Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

12-03-2021 | Año 3 | N°88

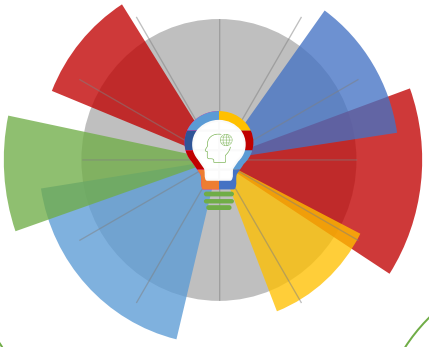
Boletín de Seguridad Cibernética

Semana del 5 al 11 de marzo de 2021

La semana en cifras

Hash
16
SHA
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron
5
URL
Asociadas a sitios fraudulentos y campañas de phishing



Parches
133
para vulnerabilidades
Las mitigaciones son útiles para productos de Microsoft, Google, Cisco, Adobe, F5 y Apple.

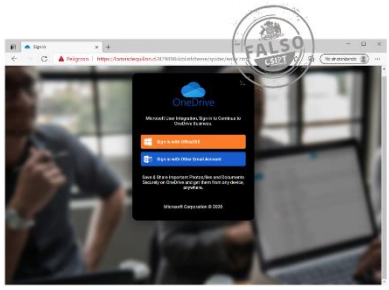
IP
17
Informadas
Listado de IP advertidas en múltiples campañas de phishing y de malware.

*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Sitios fraudulentos

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta a Microsoft OneDrive	
Alerta de seguridad cibernética	8FFR21-00912-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2021
Última revisión	8 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://lomasdequillon[.]cl/879898iikblinfdteere/spider/error.html	
IP	
[50.87.153.17]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00912-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00912-01.pdf	

Imagen del sitio

CSIRT alerta de sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00913-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2021
Última revisión	8 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://bnca-personasmsvalida[.]live/1615227156/personas/index.asp	
IP	
[198.54.116.129]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00913-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00913-01.pdf	

Imagen del sitio

CSIRT alerta de sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00914-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2021
Última revisión	8 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://appvalida-santandr[.]live/1615227171/personas/index.asp	
IP	
[68.65.122.237]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00914-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00914-01.pdf	

Imagen del sitio

CSIRT alerta de sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00915-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2021
Última revisión	8 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://smsvalidar-santder[.]website/1615227368/personas/index.asp	
IP	
[68.65.122.237]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00915-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00915-01.pdf	

Imagen del sitio

CSIRT alerta de sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-00916-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de marzo de 2021
Última revisión	9 de marzo de 2021
Indicadores de compromiso	
URL sitio falso	
https://banco-santander.cl-dg[.]xyz/1615227524/index.asp	
IP	
[104.21.33.30]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00916-01/	
https://www.csirt.gob.cl/media/2021/03/8FFR21-00916-01.pdf	

Vulnerabilidades

CSIRT informa de vulnerabilidades en Microsoft Edge	
Alerta de seguridad cibernética	9VSA21-00401-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	8 de marzo de 2021
Última revisión	8 de marzo de 2021

CVE

CVE-2021-21183	CVE-2021-21168	CVE-2021-21179
CVE-2021-21173	CVE-2021-21169	CVE-2021-21180
CVE-2021-21159	CVE-2021-21170	CVE-2021-21181
CVE-2021-21160	CVE-2021-21171	CVE-2021-21174
CVE-2021-21161	CVE-2021-21172	CVE-2021-21184
CVE-2021-21162	CVE-2020-27844	CVE-2021-21185
CVE-2021-21163	CVE-2021-21175	CVE-2021-21186
CVE-2021-21164	CVE-2021-21182	CVE-2021-21187
CVE-2021-21165	CVE-2021-21176	CVE-2021-21188
CVE-2021-21166	CVE-2021-21177	CVE-2021-21189
CVE-2021-21167	CVE-2021-21178	CVE-2021-21190

Fabricante

Microsoft

Productos afectados

Microsoft Edge (basado en Chromium) versiones de 79.0.309.71 a la 88.0.705.74.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00401-01
https://www.csirt.gob.cl/media/2021/02/9VSA21-00401-01.pdf

CSIRT alerta de vulnerabilidad que afecta a productos de Apple	
Alerta de seguridad cibernética	9VSA21-00402-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2021
Última revisión	10 de marzo de 2021

CVE

CVE-2021-1844

Fabricante

Apple

Productos afectados

iOS 14.4, iPadOS 14.4, macOS Big Sur y Apple watchOS 7.3.1. Safari 14.0.3 para macOS Catalina y macOS Mojave.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00402-01
https://www.csirt.gob.cl/media/2021/02/9VSA21-00402-01.pdf

