



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 236

semana del 5 al 11 de enero de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

4

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

8

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

45

Las mitigaciones son útiles en productos de Microsoft, Cisco e Ivanti.



HASH REPORTADOS

3

Hashes asociados a múltiples campañas de phishing con archivos que contienen malware




CONTENIDO

1. Malware.....	3
2. Sitios fraudulentos.....	4
3. Phishing	5
4. Vulnerabilidades.....	7
5. Noticias y concientización.....	10
6. Recomendaciones y buenas prácticas	11
7. Muro de la Fama	12

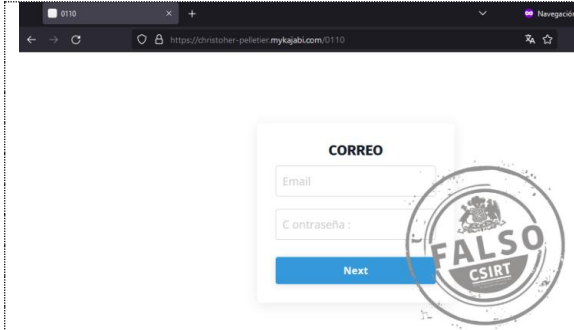
11111<

1. Malware

 <p>Acciones requeridas tras el Veredicto de Archívamiento - 606072</p> <p>Consecutoria a Revisión - info@gob.cl</p> <p>Me dirijo a usted como Laura Ramírez, Analista de Procesos en el Área de Selección de Personal de la Defensoría Pública. Adjunto encontrará el veredicto de Archívamiento Temporal.</p> <p>Veredicto de Archívamiento Temporal: 603379-05 (31.16.19)</p> <p>Cualquier pregunta que surja tras revisar el Veredicto, por favor, hágame saber.</p> <p>El no cumplimiento de las obligaciones en el plazo establecido acarreará intereses y recargos según el Artículo 899 del Código de Procedimiento Civil.</p> <p>Agradezco su atención.</p> <p>13:16:48 - 16/11/2023</p>	<h3>CSIRT alerta de nueva campaña de phishing con malware, en este caso Grandoeiro</h3> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>2CMV23-00438-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Malware</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>8 enero, 2024</td> </tr> <tr> <td>Última revisión</td> <td>8 enero, 2024</td> </tr> </table> <h3>Indicadores de compromiso</h3> <h4>URL-Dominio</h4> <p> https://espangmtes.westus2.cloudapp.azure[.]com/?25236754_966-108935108935=817902817902 https://www.dropbox[.]com/scl/fi/j3m0poowjfq9zp9glmsal/ConsultPagZDFKMQXVtlvhipmbetpeegdfYNSU.zip?rlkey=2tjq03gyi6fe4jddmo8loiarr&dl=0 http://15.229.5[.]172:24163/KvMXecvipA.xml http://15.229.5[.]172:4917/ </p> <h4>SHA256</h4> <p>cf1dc1c23e8470735195101f8d0bbaef6e9b1550326d14c54bd9d8c9127ee59c92bca8063250dcb09c12e00648e20acc8cd75eee2a7f1f83ab7755d0024049cdf5774d9f5e519d068c6d8bbf6cafaf0d46c51cd76c5364bdffc86ba74fd472ab</p> <h4>Enlaces para revisar el informe:</h4> <p>https://www.csirt.gob.cl/alertas/2cmv23-00438-01/</p>	Alerta de seguridad cibernética	2CMV23-00438-01	Clase de alerta	Fraude	Tipo de incidente	Malware	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	8 enero, 2024	Última revisión	8 enero, 2024
Alerta de seguridad cibernética	2CMV23-00438-01														
Clase de alerta	Fraude														
Tipo de incidente	Malware														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	8 enero, 2024														
Última revisión	8 enero, 2024														

CONTACTO Y REDES SOCIALES CSIRT

2. Sitios fraudulentos



CSIRT alerta de nueva página fraudulenta que suplanta inicio de sesión de correo electrónico

