Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

01 de junio 2021

Índice

1. Resumen Ejecutivo 3
2. Alcances del Informe 4
3. Tipos de Tickets 5
4. Tipos de Ticket Públicos y Privados 7
5. Estado de Ticket Procesados en el Presente Mes 8
6. Procedencia de Generación de Tickets 9
7. Fuentes de Origen Externo de Tickets 10
8. Boletines con resúmenes de alertas y vulnerabilidades del mes 11
9. Síntesis de gestión sobre concientización y buenas prácticas 12
Actualidad 14

Índice de Ilustraciones

Ilustración 1 - Tipos de tickets 5
Ilustración 3–- Tickets a Instituciones Públicas y Privadas 7
Ilustración 4 - Total Estado de Tickets 8
Ilustración 5- Distribución Porcentual de Origen de Tickets 9
Ilustración 6- Tipos de servicios externos 10

Índice de Tablas

Tabla 1 - Total Tipos de Tickets 5
Tabla 2 - Ranking de Alertas Recibidas 6
Tabla 3 - Tickets a Instituciones Públicas y Privadas 7
Tabla 4 - Total Estado de Ticket 8
Tabla 5 - Fuentes de Servicios (Interna y/o Externa) 9
Tabla 6 - Fuentes de Origen Externo de Tickets 10

1. Resumen Ejecutivo

El presente informe contiene un resumen de la totalidad de los tickets procesados en el mes de mayo de 2021. El documento muestra la composición de los tickets desagregados por categorías que corresponden al tipo de vulnerabilidad de las incidencias que originaron los tickets.

El informe también da cuenta del porcentaje de tickets que fueron cerrados con éxito en el curso del mes de mayo y también muestra la proporción de aquellos que quedan por terminar.

Asimismo, en este documento se muestra por categorías los tipos de tickets que se reportan para notificar a las instituciones públicas o privadas.

Este reporte mensual muestra, además, el origen o procedencia de la información que procesa CSIRT –si es interna o externa- y presenta en términos porcentuales el peso relativo que cada una de estas fuentes tiene dentro de la demanda de trabajo que se recibió durante el mes.

Adicionalmente, también se entrega un desagregado con el detalle que permite conocer la participación –en cantidades y en términos porcentuales- de las diversas fuentes externas que componen la actual generación de tickets desde ese origen de procedencia.

Finalmente, se presenta información proveniente de la plataforma MISP[1] que contiene la cantidad de posibles IoCs[2] o –Índices de Compromiso- que se hayan detectado. Esta información es relevante para CSIRT dado que se utiliza como punto de partida para validar correlaciones con todas nuestras plataformas de análisis. En el informe se expone una tabla donde se puede enumerar la cantidad de IoCs detectados en el presente mes, los cuales se presentan diferenciados en base a direcciones IP[3] o a URL[4].

[1] MISP es una sigla en idioma inglés que significa Malware Information Sharing Platform o "Plataforma para compartir información de Malware y amenazas".
[2] IOC es una sigla en idioma inglés que significa "Índice de compromiso", y se refiere a la descripción de un incidente de ciberseguridad, actividad y/o artefacto malicioso mediante patrones.
[3] IP es una sigla en idioma inglés que significa "Internet Protocol" y corresponde a un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone).
[4] Es una sigla en idioma inglés que significa Uniform Resource Locator o "Localizador Uniforme de Recursos". Se trata de la secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de Internet para que puedan ser localizados. Los documentos de texto, las fotografías y los audios, entre otros tipos de contenidos digitales, tienen un URL cuando se publican en Internet. Estos localizadores permiten crear hipervínculos. De esta forma, el URL, por lo tanto, es el conjunto de caracteres que posibilita la asignación de una dirección exclusiva a un recurso que se encuentra disponible en el espacio virtual. En otras palabras, el URL es una dirección de Internet que, al ser encontrada y visualizada por un navegador, muestra un recurso de información al usuario.

2. Alcances del Informe

La información que se muestra en el presente informe proviene de la gestión de CSIRT en el marco del proceso de notificación a entidades, instituciones y/u organismos afectados. Esa información se produce como consecuencia de las actividades desarrolladas por el equipo 24/7 en un período de tiempo mensual. A continuación, se enumera resumidamente esas actividades:

- Gestión de tickets generados, efectuando seguimiento y validando las acciones que se tomaron con el ticket enviado al organismo gubernamental afectado.

- Reporte de vulnerabilidades de aquellos tickets precedentes una vez validado que la falla de seguridad se encuentre aún presente.