CSIRT informa sobre nuevas vulnerabilidades informadas por Microsoft	
Alerta de seguridad cibernética	9VSA21-00403-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2021
Última revisión	10 de marzo de 2021

CVE

CVE-2021-27053	CVE-2021-26869	CVE-2021-24090
CVE-2021-27054	CVE-2021-26870	CVE-2021-24095
CVE-2021-27055	CVE-2021-26871	CVE-2021-24104
CVE-2021-27056	CVE-2021-26872	CVE-2021-24107
CVE-2021-27057	CVE-2021-26873	CVE-2021-24108
CVE-2021-27058	CVE-2021-26874	CVE-2021-24110
CVE-2021-27059	CVE-2021-26875	CVE-2021-26411
CVE-2021-27060	CVE-2021-26876	CVE-2021-26880
CVE-2021-27061	CVE-2021-26877	CVE-2021-26881
CVE-2021-26879	CVE-2021-26878	CVE-2021-26882
CVE-2021-26902	CVE-2021-27062	CVE-2021-26884
CVE-2021-27047	CVE-2021-27063	CVE-2021-26885
CVE-2021-27048	CVE-2021-27066	CVE-2021-26886
CVE-2021-27049	CVE-2021-27070	CVE-2021-26887
CVE-2021-27050	CVE-2021-27074	CVE-2021-26889
CVE-2021-27051	CVE-2021-27075	CVE-2021-26890
CVE-2021-27052	CVE-2021-27076	CVE-2021-26891
CVE-2021-26701	CVE-2021-27077	CVE-2021-26892
CVE-2021-26859	CVE-2021-27080	CVE-2021-26893
CVE-2021-26860	CVE-2021-27081	CVE-2021-26894
CVE-2021-26861	CVE-2021-27082	CVE-2021-26895
CVE-2021-26862	CVE-2021-27083	CVE-2021-26896
CVE-2021-26863	CVE-2021-27084	CVE-2021-26897
CVE-2021-26864	CVE-2021-27085	CVE-2021-26898
CVE-2021-26865	CVE-2021-1640	CVE-2021-26899
CVE-2021-26866	CVE-2021-1729	CVE-2021-26900
CVE-2021-26867	CVE-2021-21300	CVE-2021-26901
CVE-2021-26868	CVE-2021-24089	

Fabricante

Microsoft

Productos afectados

Windows	Office
Azure	Office Services
Azure DevOps	Web Apps
Azure Sphere	SharePoint Server
Internet Explorer	Visual Studio
Edge	Windows Hyper-V

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00403-01
https://www.csirt.gob.cl/media/2021/02/9VSA21-00403-01.pdf

CSIRT advierte vulnerabilidades informadas por Adobe	
Alerta de seguridad cibernética	9VSA21-00404-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de marzo de 2021
Última revisión	2 de marzo de 2021
CVE	
CVE-2021-21079	CVE-2021-21085
CVE-2021-21068	CVE-2021-21069
CVE-2021-21080	CVE-2021-21078
CVE-2021-21081	CVE-2021-21056
Fabricante	
Adobe	
Productos afectados	
Adobe Connect, versión 11.0.5 y anteriores. Adobe Creative Cloud Desktop Application, version 5.3 y anteriores. Adobe Framemaker 2020.0.2 para Windows.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00404-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00404-01.pdf	

CSIRT alerta sobre vulnerabilidades en productos F5	
Alerta de seguridad cibernética	9VSA21-00405-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2021
Última revisión	10 de marzo de 2021
CVE	
CVE-2021-22986	CVE-2021-22990
CVE-2021-22987	CVE-2021-22991
CVE-2021-22988	CVE-2021-22992
CVE-2021-22989	
Fabricante	
F5	
Productos afectados	
BIG-IP BIG-IQ BIG-IP Advanced WAF/ASM	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00405-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00405-01.pdf	

CSIRT alerta sobre vulnerabilidades en switches Cisco Nexus 3000 Series Y Nexus 9000 Series	
Alerta de seguridad cibernética	9VSA21-00406-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de marzo de 2021
Última revisión	10 de marzo de 2021
CVE	
CVE-2021-1361	
Fabricante	
Cisco	
Productos afectados	
Switches Nexus 3000 Series y Nexus 9000 Series que usen Cisco NX-OS versiones 9.3 (5) o 9.3 (6).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00406-01	
https://www.csirt.gob.cl/media/2021/02/9VSA21-00406-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.

CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash de archivos maliciosos	Documento web
1f29f028fa98c6bc13f16a560cce47516b18a23cf7bc2ae3c96e3dc05d4fd907	2CMV21-00152-01
a79c8527653260a362ccb804a3f2916461f54f844b93d30e00294b976c49e12a	2CMV21-00152-01
bb112d4e23f3835f3a1d8badc92b3081e4d92e8c73a7837e90f2f29b7ef6da65	2CMV21-00152-01
a5304c2f60b15a67a86f7611b2ff47e5b2a39000a93929ba93f995b2c7d4b7d1	2CMV21-00152-01
bc408f72c8be09e949ccc77140d5a7994429fb1a2c61a709e13905e331e070ae	2CMV21-00152-01
c35e35461f5e7f082ece0a7c56a0a0c52d8e33e6066326ef0193729b4b4bdba8	2CMV21-00152-01
5f81706144c6ab4979d34f5f5e874b6a74c14d061fb9b2994b21456076696c1a	2CMV21-00152-01
768e3902e97b4f455c601938013a3bb54ff9cf069e2249d3a47c191f8097f69e	2CMV21-00152-01
11c2e6a14362b67851b39d700438412b812c60a42c6ea2bbceaf8500efdea4b1	2CMV21-00152-01
f31eb91f999f372c0bf29efebd9b7aff42fc737895f5e8f79f73f419ac7da279	2CMV21-00152-01
849f6ca81256c6c83749cae8ea06fdc298d0a5bdbffdf8fdf699969e859d2dc8	2CMV21-00152-01
4a5d3f604434e49d1c7930783a99ff4de0c68264300ec0534e9e779fbf8c269d	2CMV21-00152-01
4a32747eaf957a032a507675509b32c1b8f890c0316e58f7a01bcbdca3ccbfd3	2CMV21-00152-01
1950780ba11f97f2e67d0c16d66be88afc0a0269c568ab53d468fbe20e06250f	2CMV21-00152-01
c8c0f14667c269845970022ca4c61267b3e8f554e7cbc0c91963c55f1ad97832	2CMV21-00152-01
6b610061618fd7775855d695fc4af8518f312ba53d6709c657d560165e4d7c79	2CMV21-00152-01

Direcciones IP de servidor SMTP donde es enviado el correo malicioso: Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

IP	Etiqueta de sistema autónomo	Documento web
190.210.186.137	NSS S.A.	2CMV21-00152-01
49.12.124.200	Hetzner Online GmbH	2CMV21-00152-01
192.232.198.199	UNIFIEDLAYER-AS-1	2CMV21-00152-01
84.38.133.32	DataClub S.A.	2CMV21-00152-01
103.151.122.27	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	2CMV21-00152-01
37.49.225.171	PEENQ.NL	2CMV21-00152-01

142.147.97.145	UNREAL-SERVERS	2CMV21-00152-01
45.85.90.232	Des Capital B.V.	2CMV21-00152-01
37.49.225.139	PEENQ.NL	2CMV21-00152-01
174.136.28.112	AS-TIERP-36024	2CMV21-00152-01
199.127.59.214	FIBERHUB	2CMV21-00152-01
66.154.98.110	PERFORMIVE	2CMV21-00152-01
31.210.20.191	Des Capital B.V.	2CMV21-00152-01

Correos electrónicos de donde son enviados los archivos adjunto con malware.

Dirección	Documento web
rania@lecercle.me	2CMV21-00152-01
Lourdes.Martinez@heidelberg.com	2CMV21-00152-01
osaimiao@sabic.com	2CMV21-00152-01
info@starlinktradings.com	2CMV21-00152-01
codink@sealcode.com	2CMV21-00152-01
acts@sreetrans.in	2CMV21-00152-01
account@db.com	2CMV21-00152-01
sales@shshenke.com.cn	2CMV21-00152-01
info@acc.com	2CMV21-00152-01
ops@tanbinhshipping.com	2CMV21-00152-01
ivan@aikom-kvalitet.com	2CMV21-00152-01
marjie@aimstelecom.com	2CMV21-00152-01
sales@carlinkmotors.com	2CMV21-00152-01
noreply@ir.netease.com	2CMV21-00152-01
rania@lecercle.me	2CMV21-00152-01
Lourdes.Martinez@heidelberg.com	2CMV21-00152-01
osaimiao@sabic.com	2CMV21-00152-01
info@starlinktradings.com	2CMV21-00152-01
codink@sealcode.com	2CMV21-00152-01
acts@sreetrans.in	2CMV21-00152-01
account@db.com	2CMV21-00152-01
sales@shshenke.com.cn	2CMV21-00152-01
info@acc.com	2CMV21-00152-01

Actualidad

SUSESO firma normativa en materia de ciberseguridad junto al CSIRT de Gobierno

En presencia del Subsecretario del Interior, Juan Francisco Galli, la Superintendenta (s) de Seguridad Social (SUSESO), Patricia Soto Altamirano, firmó hoy la circular que fija los estándares y normativas para la gestión de la información e implementación de la ciberseguridad para la Intendencia de Seguridad y Salud en el Trabajo (ISESAT), iniciativa llevada a cabo junto al Equipo de Respuesta Ante Incidentes de Seguridad Informática (CSIRT) de Gobierno.

