



Informe de gestión de Seguridad Cibernética

01 de julio 2021



```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```





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
10. Actualidad	13

Índice de Ilustraciones

Ilustración 1 - Tipos de tickets	5
Ilustración 2 - Tickets a Instituciones Públicas y Privadas	7
Ilustración 3- Total Estado de Tickets	8
Ilustración 4- Distribución porcentual de origen de ticket.....	9
Ilustración 5- 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 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 MISP¹ que contiene la cantidad de posibles IoCs² 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 IP³ o a URL⁴.

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 RCE⁵ (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	11000	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

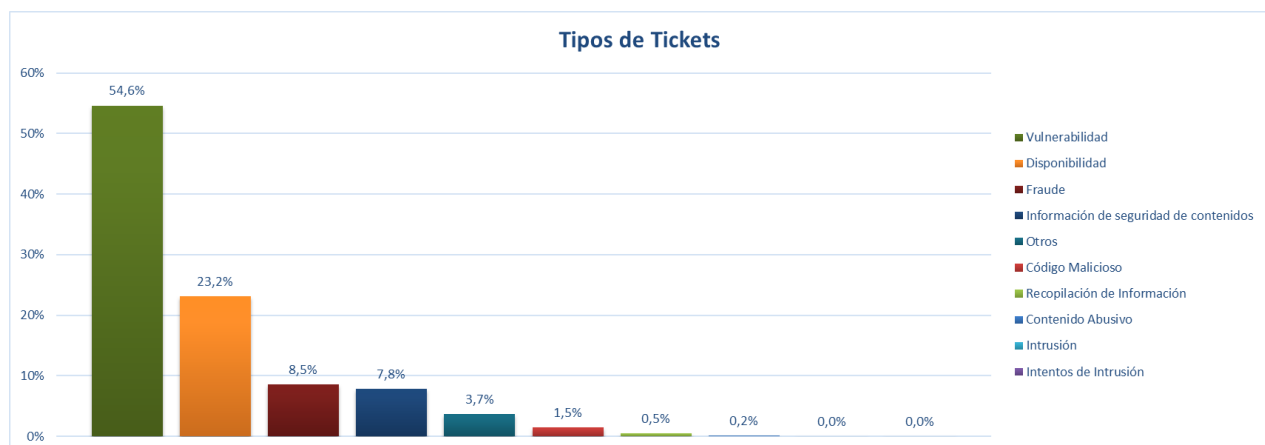


Ilustración 1 - Tipos de tickets



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.

Nº	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 desgregado 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.

Tickets a Instituciones Públicas y Privadas

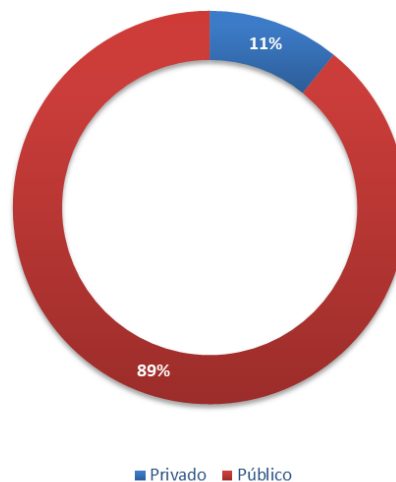


Ilustración 2-- Tickets a Instituciones Públicas y Privadas



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

Total Estado de Tickets

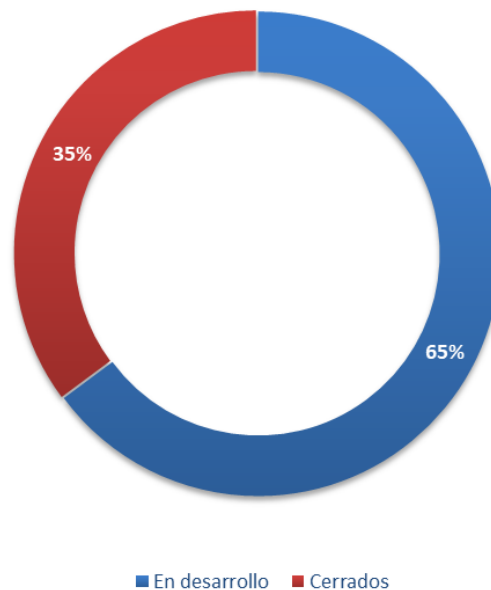


Ilustración 3 - Total Estado de Tickets



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.