- Generación de análisis y reporte de vulnerabilidades detectadas dentro de la RCE[5] (falta cifrado, CMS obsoletos, credenciales recuperadas, servidores desactualizados, puertos expuestos, Phishing, deface, etc…).

- Seguimiento a los tickets reportados (contacto mediante llamada telefónica y/o correo electrónico) para validar qué acciones ha tomado la entidad reportada con la información de la vulnerabilidad detectada.

- Análisis y monitoreo de un listado de -6.200 sitios aproximadamente- los cuales corresponden a portales gubernamentales, a los que se ha validado su estatus utilizando las plataformas Splunk, Pingdom y PRTG.

- Monitoreo de los dispositivos de las instituciones que se encuentran conectadas dentro de la RCE.

- Generación de ticket para notificar a la entidad y/u organismo afectado, ante la identificación de cualquier eventualidad sucedida con los dispositivos y sitios que se encuentran dentro del alcance de monitoreo de CSIRT.

[5] RCE significa Red de Conectividad del Estado

3. Tipos de Tickets

En la siguiente tabla se expone las categorías, o tipos de tickets, que son generados por el equipo CSIRT. La información se presenta ordenada, de mayor a menor, respecto a la cantidad de tickets que se generó por cada tipología. Los cuales se agrupan según la matriz de clasificación de incidentes de ENISA, (Agencia de la Unión Europea para la Ciberseguridad) en 10 categorías relacionadas a incidentes de seguridad informática y acciones preventivas y operacionales, programadas de las instituciones que resultan en la interrupción parcial de un servicio. Más abajo se muestra un gráfico que refleja esta misma información, pero como una distribución en términos porcentuales de lo que representa la participación de cada tipo de ticket dentro del total de la demanda de trabajo que recibe y procesa CSIRT.

N°	Tipos de ticket	Código	Total
1	Vulnerabilidad	9V00	1326
2	Disponibilidad	6D00	330
5	Intentos de Intrusión	4I00	238
6	Operaciones Ciberseguridad CSIRT	19OC	204
4	Fraude	8F00	99
3	Información de seguridad de contenidos	7S00	88
9	Recopilación de Información	3R00	85
8	Código Malicioso	2C00	24
10	Contenido Abusivo	1A00	20
7	Intrusión	5I00	15
	Total		2429

Tabla 1 - Total Tipos de Tickets

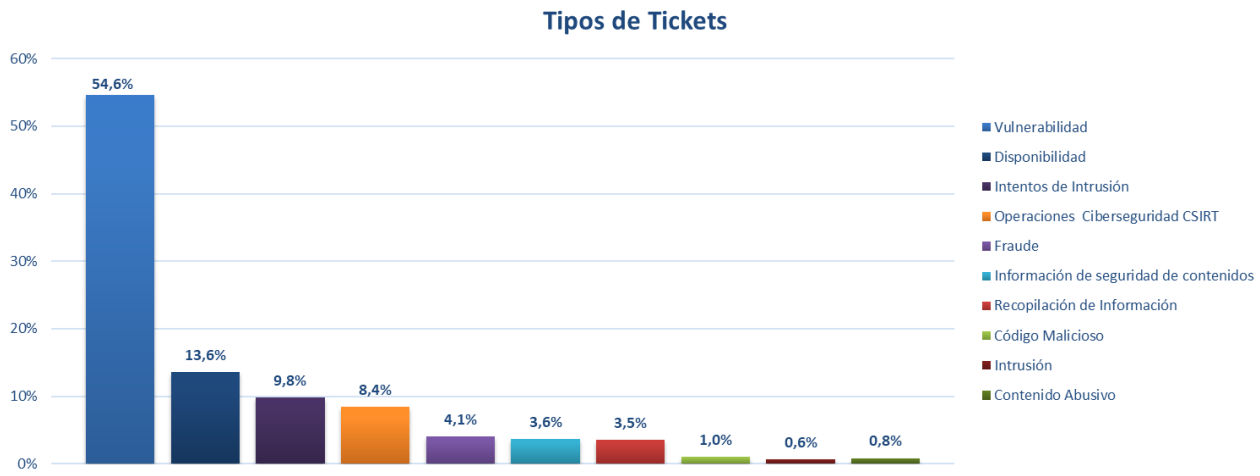


Ilustración 1 - Tipos de tickets

En la siguiente tabla se muestran la tendencia y los cambios en el ranking que experimentan los tipos de tickets generados por CSIRT en el mes de mayo, respecto a abril de 2021.