Con esta firma se concreta un importante hito en cuanto al trabajo que ha estado realizando el Gobierno con las superintendencias para entregar los lineamientos de ciberseguridad a los sectores no regulados, y así proteger y cuidar la información y datos de los chilenos e instituciones.

En una reunión encabezada por el Subsecretario del Interior, Juan Francisco Galli en La Moneda, junto con la Superintendenta (s) de Seguridad Social, Patricia Soto Altamirano, se llevó a cabo la firma de la Normativa de Ciberseguridad para la Gestión de la Seguridad de la Información que será aplicada a las mutuales, entidades fiscalizadas por la Intendencia de Seguridad y Salud en el Trabajo.

En 2020 la Subsecretaría del Interior, a través del Equipo de Respuesta Ante Incidentes de Seguridad Informática (CSIRT de Gobierno), comenzó a trabajar en conjunto con las distintas superintendencias y subsecretarías "para entregar lineamientos que permitan establecer estándares de ciberseguridad, y así fortalecer a las entidades y proteger su información. Para esto, definimos pilares que aseguran que cada organización cuente con medidas de análisis de riesgo, prevención y gestión de la ciberseguridad, criterios de notificación y notificación", explica el Subsecretario del Interior, Juan Francisco Galli.

"Este es un importante avance en materia de ciberseguridad para Chile. Así, pese a que aún nos falta contar con una ley que regule a todos los sectores de la economía, esta normativa nos permite establecer criterios de seguridad a las instituciones supervisadas o reguladas, para también coordinarlas y sentar bases comunes en preparación para la eventual legislación. De esta manera, podemos proteger la información de todos los chilenos y asegurar la continuidad de las operaciones y servicios, aún sin existir todavía la ley. Esta firma concreta el trabajo que hemos realizado desde agosto con la Subsecretaría de Telecomunicaciones, y posteriormente con la SUSESO, además de otras superintendencias con las que igualmente estamos trabajando en la definición de normativas", enfatiza el Subsecretario del Interior.

A su vez, la Superintendenta (s) Patricia Soto Altamirano, anunció el inicio de trabajo conjunto entre la Intendencia de Beneficios Sociales (IBS) de SUSESO y CSIRT, para desarrollar colaborativamente la norma técnica en materia de ciberseguridad para las Cajas de Compensación y Asignación Familiar (CCAF): "Es prioridad para nuestra institución extender a otros ámbitos estas normativas, particularmente a las instituciones que manejan datos e información de la ciudadanía, como lo son las Cajas de Compensación, debido a los múltiples servicios que prestan en materia de seguridad social", aseveró la Superintendenta (s).

La normativa está disponible en el sitio web www.suseso.cl

Día Internacional de la Mujer: Ciberconsejos para estar más protegidas en el mundo virtual

Hoy se recuerda un nuevo Día Internacional de la Mujer, fecha oficialmente conmemorada por las Naciones Unidas cada 8 de marzo. Y debido a que internet es una de las vías por las cuales muchas mujeres son víctimas cada día de violencia de género, queremos aprovechar esta efeméride para recordar algunos de los principales riesgos al desenvolverse en la red, y algunas conductas seguras que es recomendable adoptar para reducirlos.

La infografía completa en PDF, con todos los consejos, aquí:
https://www.csirt.gob.cl/recomendaciones/dia-internacional-de-la-mujer/

.

Vulnerabilidades críticas en Microsoft Exchange

Si bien ante la revelación de vulnerabilidades críticas en Exchange hecha por Microsoft el 2 de marzo, el CSIRT de Gobierno publicó un reporte para advertir a la comunidad de la necesidad de parchar servidores de Exchange (el documento, aquí: csirt.gob.cl/vulnerabilidades/9vsa21-00400-01), la gravedad de las vulnerabilidades y el hecho de que están siendo activamente explotadas por actores estatales nos conminó a publicar un nuevo documento, el que fue publicado en la sección de Noticias de nuestra web, con detalles de los efectos que han tenido estas vulnerabilidades y los pasos para remediarlas, explicados en más detalle.

Este archivo puede ser encontrado en el siguiente enlace:
https://www.csirt.gob.cl/noticias/resumen-de-la-alerta-por-vulnerabilidades-criticas-en-microsoft-exchange/.

Recomendaciones y Buenas Prácticas

Recomendaciones generales de seguridad

- 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 los sitios web que se ingresen sean los oficiales.

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 públicos del Estado, al informar problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Ewald Beekman
- Álvaro Salinas
- Jeremías Rojas Leal
- Diego Sebastián Valenzuela Castillo

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.12 16:21:16 -03'00'