Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

17-06-2022 | Año 4 | N°154

Boletín de Seguridad Cibernética

Semana del 10 al 16 de junio de 2022

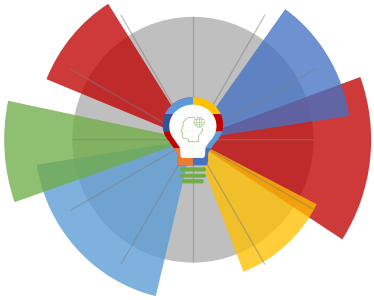
La semana en cifras

Parches

121

para vulnerabilidades

Sus mitigaciones son útiles en productos de Drupal, Microsoft, Adobe, Cisco y Google.



Se advirtieron

4

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

IP

4

Informadas

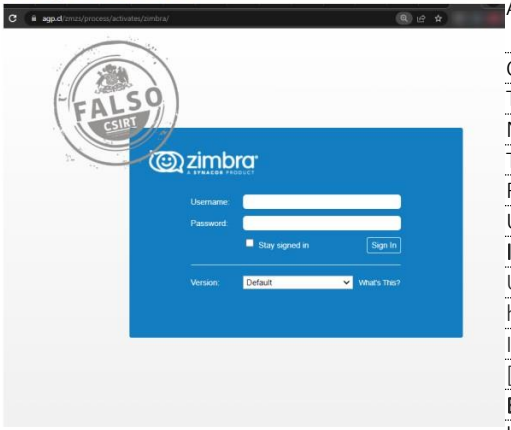
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

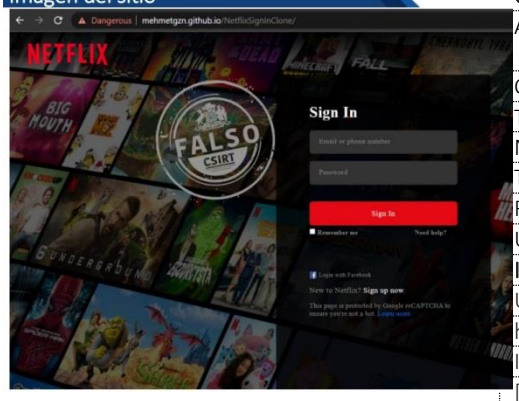
Sitios fraudulentos

Imagen del sitio



CSIRT informa página falsa de Zimbra web	
Alerta de seguridad cibernética	8FFR22-01087-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de junio de 2022
Última revisión	10 de junio de 2022
Indicadores de compromiso	
URL sitio falso	
https://agp[.]cl/zmzs/process/activates/zimbra/	
IP	
[186.64.118.20]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01087-01/	
https://www.csirt.gob.cl/media/2022/06/8FFR22-01087-01.pdf	

Imagen del sitio



CSIRT informa página web que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR22-01088-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de junio de 2022
Última revisión	13 de junio de 2022
Indicadores de compromiso	
URL sitio falso	
https://mehmetgzn.github[.]io/NetflixSignInClone/	
IP	
[185.199.111.153]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01088-01/	
https://www.csirt.gob.cl/media/2022/06/8FFR22-01088-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing con falsa cuenta bloqueada	
Alerta de seguridad cibernética	8FPH22-00541-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2022
Última revisión	14 de junio de 2022
Indicadores de compromiso	
URL Redirección	
http://asedl[.]am/Servicio_Estado/cuenta-tfzg/	
URL sitio falso	
https://sixthstartech[.]com/Resumen/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[168.232.165.2]	
[192.254.225.27]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00541-01/	
https://www.csirt.gob.cl/media/2022/06/8FPH22-00541-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidades que afectan a Drupal	
Alerta de seguridad cibernética	9VSA22-00654-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2022
Última revisión	14 de junio de 2022
CVE	
CVE-2022-31042 CVE-2022-31043	
Fabricante	
Drupal	
Productos afectados	
Drupal 8 y 9 Drupal 9.4, actualizar a Drupal 9.4.0-rc2. Drupal 9.3, actualizar a Drupal 9.3.16. Drupal 9.2, actualizar a Drupal 9.2.21.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00654-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00654-01-2.pdf	

CSIRT informa de nuevas vulnerabilidades en Google Chrome	
Alerta de seguridad cibernética	9VSA22-00655-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2022
Última revisión	14 de junio de 2022
CVE	
CVE-2022-2007 CVE-2022-2008 CVE-2022-2010 CVE-2022-2011	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones anteriores a 102.0.5005.115. Actualizar a Chrome 102.0.5005.115.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00655-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00655-01-1.pdf	

