enviar una actualización de lo que ocurrió.

Ver más: <https://csirt.gob.cl/noticias/incidente-ciberseguridad/>

CONTACTO Y REDES SOCIALES CSIRT

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.

CONTACTO Y REDES SOCIALES CSIRT

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.

- Manuel Zamorano
- Miguel Morales
- Miguel Burgos
- Luis Miranda

CONTACTO Y REDES SOCIALES CSIRT