Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe de gestión de Seguridad Cibernética

01 de julio 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 junio 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 junio 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 -4.200 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	870
2	Disponibilidad	6D00	369
3	Fraude	8F00	136
4	Información de seguridad de contenidos	7S00	125
5	Otros	11O00	59
6	Código Malicioso	2C00	24
8	Recopilación de Información	3R00	8
9	Contenido Abusivo	1A00	2
10	Intentos de Intrusión	4I00	0
11	Intrusión	5I00	0
Total			**1593**

Tabla 1 - Total Tipos de Tickets

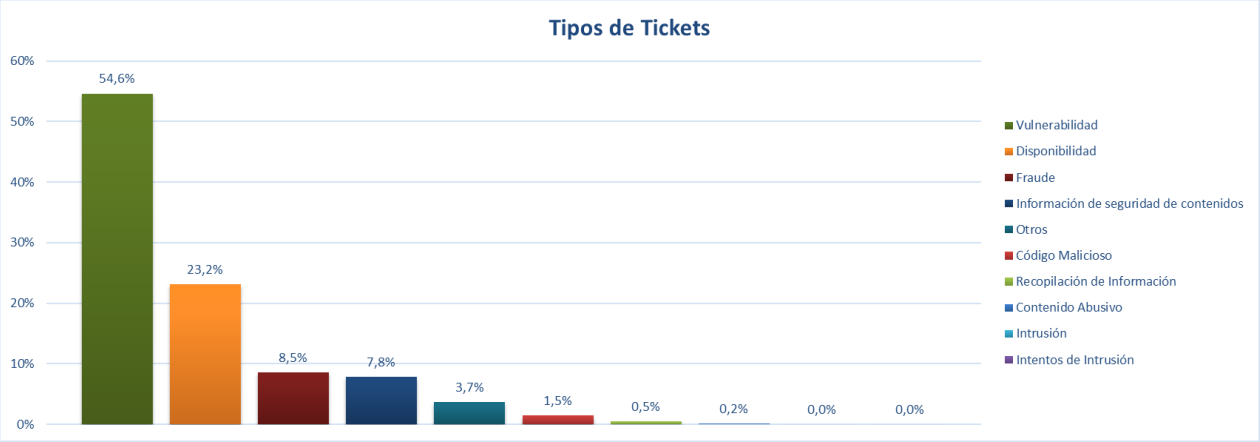


Ilustración 1 - Tipos de tickets

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 junio, respecto a mayo de 2021.

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

N°	Mayo	Junio	Tendencia	Variante
1	Vulnerabilidad	Vulnerabilidad	▼	➡
2	Disponibilidad	Disponibilidad	▲	➡
3	Intentos de Intrusión	Fraude	▲	⬆
4	Operaciones Ciberseguridad CSIRT	Información de seguridad de contenidos	▲	⬆
5	Fraude	Otros	▲	⬆
6	Información de seguridad de contenidos	Código Malicioso	➡	⬆
7	Recopilación de Información	Recopilación de Información	▼	➡
8	Código Malicioso	Contenido Abusivo	▼	⬆
9	Contenido Abusivo	Intentos de Intrusión	▼	⬇
10	Intrusión	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	12	858	870
Disponibilidad	12	357	369
Fraude	44	92	136
Información de seguridad de contenidos	96	29	125
Otros	5	54	59
Código Malicioso	21	3	24
Recopilación de Información	1	7	8
Contenido Abusivo	0	2	2
Intentos de Intrusión	0	0	0
Intrusión	0	0	0
Total	**191**	**1402**	**1593**

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.

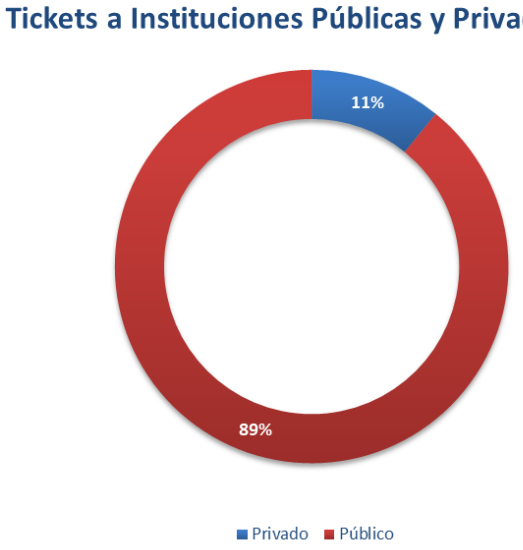


Ilustración 2–- Tickets a Instituciones Públicas y Privadas

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 junio de 2021. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 1.593 unidades. De este total, 560 tickets fueron cerrados exitosamente, lo que representa un 35% de eficacia, mientras que 1.033 tickets 65% siguen en desarrollo para terminar de ser procesados en el período siguiente.

