Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

01 de abril 2021

Índice

Índice de Ilustraciones

Índice de Tablas

1. Resumen Ejecutivo

El presente informe contiene un resumen de la totalidad de los tickets procesados en el mes de marzo 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 marzo 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	1402
2	Operaciones Ciberseguridad CSIRT	19OC	173
3	Recopilación de Información	3R00	132
4	Código Malicioso	2C00	79
5	Información de seguridad de contenidos	7S00	77
6	Fraude	8F00	40
7	Intrusión	5I00	23
8	Contenido Abusivo	1A00	23
9	Disponibilidad	6D00	5
10	Intentos de Intrusión	4I00	7
	Total		1.961

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 marzo, respecto a febrero de 2020.

Como se aprecia en la tabla, los tickets de las categorías de, recopilación de información, código malicioso, contenido abusivo y disponibilidad decrecen en su tendencia (hay menos números de tickets), mientras que las restantes seis categorías experimentan una tendencia creciente al comparar el mes de marzo con el pasado mes de febrero.

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

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.

Ticket	Privado	Público	Total
Vulnerabilidad	48	1354	1402
Operaciones Ciberseguridad CSIRT	101	72	173
Recopilación de Información	12	120	132
Código Malicioso	38	41	79
Información de seguridad de contenidos	66	11	77
Fraude	28	12	40
Intrusión	2	21	23
Contenido Abusivo	2	21	23
Disponibilidad	0	5	5
Intentos de Intrusión	2	5	7
Total	**299**	**1662**	**1961**

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.

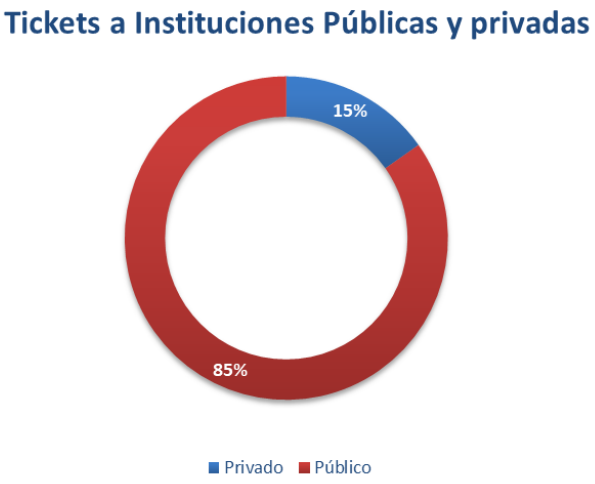


Ilustración 2–- Tickets a Instituciones Públicas y Privadas

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 marzo de 2021. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 1.961 unidades. De este total, 866 tickets fueron cerrados exitosamente, lo que representa un 44% de eficacia, mientras que 1.095 tickets 56% siguen en desarrollo para terminar de ser procesados en el período siguiente.

Total estado Ticket	Total
En desarrollo	1.095
Cerrados	866
Total general	1.961

Tabla 4 - Total Estado de Ticket

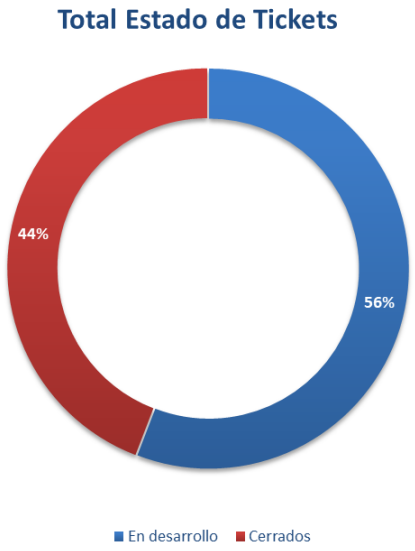


Ilustración 3 - Total Estado de Tickets

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 marzo 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	1699
Servicios Externos	262
Total Fuentes de Tickets	1.961

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

Como se puede observar en el siguiente gráfico, un 87% de la demanda de trabajo que recibió CSIRT en el pasado mes de marzo tiene un origen interno, mientras que el 13% restante proviene de fuentes externas.