Como se aprecia en la tabla, los tickets de las categorías de, información de seguridad de contenidos, recopilación de información, código malicioso, contenido abusivo e intrusión decrecen en su tendencia (hay menos números de tickets), mientras que las restantes cinco categorías experimentan una tendencia creciente al comparar el mes de mayo con el pasado mes de abril.

	Abril	Mayo	Tendencia	Variante
1	Vulnerabilidad	Vulnerabilidad	▲	➡
2	Recopilación de Información	Disponibilidad	▲	⬆
3	Información de seguridad de contenidos	Intentos de Intrusión	▲	⬆
4	Operaciones Ciberseguridad CSIRT	Operaciones Ciberseguridad CSIRT	▲	➡
5	Fraude	Fraude	▲	➡
6	Código Malicioso	Información de seguridad de contenidos	▼	⬇
7	Contenido Abusivo	Recopilación de Información	▼	⬇
8	Intrusión	Código Malicioso	▼	⬇
9	Intentos de Intrusión	Contenido Abusivo	▼	⬇
10	Disponibilidad	Intrusión	▼	⬇

Tabla 2 - Ranking de Alertas Recibidas

4. Tipos de Ticket Públicos y Privados

En la siguiente tabla se presenta el desagregado de los tickets que fueron reportados a instituciones públicas o privadas, por las distintas categorías presentadas.

Tickets	Privado	Público	Total
Vulnerabilidad	15	1311	1326
Disponibilidad	17	313	330
Intentos de Intrusión	58	180	238
Operaciones Ciberseguridad CSIRT	8	196	204
Fraude	85	14	99
Información de seguridad de contenidos	67	21	88
Recopilación de Información	20	65	85
Código Malicioso	5	19	24
Contenido Abusivo	8	12	20
Intrusión	0	15	15
Total	283	2146	2429

Tabla 3 - Tickets a Instituciones Públicas y Privadas

En el siguiente gráfico expone el porcentaje de participación que tiene cada destino de los tickets que son enviados a instituciones públicas o privadas.

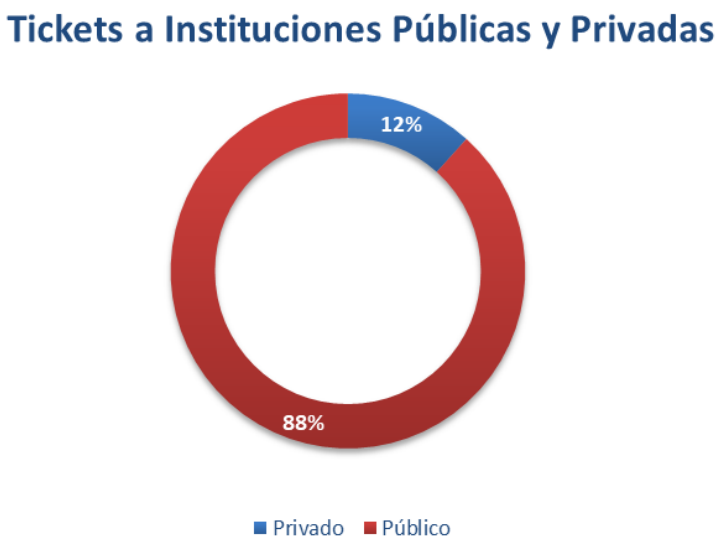


Ilustración 2–- Tickets a Instituciones Públicas y Privadas

5. Estado de Ticket Procesados en el Presente Mes

En la siguiente tabla y gráfico de distribución se muestra el estado de los tickets procesados en el mes de mayo de 2021. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 2.429 unidades. De este total, 624 tickets fueron cerrados exitosamente, lo que representa un 26% de eficacia, mientras que 1813 tickets 74% siguen en desarrollo para terminar de ser procesados en el período siguiente.