Total estado Ticket	Total
En desarrollo	1033
Cerrados	560
Total general	**1593**

Tabla 4 - Total Estado de Ticket

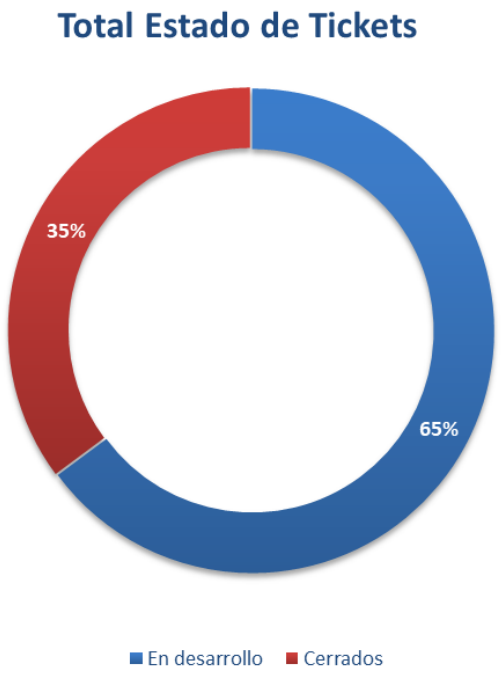


Ilustración 3 - Total Estado de Tickets

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 junio 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	1437
Servicios Externos	156
Total Fuentes de Tickets	**1593**

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

Como se puede observar en el siguiente gráfico, un 90% de la demanda de trabajo que recibió CSIRT en el pasado mes de junio tiene un origen interno, mientras que el 10% restante proviene de fuentes externas.

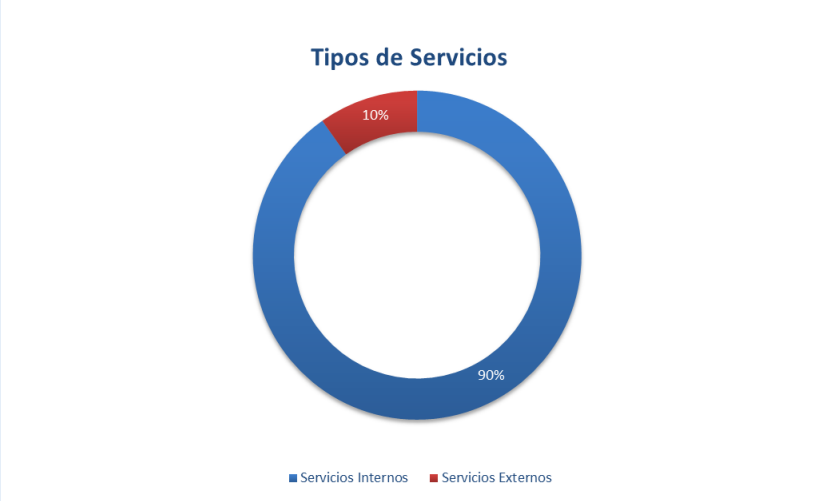


Ilustración 4- Distribución Porcentual de Origen de Tickets

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 junio de 2021.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Generados por información entregada por empresas privadas sin convenio de ciberseguridad	7
Generados por información entregada por empresas privadas con convenio de ciberseguridad	0
Generados por privados vía formulario web	114
Generados por privados vía email	33
Generados por privados vía call center	2
Generados por información de otros CSIRT internacionales	0
Total	**156**

Tabla 6 - Fuentes de Origen Externo de Tickets

El siguiente gráfico de distribución muestra que en junio de 2021 el porcentaje mayor de tickets externos son generados por aquellos tickets que provienen de “de privados vía formulario web”, con un 73% de participación. En segundo lugar, se ubican aquellos tickets que provienen de “de privados vía email” con un 22,2% de contribución.