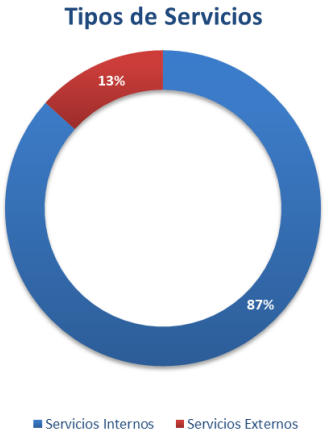


Ilustración 4- Distribución Porcentual de Origen de Tickets

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 marzo de 2021.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Tickets generados por información entregada por empresas privadas sin convenio de ciberseguridad	160
Tickets generados por información entregada por empresas privadas con convenio de ciberseguridad	0
Tickets generados por privados vía formulario web	102
Tickets generados por privados vía email	0
Tickets generados por privados vía call center	0
Tickets generados por información de otros CSIRT internacionales	0
Total	**262**

Tabla 6 - Fuentes de Origen Externo de Tickets

El siguiente gráfico de distribución muestra que en marzo de 2021 el porcentaje mayor de tickets externos son generados por reportes entregados por "Empresas privadas sin convenio de ciberseguridad CSIRT", con un 61% de participación. En segundo lugar, se ubican aquellos tickets que provienen de "de privados vía formulario web" con un 39% de contribución.

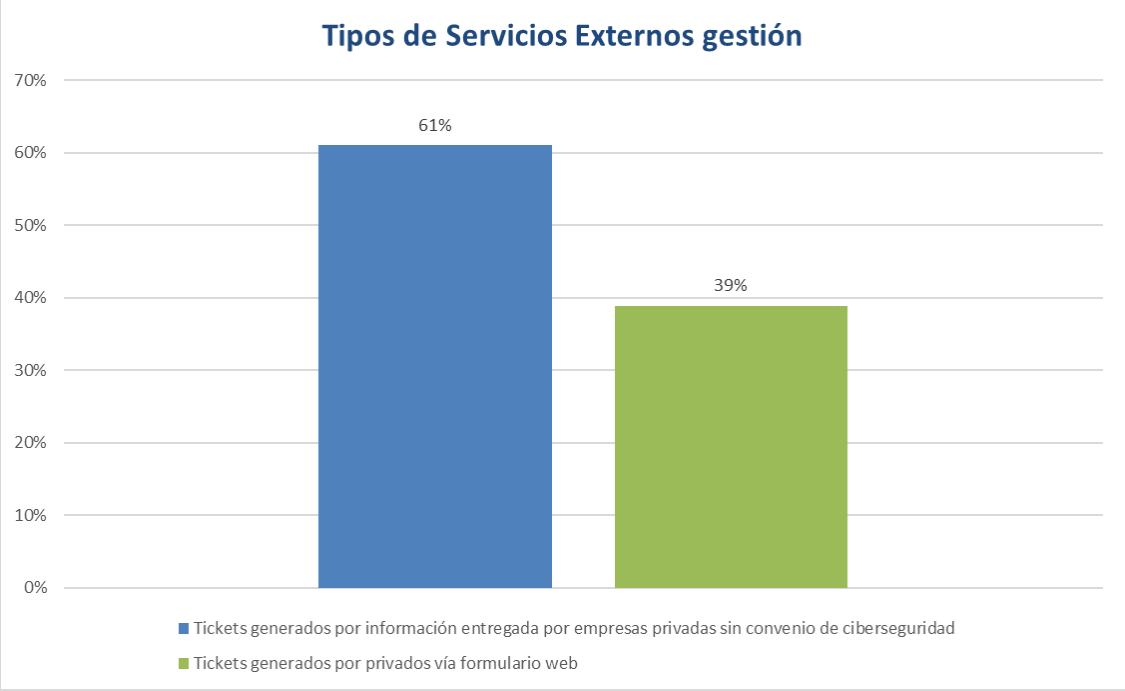
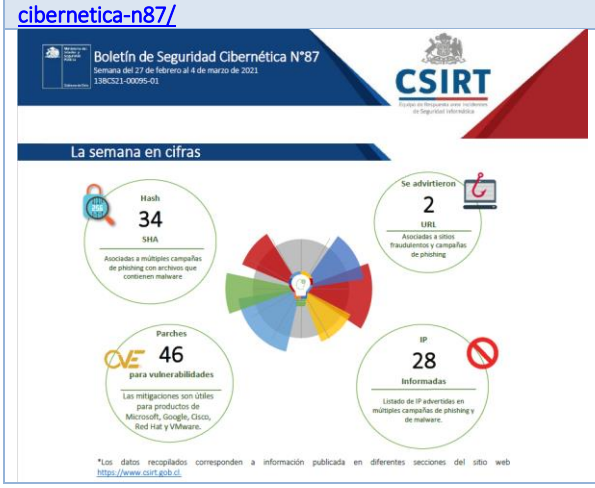
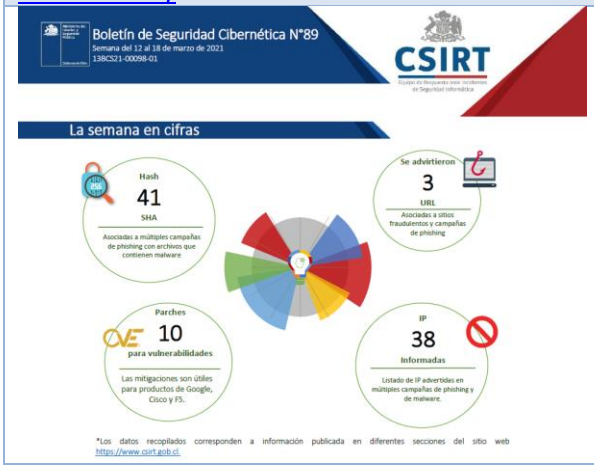
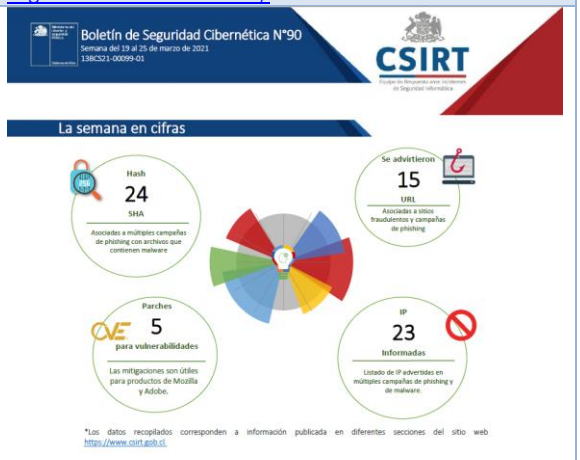