Total estado Ticket	Total
En desarrollo	1813
Cerrados	624
Total general	2429

Tabla 4 - Total Estado de Ticket

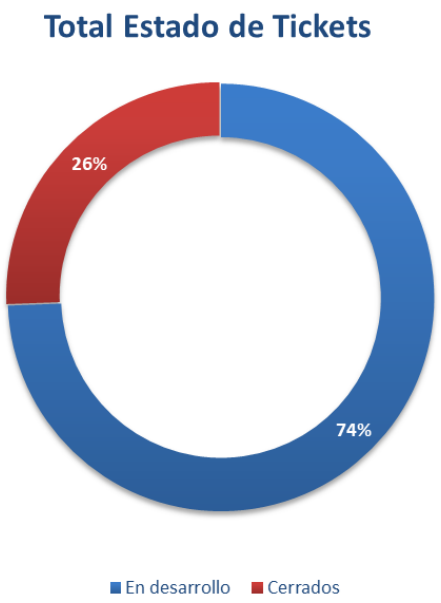


Ilustración 3 - Total Estado de Tickets

6. Procedencia de Generación de Tickets

En la siguiente tabla se presenta la composición -del origen de los tickets- que procesó CSIRT para el desarrollo de su labor durante el mes de mayo de 2021.

Como se aprecia en la tabla, los tickets se pueden originar tanto interna como externamente.

Los tickets de origen internos son todos aquellos que fueron generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante el software que utiliza CSIRT -que también considera los sensores que dan aviso o reportan- desde otros servicios públicos o de las FF.AA.

Por otro lado, los tickets de origen externo son todos aquellos que provienen de proveedores vinculados a CSIRT vía contractual o que se generan a través de call center, por formulario web, por medio de otros CSIRT internacionales, o por correos electrónicos de empresas privadas.

Tipo de Fuente	Cantidad de Tickets
Servicios Internos	2075
Servicios Externos	354
Total Fuentes de Tickets	2429

Tabla 5 - Fuentes de Servicios (Interna y/o Externa)

Como se puede observar en el siguiente gráfico, un 88% de la demanda de trabajo que recibió CSIRT en el pasado mes de mayo tiene un origen interno, mientras que el 12% restante proviene de fuentes externas.

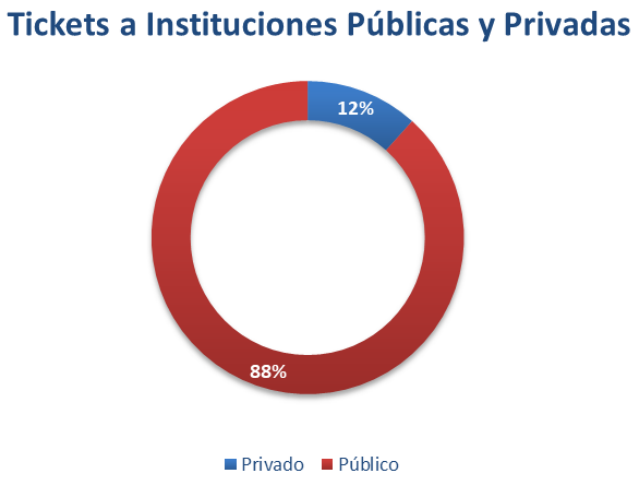


Ilustración 4- Distribución Porcentual de Origen de Tickets

7. Fuentes de Origen Externo de Tickets

En la siguiente tabla se presenta información que da cuenta de las fuentes externas que dieron origen a tickets de esa procedencia durante mayo de 2021.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Tickets generados por información entregada por empresas privadas sin convenio de ciberseguridad	317
Tickets generados por información entregada por empresas privadas con convenio de ciberseguridad	0
Tickets generados por privados vía formulario web	25
Tickets generados por privados vía email	0
Tickets generados por privados vía call center	2
Tickets generados por información de otros CSIRT internacionales	10
Total	**354**

Tabla 6 - Fuentes de Origen Externo de Tickets

El siguiente gráfico de distribución muestra que en mayo de 2021 el porcentaje mayor de tickets externos son generados por reportes entregados por "Empresas privadas sin convenio de ciberseguridad CSIRT", con un 89,5% de participación. En segundo lugar, se ubican aquellos tickets que provienen de "de privados vía formulario web" con un 7,1% de contribución.