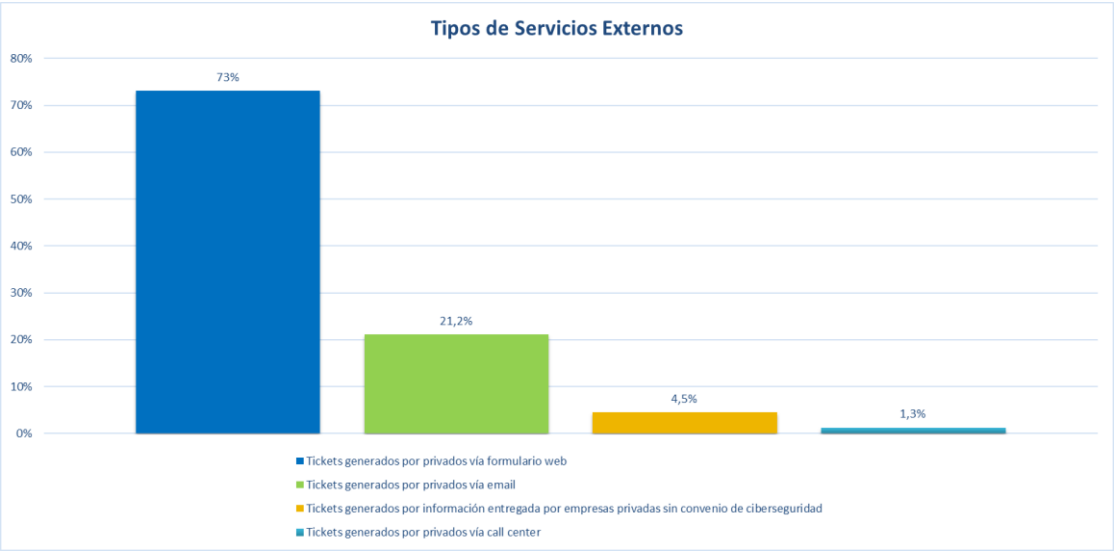
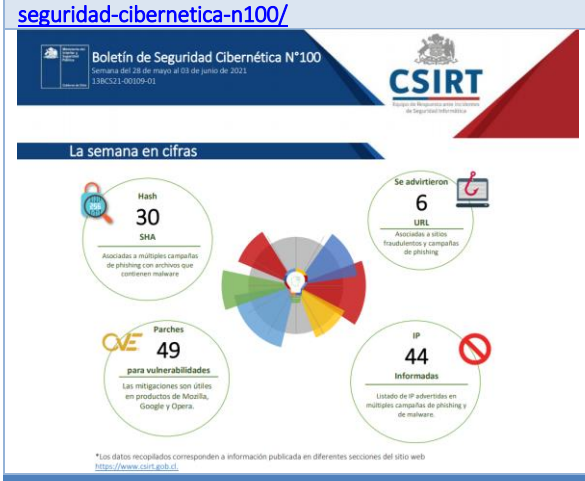
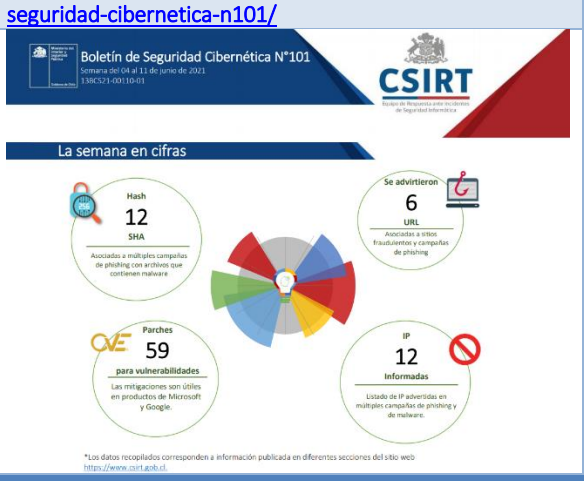
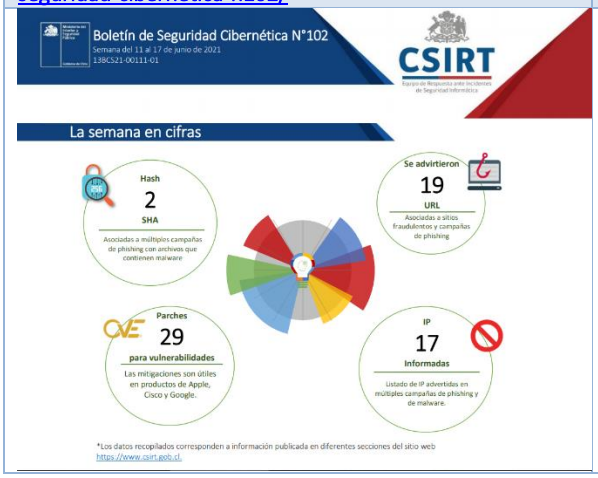
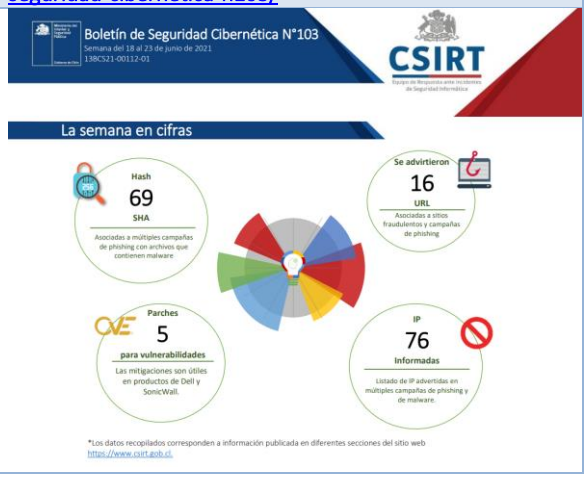