CSIRT comparte vulnerabilidades del Update Tuesday de Microsoft Junio 2022	
Alerta de seguridad cibernética	9VSA22-00656-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2022
Última revisión	14 de junio de 2022

CVE

CVE-2022-21123 - CVE-2022-21125 - CVE-2022-21127
CVE-2022-21166 - CVE-2022-22018 - CVE-2022-29111
CVE-2022-29119 - CVE-2022-29143 - CVE-2022-29149
CVE-2022-30131 - CVE-2022-30132 - CVE-2022-30135
CVE-2022-30136 - CVE-2022-30137 - CVE-2022-30139
CVE-2022-30140 - CVE-2022-30141 - CVE-2022-30142
CVE-2022-30143 - CVE-2022-30145 - CVE-2022-30146
CVE-2022-30147 - CVE-2022-30148 - CVE-2022-30149
CVE-2022-30150 - CVE-2022-30151 - CVE-2022-30152
CVE-2022-30153 - CVE-2022-30154 - CVE-2022-30155
CVE-2022-30157 - CVE-2022-30158 - CVE-2022-30159
CVE-2022-30160 - CVE-2022-30161 - CVE-2022-30162
CVE-2022-30163 - CVE-2022-30164 - CVE-2022-30165
CVE-2022-30166 - CVE-2022-30167 - CVE-2022-30168
CVE-2022-30171 - CVE-2022-30172 - CVE-2022-30173
CVE-2022-30174 - CVE-2022-30177 - CVE-2022-30178
CVE-2022-30179 - CVE-2022-30180 - CVE-2022-30184
CVE-2022-30188 - CVE-2022-30189 - CVE-2022-30193
CVE-2022-32230

Fabricante

Microsoft

Productos afectados

.NET 6.0
.NET Core 3.1
AV1 Video Extension
Azure Automation State Configuration, DSC Extension
Azure Automation Update Management
Azure Diagnostics (LAD)
Azure Open Management Infrastructure
Azure Real Time Operating System
Azure Real Time Operating System GUIX
Azure Security Center
Azure Sentinel
Azure Service Fabric
Azure Stack Hub
Container Monitoring Solution
HEVC Video Extension
HEVC Video Extensions
Log Analytics Agent

Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Photos
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (CU 17)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connectivity Pack
Microsoft SQL Server 2017 for x64-based Systems (CU 29)
Microsoft SQL Server 2017 for x64-based Systems (GDR)
Microsoft SQL Server 2019 for x64-based Systems (CU 16)
Microsoft SQL Server 2019 for x64-based Systems (GDR)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8)
Microsoft Visual Studio 2022 version 17.0
Microsoft Visual Studio 2022 version 17.2
NuGet.exe
System Center Operations Manager (SCOM) 2016
System Center Operations Manager (SCOM) 2019
System Center Operations Manager (SCOM) 2022
Visual Studio 2019 for Mac version 8.10
Visual Studio 2022 for Mac version 17.0
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 20H2 for 32-bit Systems

Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for x64-based Systems Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 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 11 for ARM64-based Systems Windows 11 for x64-based Systems Windows 7 for 32-bit Systems Service Pack 1 Windows 7 for x64-based Systems Service Pack 1 Windows 8.1 for 32-bit systems Windows 8.1 for x64-based systems Windows RT 8.1 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 Azure Edition Core Hotpatch Windows Server, version 20H2 (Server Core Installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00656-01/
https://www.csirt.gob.cl/media/2022/06/9VSA22-00656-01.pdf

CSIRT comparte vulnerabilidades informadas para productos Cisco	
Alerta de seguridad cibernética	9VSA22-00657-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2022
Última revisión	15 de junio de 2022
CVE	
CVE-2021-1579 - CVE-2022-22965 - CVE-2022-20742 CVE-2022-20742 - CVE-2022-20715 - CVE-2022-20759 CVE-2022-20745 - CVE-2022-20737 - CVE-2022-20760 CVE-2022-20774 - CVE-2022-20821 - CVE-2022-20806 CVE-2022-20807 - CVE-2022-20809	
Fabricante	
Cisco	
Productos afectados	
CVE-2022-22965: Vulnerabilidad en el Spring Framework, que afecta a las aplicaciones Spring MVC y Spring WebFlux que corren en JDK 9+.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00657-01/	
https://www.csirt.gob.cl/media/2022/06/9VSA22-00657-01.pdf	