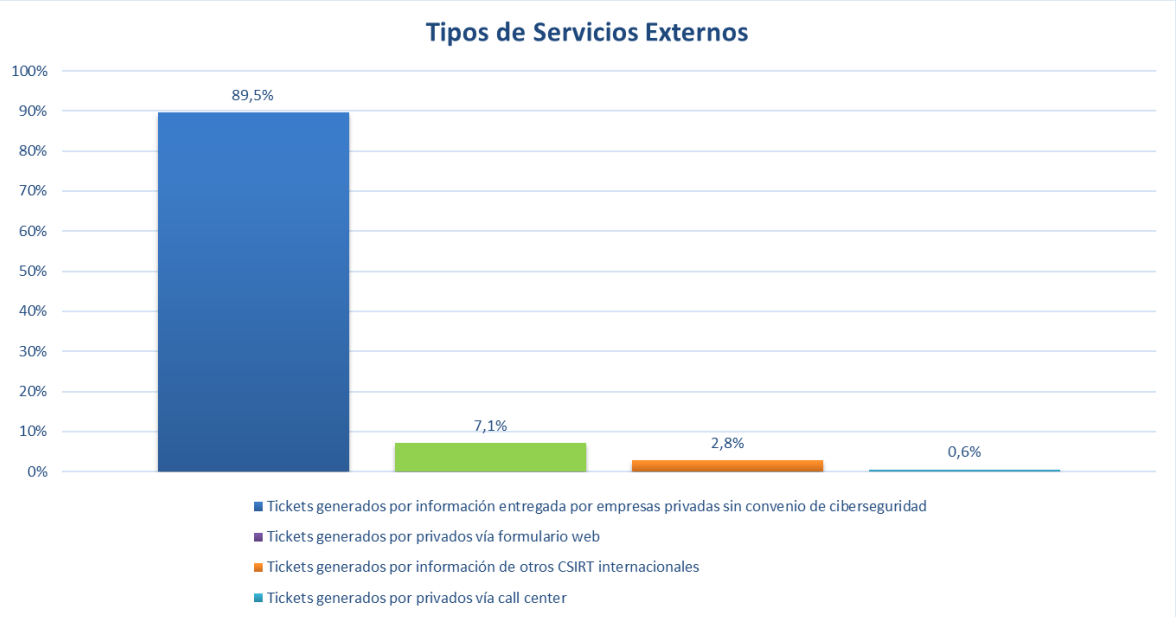
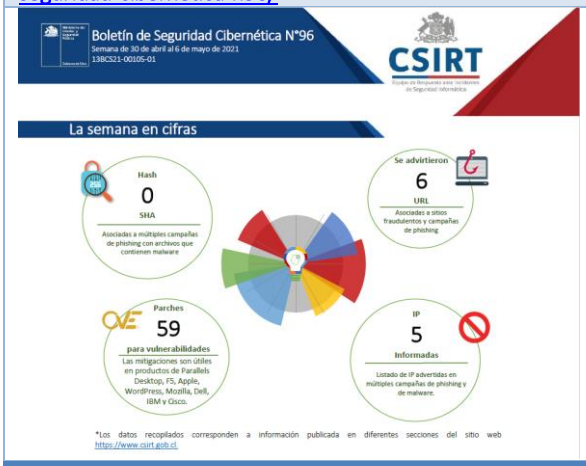
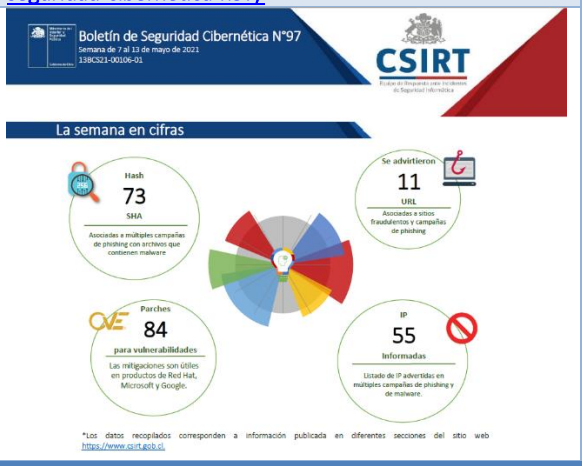
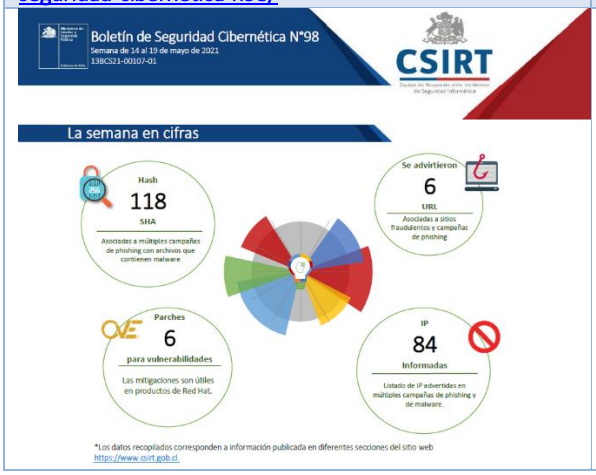
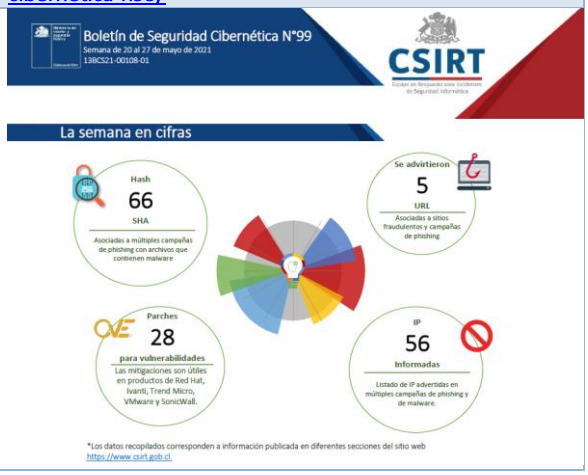