Ilustración 5- Tipos de servicios externo

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 junio 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°100	Boletín de Seguridad Cibernética n°101
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n100/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n101/
	
Boletín de Seguridad Cibernética n°102	**Boletín de Seguridad Cibernética n°103**
https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n102/	https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n103/
	

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

Ciberconsejos | Qué es el SIM Swapping y qué hacer si se es víctima	Ciberguía | Medidas preventivas de conductas abusivas en RR.SS.
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-que-es-el-sim-swapping-y-que-hacer-si-se-es-victima/	https://www.csirt.gob.cl/recomendaciones/ciberguia-medidas-preventivas-de-conductas-abusivas-en-rrss/
	
Ciberconsejos | Cómo evitar que tu hijo sea víctima del grooming	**CiberSucesos No. 11 | Secuestro de WhatsApp y SIM Swapping**
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-como-evitar-que-tu-hijo-sea-victima-del-grooming/	https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-11-secuestro-de-whatsapp-y-sim-swapping/
	

10. Actualidad

Presidente Piñera anuncia proyecto de ley que crea la Agencia Nacional de Ciberseguridad

El Presidente Piñera anunció durante su Cuenta Pública la ampliación de la agenda de Seguridad Pública del Gobierno al mundo digital, **anunciando la creación de la Agencia Nacional de Ciberseguridad, proyecto desarrollado en conjunto con el CSIRT de Gobierno**, dependiente de la Subsecretaría del Interior.

"Esta agencia será el órgano que entregue seguridad a los chilenos en el ciberespacio, que proteja los bienes y activos de la sociedad digital, y que se coordine con el sector privado de manera permanente para garantizar la seguridad de los ciudadanos en el ciberespacio", indica el Subsecretario del Interior, Juan Francisco Galli, "ya que no podemos olvidar que en los sectores productivos privados se concentran la mayor cantidad de las iniciativas digitales, que constituyen las nuevas infraestructuras críticas informáticas de la cuarta revolución industrial", agrega.

Los detalles en: https://www.csirt.gob.cl/noticias/presidente-pinera-anuncia-proyecto-de-ley-que-crea-la-agencia-nacional-de-ciberseguridad/.