Ilustración 5- Tipos de servicios externos

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 marzo 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°87	Boletín de Seguridad Cibernética n°88
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n87/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n88/
	

Boletín de Seguridad Cibernética n°89	Boletín de Seguridad Cibernética n°90
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n89/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n90/
	

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 marzo y que están disponibles en el sitio web https://www.csirt.gob.cl/recomendaciones/

Ciberconsejos para una conexión segura a las clases virtuales	Ciberconsejos para estar más protegidas en el mundo virtual
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-una-conexion-segura-a-las-clases-virtuales/	https://www.csirt.gob.cl/recomendaciones/dia-internacional-de-la-mujer/
	

Ciberguía de Denuncia del Acoso Digital	Cibersucesos no. 8
https://www.csirt.gob.cl/recomendaciones/ciberguia-acoso-digital/	https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-8/
	

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 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.

Los detalles en: https://www.csirt.gob.cl/noticias/suseso-publica-normativa-en-materia-de-ciberseguridad-desarrollada-junto-al-csirt-de-gobierno/.

❖ 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/.

❖ Director nacional participa en artículo de La Tercera sobre vulnerabilidad en MS Exchange


Secciones LA TERCERA SUSCRÍBETE Inicio de sesión

PULSO Ciberseguridad CMF

Alertas, protocolos y casos internacionales: cómo fue el incidente de ciberseguridad que sufrió la CMF

A inicios de mes el CSIRT había advertido sobre esta vulnerabilidad que requería parches para ser subsanada. La banca también lo tenía en el radar y había parchado sus sistemas con anterioridad. El sábado la industria se enteró oficialmente de la brecha que estaba afectando a la autoridad, por lo que se encendieron las alarmas. Fue el mismo que afectó a la Autoridad Bancaria Europea y al parlamento de Noruega.