CSIRT alerta de nuevas vulnerabilidades en productos Adobe		
Alerta de seguridad cibernética	9VSA22-00658-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	15 de junio de 2022	
Última revisión	15 de junio de 2022	
CVE		
CVE-2022-30664	CVE-2022-30661	CVE-2022-30640
CVE-2022-28839	CVE-2022-30662	CVE-2022-30641
CVE-2022-28840	CVE-2022-30663	CVE-2022-30642
CVE-2022-28841	CVE-2022-30665	CVE-2022-30643
CVE-2022-28842	CVE-2022-30660	CVE-2022-30644
CVE-2022-28843	CVE-2022-30652	CVE-2022-30645
CVE-2022-28844	CVE-2022-30653	CVE-2022-30646
CVE-2022-28845	CVE-2022-30654	CVE-2022-30647
CVE-2022-28846	CVE-2022-30655	CVE-2022-30648
CVE-2022-28847	CVE-2022-30656	CVE-2022-30649
CVE-2022-28848	CVE-2022-30657	CVE-2022-30666
CVE-2022-28849	CVE-2022-28850	CVE-2022-30667
CVE-2022-30650	CVE-2022-30637	CVE-2022-30668
CVE-2022-30651	CVE-2022-30638	CVE-2022-30669

CVE-2022-30658 CVE-2022-30659	CVE-2022-30639	CVE-2022-30670
Fabricante		
Adobe		
Productos afectados		
Adobe Animate 22.0.5 y anteriores. Adobe Bridge 12.0.1 y anteriores. Adobe Illustrator 2022 26.0.2 y anteriores. Adobe Illustrator 2021 25.4.5 y anteriores. Adobe InCopy 17.2 y anteriores. RoboHelp Server 11		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00658-01/		
https://www.csirt.gob.cl/media/2022/06/9VSA22-00658-01.pdf		

Actualidad

Internet Explorer 11 dejó de ser compatible con algunos sistemas operativos

El CSIRT de Gobierno informa que Internet Explorer 11 (IE11), componente del sistema operativo (SO) Windows, dejó de ser compatible con ciertos sistemas operativos a partir del 15 de junio de 2022. Esto significa que algunas aplicaciones web diseñadas para Internet Explorer 11 dejarán de funcionar. Llamamos a analizar sus recursos web y seguir las acciones delineadas a continuación.

https://www.csirt.gob.cl/noticias/internet-explorer-11-dejara-de-ser-compatible-con-algunos-sistemas-operativos/

Implicancias

Algunas aplicaciones web fueron desarrolladas manteniendo compatibilidad únicamente con Internet Explorer 11. Por eso, desde el 15 de junio se pone en riesgo la operatividad del acceso web de dichos aplicativos, y en consecuencia, el funcionamiento mismo de los aplicativos o sistemas construidos con esta dependencia. Desafortunadamente, un conjunto de aplicaciones *legacy* no migradas oportunamente se ven enfrentadas a un potencial "naufragio" al perder su navegador.

¿Cómo responder?

Se recomiendan dos alternativas:

- Articular con el área TI que los usuarios reemplacen el navegador Internet Explorer 11, usando en su lugar Microsoft Edge con el modo IE, el cual promete compatibilidad con versiones anteriores hasta al año 2029, aproximadamente.

Existe un conjunto de sistema operativos que mantendrán aun compatibilidad con IE11, los que se podrían utilizar pero solo como un mecanismo para obtener un poco más de tiempo y poder activar lo antes posible los procesos de migración necesarios para eliminar los sitios *legacy* de la institución.

- Migrar las aplicaciones dependientes del IE11 hacia un nuevo desarrollo que guarde compatibilidad con los navegadores actuales. Esta es la real solución y la acción a realizar cuanto antes sea posible.

IMPORTANTE: Si bien se ha propuesto como solución de emergencia suspender las actualizaciones a partir del 15 de junio, esta alternativa no hace más que contener un riesgo e incrementar muchos otros, al no permitir la normal actualización del resto de aplicaciones. Por lo tanto, el CSIRT de Gobierno recomienda no implementar esta estrategia.

¿Qué sistemas operativos se ven afectados por esta acción?