Alerta de seguridad cibernética	8FFR23-01629-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 enero, 2024
Última revisión	8 enero, 2024

Indicadores de compromiso

URL del sitio falso

[https://christoher-pelletier.mykajabi\[.\]com/0110](https://christoher-pelletier.mykajabi[.]com/0110)

URL de redirección

[https://new.express.adobe\[.\]com/webpage/ZRSKzIMNn4E05](https://new.express.adobe[.]com/webpage/ZRSKzIMNn4E05)

Dirección IP sitio falso

[172.64.145.117]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8ffr23-01629-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

3. Phishing



Imagen 1: Correo Electrónico



CSIRT alerta de nueva campaña de phishing via sms (smishing) que suplanta a Banco de Chile

Alerta de seguridad cibernética	8FPH23-00919-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 enero, 2024
Última revisión	8 enero, 2024

Indicadores de compromiso

URL del sitio falso

[https://support-appmibancochile.bovgn5\[.\]online/1704727026/bchile-web/persona/login/index.html/login](https://support-appmibancochile.bovgn5[.]online/1704727026/bchile-web/persona/login/index.html/login)

URL de redirección

[https://bit\[.\]ly/appmibanco](https://bit[.]ly/appmibanco)

Dirección IP sitio falso

[162.241.85.202]

Enlace para revisar loC:

<https://www.csirt.gob.cl/alertas/8fph23-00919-01/>



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

Alerta de seguridad cibernética	8FPH24-00920-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 enero, 2024
Última revisión	9 enero, 2024

Indicadores de compromiso

URL del sitio falso

[https://ifepatito.khansouq\[.\]com/1704804454/imagenes/_personas/home/default.asp](https://ifepatito.khansouq[.]com/1704804454/imagenes/_personas/home/default.asp)

URL de redirección

[https://www.cajaabogadossanjuan\[.\]org.ar/activacion/cuenta-acbv/](https://www.cajaabogadossanjuan[.]org.ar/activacion/cuenta-acbv/)

Dirección IP sitio falso

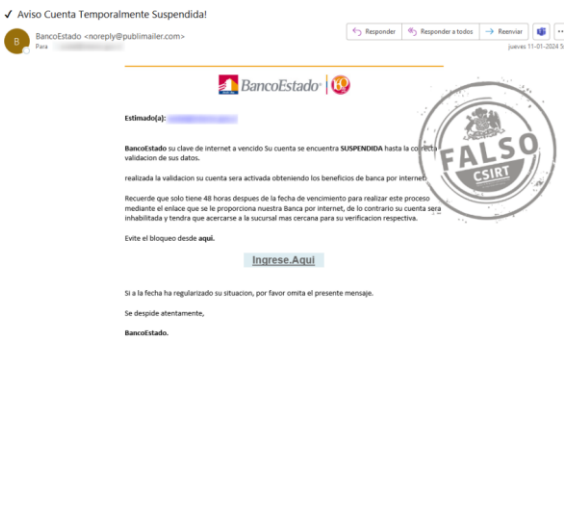
[199.188.200.192]

Enlace para revisar loC:





<https://csirt.gob.cl/alertas/8fph24-00920-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