El director nacional del CSIRT de Gobierno, Carlos Landeros, fue entrevistado por Mariana Marusic de La Tercera, instancia en la que explicó que el incidente anunciado por la CMF el domingo 14 de marzo correspondió, tal como a los ataques sufridos por el Parlamento de Noruega y la Autoridad Bancaria Europea, a servidores de correos comprometidos por vulnerabilidades de Microsoft Exchange.

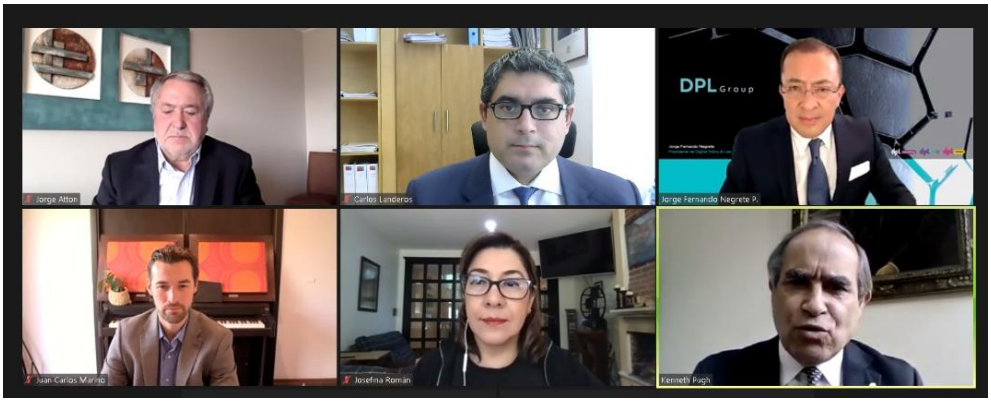
Nuestro director también detalló que el ingreso no autorizado sufrido por la CMF aprovecha la vulnerabilidad de Microsoft Exchange, para hacerse pasar por alguien que tiene acceso autorizado al sistema, y que la CMF no es un blanco particular de esta campaña de ataques, sino que estos están afectando a diversas instituciones en todo el mundo, solo basta que tengan servidores de Exchange vulnerables.

La noticia completa, aquí: Alertas, protocolos y casos internacionales: cómo fue el incidente de ciberseguridad que sufrió la CMF - La Tercera.

❖ Director nacional participa en la importante conferencia “Chile 5G”

El día 30 de marzo e inaugurado por el Presidente de la República, Sebastian Piñera, se llevó a cabo la importante conferencia Chile 5G la cual es organizada por el Ministerio de Transporte y Telecomunicaciones de Chile, a través de la Subsecretaría de Telecomunicaciones, el Observatorio Regional de Banda Ancha de la Comisión Económica para América Latina y el Caribe (CEPAL) y DPL Live, con el objetivo de generar un diagnóstico del entorno económico y normativo, además de compartir las mejores ideas digitales, prácticas y acciones regulatorias y de política pública que permitan iniciar el despliegue de 5G.

La participación de Carlos Landeros, estuvo enfocada en entregar una visión de datos personales y ciberseguridad en el ecosistema 5G, además de compartir las mejores prácticas y acciones regulatorias y de política pública en la materia.



❖ CSIRT de Gobierno imparte charla de ciberseguridad a miembros de la FACH

Miembros del CSIRT de Gobierno, encabezados por nuestro director nacional Carlos Landeros, realizaron charlas de ciberseguridad a alumnos de la cátedra de Inteligencia de la Academia de Guerra Aérea de la Fuerza Aérea de Chile, revisando diversos temas técnicos y normativos y generando una ronda de preguntas y respuestas con los alumnos.

Estas iniciativas refuerzan la importancia de la colaboración entre distintas organizaciones y empresas para lograr entre todos tener un país más ciberseguro.

Los detalles pueden encontrarse aquí: https://www.csirt.gob.cl/noticias/csirt-fach/