Aplicación de escritorio Internet Explorer 11 entregada a través del canal semestral (SAC):

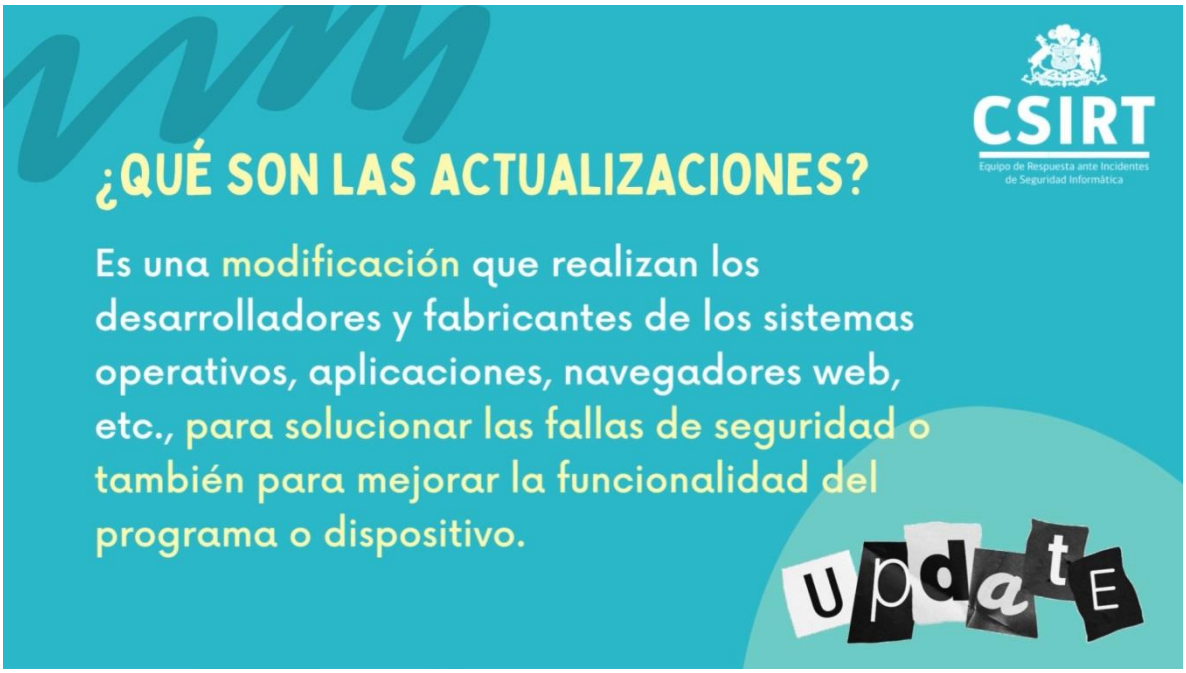
Windows 10 (versión 20H2 y posteriores)
Windows 10 IoT (versión 20H2 y posterior)
Fuera del alcance en el momento de este anuncio (no afectado):

Modo Internet Explorer en Microsoft Edge.
Plataforma Internet Explorer (MSHTML/Trident), incluido WebOC.
Aplicación de escritorio Internet Explorer 11 en:
Windows 8.1
Actualizaciones de seguridad extendidas de Windows 7 (ESU)
Windows Server SAC (todas las versiones)
Canal de mantenimiento a largo plazo (LTSC) de Windows 10 IoT (todas las versiones)
Windows Server LTSC (todas las versiones)
Cliente de Windows 10 LTSC (todas las versiones)

Ciberconsejos | ¿En qué consisten las Actualizaciones de Seguridad?

Todos los sistemas operativos, navegadores web y/o aplicaciones pueden tener un fallo de seguridad. Esto incluye los smartphones, tablets, televisores inteligentes e incluso las consolas de videojuegos. Para corregir estos fallos, se debe actualizar. Pero qué son y por qué se consideran tan importantes.

Se los contamos en el siguiente video: https://www.csirt.gob.cl/recomendaciones/actualizacion/



Ciberconsejos | Control Parental

De cara a las próximas vacaciones de invierno y a que muchos niños pasan mucho tiempo frente a las pantallas, decidimos dedicar nuestros ciberconsejos de esta semana a comentarles de qué se trata y cuándo pueden ser útiles los sistemas de Control Parental, que permiten limitar el contenido al que acceden los niños y también registrar lo que hacen en línea.

Pueden revisar y compartir estos consejos también a través del siguiente enlace: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-control-parental/

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 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 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 (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.

- Gonzalo Araya
- Álvaro Villalón
- Paulina Cáceres
- Roberto Mira
- Matías Peña
- Andrés Aldana
- Hans Sandoval
- José Gastón Muñoz
- Vanessa Hernández
- María Soledad Apostolidis
- Enrique Céspedes
- Mathias Roco
- Matías Peña
- Óscar Guarda