Chile avanza nueve puestos a nivel mundial y dos en América en ranking global de ciberseguridad de la ONU


MIÉRCOLES 30.06.2021

Las altas expectativas de restaurantes y bares en su reapertura

A LA CALLE ORREGO LUCO

LT LATERCERA PULSO 30JUN21

Ranking de ciberseguridad de la ONU: Chile sube nueve puestos y queda 74 a nivel mundial

Conexiones de fibra óptica a internet fija se disparan en el primer trimestre por pandemia

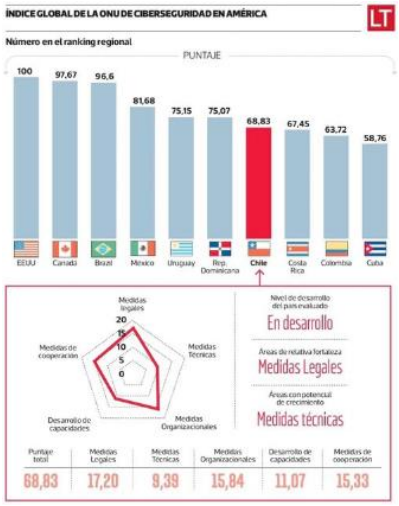
Sectores comercio y silvoagropecuario tienen dificultad para encontrar trabajadores

En la cuarta edición del prestigioso ranking de ciberseguridad mundial Global Cybersecurity Index, desarrollado por la Unión Internacional de Telecomunicaciones (ITU, agencia de las Naciones Unidas especializada en la coordinación de las telecomunicaciones a nivel global), el cual refleja los avances logrados en materia de ciberseguridad por los 194 estados miembros y presentado hoy, **Chile subió nueve lugares a nivel mundial, llegando al puesto 74, y dos en términos del continente americano, ubicándose séptimo en la región**.

El Subsecretario del Interior, Juan Francisco Galli, destaca reconocimiento del avance de nuestro país en la protección del ciberespacio, aunque llama a mantener e intensificar la concientización de la ciudadanía en la adopción de prácticas seguras en internet.

Nuestro puesto en este listado internacional deberá mejorar aún más el próximo año, con la creación de la Agencia Nacional de Ciberseguridad. La noticia completa, pueden leerla en el siguiente enlace:

https://www.csirt.gob.cl/noticias/chile-avanza-nueve-puestos-a-nivel-mundial-y-dos-en-america-en-ranking-global-de-ciberseguridad-de-la-onu/



Este jueves 8 de julio comienza el OEA Cyberwomen Challenge Chile 2021, competencia para mujeres con habilidades en ciberseguridad

Este jueves 8 de julio comienza el OEA Cyberwomen Challenge Chile, competencia de hacking entre equipos conformados solo por mujeres. El evento, organizado desde el año 2018 por el CSIRT de Gobierno del Ministerio del Interior y la Organización de Estados Americanos (OEA) en alianza junto a TrendMicro, se desarrolla en 10 países de Latinoamérica: Colombia, Guatemala, México, Uruguay, Perú, República Dominicana, Argentina, Brasil, Costa Rica y Chile.

El Cyberwomen Challenge nace con el objetivo de potenciar a las mujeres en una industria donde existe una baja tasa de ocupación femenina (en 2020 sólo un 25% de los puestos de trabajo en ciberseguridad a nivel global eran ocupados por mujeres). Para ello, se creó esta instancia anual, donde cientos de mujeres con interés y habilidades en la ciberseguridad puedan conocerse, generar contactos y demostrar sus capacidades.

Gobierno Invita

Ministra de la Mujer y Equidad de Género Mónica Zalaquett: youtube.com/watch?v=UTOJ81bJRd8

Ministro Secretario General de Gobierno Jaime Bellolio: http://youtube.com/watch?v=x2lC8Y2QSzo

Ministro del Interior Rodrigo Delgado: https://www.youtube.com/watch?v=cm9P5esveFI

Subsecretaria de Ciencia Carolina Torrealba: https://www.youtube.com/watch?v=_pX5zVXhF_I

Subsecretario del Interior Juan Francisco Galli: https://www.youtube.com/watch?v=yhfOs0tpnUQ

En nuestro país y desde 2018, ya han participado en el Cyberwomen Challenge más de 300 mujeres de distintas edades y carreras. El evento de Chile, como aquellos en sus pares de la región, es clasificatorio para el OEA Cyberwomen Regional, a realizarse en 2022. La inscripción se realiza en el siguiente sitio web oficial: https://women-challenge.interior.gob.cl

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.02 09:51:05 -04'00'