 <p>✓ Aviso Cuenta Temporalmente Suspendida! BancoEstado <moreply@publmailier.com> Para [redacted] junio 11:01-2023</p> <p>BancoEstado</p> <p>Estimado(a):</p> <p>BancoEstado su clave de internet a vencido su cuenta se encuentra SUSPENDIDA hasta la correcta validación de sus datos.</p> <p>realizada la validación su cuenta sera activada obteniendo los beneficios de banca por internet.</p> <p>Recuerde que solo tiene 48 horas despues de la fecha de vencimiento para realizar este proceso mediante el enlace que se le proporciona nuestra Banca por internet, de lo contrario su cuenta sera inhabilitada y tendra que acercarse a la sucursal mas cercana para su verificación respectiva.</p> <p>Evite el bloqueo desde aquí.</p> <p>Ingrese Aquí</p> <p>Si a la fecha ha regularizado su situación, por favor omita el presente mensaje.</p> <p>Se despide atentamente,</p> <p>BancoEstado.</p>	<p>CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH24-00921-01</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>11 enero, 2024</td> </tr> <tr> <td>Última revisión</td> <td>11 enero, 2024</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL del sitio falso https://ucerhometadoscl[.]com/1704982755/imagenes/_personas/home/default.asp</p> <p>URL de redirección https://patitoqxshometado[.]com/activacion/cuenta-illd/</p> <p>Dirección IP sitio falso [186.64.116.145]</p> <p>Enlace para revisar IoC: https://csirt.gob.cl/alertas/8fph24-00921-01/</p>	Alerta de seguridad cibernética	8FPH24-00921-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	11 enero, 2024	Última revisión	11 enero, 2024
Alerta de seguridad cibernética	8FPH24-00921-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	11 enero, 2024														
Última revisión	11 enero, 2024														

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. Vulnerabilidades



INFORME DE Vulnerabilidad

9VSA23-00950-01
CSIRT información de vulnerabilidad crítica en Ivanti EPM

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

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de nueva vulnerabilidad crítica en Ivanti EPM

Alerta de seguridad cibernética	9VSA23-00950-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 enero, 2024
Última revisión	5 enero, 2024
CVE	
CVE-2023-39336	
Fabricante	
Ivanti	
Productos afectados	
Ivanti EPM 2021/EPM 2022 anterior a 2022 Service Update 5 (SU5).	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa23-00950-01/	



INFORME DE Vulnerabilidad

9VSA24-00951-01
CSIRT informa de actualización Update Tuesday Microsoft para enero 2024

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

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de actualización Microsoft Update Tuesday 2024 enero

Alerta de seguridad cibernética	9VSA24-00951-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	10 enero, 2024	
Última revisión	10 enero, 2024	
CVE		
CVE-2024-0056	CVE-2024-21316	CVE-2024-21309
CVE-2024-21312	CVE-2024-20660	CVE-2024-20700
CVE-2024-0057	CVE-2024-20652	CVE-2024-20699
CVE-2024-21319	CVE-2024-20658	CVE-2024-20698
CVE-2024-20677	CVE-2024-20656	CVE-2024-20696
CVE-2024-21320	CVE-2024-20653	CVE-2024-20694
CVE-2024-21318	CVE-2024-20674	CVE-2024-20691
CVE-2024-21307	CVE-2024-20672	CVE-2024-20690
CVE-2024-21306	CVE-2024-21325	CVE-2024-20662
CVE-2024-21305	CVE-2024-20666	CVE-2024-20661
CVE-2024-20697	CVE-2024-21310	CVE-2024-20657
CVE-2022-35737	CVE-2024-21314	CVE-2024-20655
CVE-2024-20692	CVE-2024-21313	CVE-2024-20654
CVE-2024-20687	CVE-2024-21311	CVE-2024-20676
CVE-2024-20683		
Fabricante		
Microsoft		
Productos afectados		
.NET 6.0		
.NET 7.0		
.NET 8.0		
Azure Storage Mover Agent		