Ilustración 5- Tipos de servicios externos

8. Boletines con resúmenes de alertas y vulnerabilidades del mes

Los enlaces que se comparten a continuación, corresponden a los boletines semanales publicados durante el mes de mayo que contienen el resumen de actividades realizadas por el CSIRT y que fueron publicadas en el sitio web www.csirt.gob.cl.

Boletín de Seguridad Cibernética n°96	Boletín de Seguridad Cibernética n°97
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n96/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n97/
	
Boletín de Seguridad Cibernética n°98	**Boletín de Seguridad Cibernética n°99**
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n98/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n99/
	

9. Síntesis de gestión sobre concientización y buenas prácticas

Los enlaces que se comparten a continuación, corresponden a campaña de concientización y buenas prácticas publicadas por CSIRT durante el mes de mayo y que están disponibles en el sitio web https://www.csirt.gob.cl/recomendaciones/

Ciberconsejos para no caer en estafas en este nuevo retiro de tu 10%	Ciberguía | Fake news: los peligros de la desinformación
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-no-caer-en-estafas-en-este-nuevo-retiro-de-tu-10/	https://www.csirt.gob.cl/recomendaciones/ciberguia-fake-news-los-peligros-de-la-desinformacion/
	

Ciberconsejos para evitar los peligros del Smishing	Ciberconsejos | Qué son las Amenazas Persistentes Avanzadas y cómo protegernos
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-evitar-los-peligros-del-smishing/	https://www.csirt.gob.cl/recomendaciones/ciberconsejos-que-son-las-amenazas-persistentes-avanzadas-y-como-protegernos/
	

Ciberconsejos para comprar seguro este CyberDay 2021	CiberSucesos No. 10 | Nuestra vida en la nube
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-comprar-seguro-este-cyberday-2021/	https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-10-nuestra-vida-en-la-nube/
	

Actualidad

CSIRT de Gobierno organiza la primera conferencia 8.8 vertical gobierno

El jueves 13 de mayo tuvo lugar la primera conferencia 8.8 dedicada al trabajo de ciberseguridad y ciberinteligencia de los gobiernos e instituciones de carácter nacional. Hecha de forma virtual, contó con invitados de Latinoamérica, Israel, España y Estonia, y logró reunir a más de mil espectadores. La conferencia fue abierta por el Ministro del Interior y Seguridad Pública, Rodrigo Delgado, mientras que el cierre del evento estuvo a cargo del Subsecretario del Interior, Juan Francisco Galli.

Los detalles en: https://www.csirt.gob.cl/noticias/exitosa-primera-edicion-de-8-8-gobierno-reune-gran-audiencia-gracias-a-sus-importantes-expertos-internacionales/.

CSIRT de Gobierno denuncia sitio de notaría falsa para que sea dado de baja

El 26 de mayo, el CSIRT de Gobierno denunció al sitio web notariavaleriabarros[.]cl como falso ante el Ministerio de Justicia y Derechos Humanos, el Poder Judicial y NIC Chile, con el objetivo de dar de baja el dominio de internet que esta página web utiliza en ".cl" y que fueran identificados los responsables de los delitos cometidos, para que se les aplique todo el rigor de la ley.

Como resultado, el sitio fue suspendido, el Ministerio de Justicia instruyó a la Corte de Apelaciones para que fiscalizara la situación, y existen demandas contra quienes establecieron esta falsa notaría y realizaron delitos con ella.

La noticia completa, aquí: https://www.csirt.gob.cl/noticias/csirt-de-gobierno-denuncia-sitio-de-notaria-falsa-para-que-sea-dado-de-baja/.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.01 17:26:20 -04'00'