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>

Boletín de Seguridad Cibernética N° 236





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



BOLETÍN 13BCS23-00245-01 | Semana del 5 al 11 de enero de 2024

CBL Mariner 1.0 ARM
CBL Mariner 1.0 x64
CBL Mariner 2.0 ARM
CBL Mariner 2.0 x64
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5 AND 4.8.1
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Identity Model v5.0.0
Microsoft Identity Model v5.0.0 for Nuget
Microsoft Identity Model v6.0.0
Microsoft Identity Model v6.0.0 for Nuget
Microsoft Identity Model v7.0.0
Microsoft Identity Model v7.0.0 for Nuget
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Printer Metadata Troubleshooter Tool
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft SQL Server 2022 for x64-based Systems (CU 10)
Microsoft SQL Server 2022 for x64-based Systems (GDR)
Microsoft Visual Studio 2015 Update 3
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 – 15.8)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)
Microsoft Visual Studio 2022 version 17.2
Microsoft Visual Studio 2022 version 17.4
Microsoft Visual Studio 2022 version 17.6
Microsoft Visual Studio 2022 version 17.8
Microsoft.Data.SqlClient 2.1
Microsoft.Data.SqlClient 3.1
Microsoft.Data.SqlClient 4.0
Microsoft.Data.SqlClient 5.1
System.Data.SqlClient
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 22H2 for 32-bit Systems
Windows 10 Version 22H2 for ARM64-based Systems

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>

Windows 10 Version 22H2 for x64-based Systems
Windows 11 version 21H2 for ARM64-based Systems
Windows 11 version 21H2 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 Version 22H2 for x64-based Systems
Windows 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64-based Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)
Windows Server 2022, 23H2 Edition (Server Core installation)
Enlaces para revisar el informe:
https://csirt.gob.cl/vulnerabilidades/9vsa24-00951-01/



CSIRT comparte información de vulnerabilidad parchada por Cisco en Unity Connection	
Alerta de seguridad cibernética	9VSA24-00952-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 enero, 2024
Última revisión	11 enero, 2024
CVE	
CVE-2024-20272	
Fabricante	
Cisco	
Productos afectados	
Cisco Unity Connection 14, 12.5 y anteriores.	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa23-00952-01/	

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>

5. Noticias y concientización

Ciberconsejos | Evita caer en arriendos falsos este verano

Si buscas a través de sitios web alguna propiedad para arrendar estas vacaciones, cuidado con las falsas ofertas. Evita caer en una estafa siguiendo nuestros ciberconsejos. Más recomendaciones aquí:

<https://csirt.gob.cl/recomendaciones/>



CIBERCONSEJOS

¿Cómo protegerse de los fraudes de verano?

Algunos fraudes de verano:

- Anuncios falsos en el que se utilizan fotografías robadas de otros avisos con una descripción y un precio muy atractivo.
- También existen avisos falsos en sitios especializados como Tripadvisor y Airbnb.
- Campañas de phishing con enlaces a webs falsas para robar datos bancarios, información personal u otros datos sensibles.





CIBERCONSEJOS

¿Cómo protegerse de los fraudes de verano?

Recomendaciones:

1. Desconfía de anuncios muy atractivos y demasiado económicos.
2. Sospecha si el anuncio está mal redactado o tiene faltas de ortografía.





CIBERCONSEJOS

¿Cómo protegerse de los fraudes de verano?

Recomendaciones:

3. Intenta comprobar la identidad del anunciante, la titularidad y existencia del inmueble, mediante herramientas como Google Street View.
4. Sospecha si piden un adelanto o proponen formas alternativas de pago.





CIBERCONSEJOS





¿Cómo protegerse de los fraudes de verano?

Si fuiste víctima de una estafa:

- 1 Denuncia la falsa oferta a los responsables de la plataforma.
- 2 Recopila todas las pruebas que puedas de la estafa e información sobre el anunciante.
- 3 Denuncia con las autoridades pertinentes, como la Policía de Investigaciones (PDI), llamando al +562 2708 0658.



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>

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.

- Andrés Ignacio Castro Zuleta Phishing
- Felipe Vidal Phishing
- OSI - VTI UCHILE Phishing
- Fernando Enrique González Phishing
- María José Fuentes Urrutia Phishing
- Hugo Gabriel Montecinos Ataque de denegación de servicio
- Felipe Hott Delgado Exfiltración de Información
- Vicente Andrés Mancilla Phishing
- Miguel Morales Saravia Phishing

CONTACTO Y REDES SOCIALES CSIRT