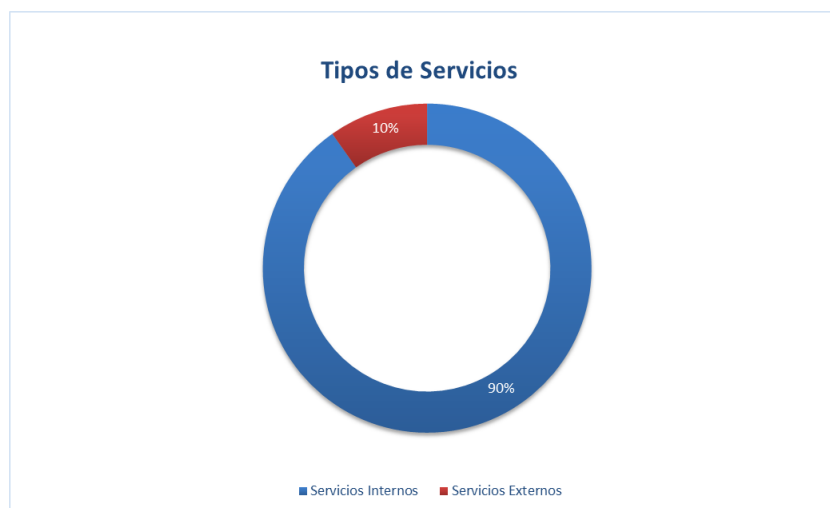


Ilustración 4- Distribución Porcentual de Origen de Tickets



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.

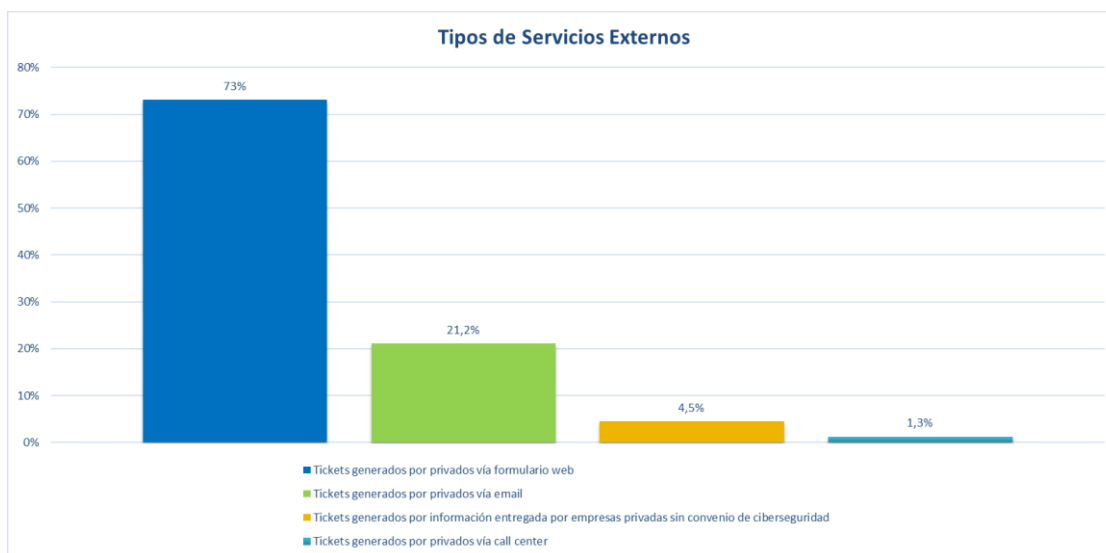


Ilustración 5- Tipos de servicios externo



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.





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.
<p>https://www.csirt.gob.cl/recomendaciones/ciberconsejos-que-es-el-sim-swapping-y-que-hacer-si-se-es-victima/</p>  <p>¿QUÉ ES EL SIM SWAPPING? El SIM Swapping o intercambio de SIM, también llamado robo de SIM o secuestro de SIM, es una forma de robo de identidad en la que un delincuente roba tu número de teléfono móvil asignándolo a una nueva tarjeta SIM. Luego pueden insertar la nueva SIM en un teléfono diferente para acceder a tu cuenta y causar un daño real.</p>	<p>https://www.csirt.gob.cl/recomendaciones/ciberguia-medidas-preventivas-de-conductas-abusivas-en-rrss/</p>  <p>MEDIDAS PREVENTIVAS A CONDUCTAS ABUSIVAS EN RRSS</p>
Ciberconsejos Cómo evitar que tu hijo sea víctima del grooming	CiberSucesos No. 11 Secuestro de WhatsApp y SIM Swapping
<p>https://www.csirt.gob.cl/recomendaciones/ciberconsejos-como-evitar-que-tu-hijo-sea-victima-del-grooming/</p>  <p>CÓMO EVITAR QUE TU HIJO SEA MANIPULADO POR UN ADULTO EN INTERNET Como grooming se conoce a la práctica en la cual un adulto engaña a un niño, generalmente haciéndose pasar por otro menor de edad, para ganarse su confianza, crear lazos emocionales y así abusar sexualmente de ellos u obtener contenido pornográfico.</p> <p>El contacto inicial se suele dar a través de las redes sociales y plataformas de juego online que frecuentan los menores.</p>	<p>https://www.csirt.gob.cl/recomendaciones/cibersucesos-no-11-secuestro-de-whatsapp-y-sim-swapping/</p>  <p>HAN SECUESTRADO MI WHATSAPP PERDÍ MI CELULAR Y NO SALÍ DE MI BOLSILLO: SIM Swapping</p> <p>Cooperación Internacional República Dominicana</p> <p>Tendencias Amenazas a la seguridad móvil: Mi Smartphone Infectado</p> <p>Comunidades Nacionales Unidad Vía de Mar</p> <p>Legal Políticas de privacidad para WhatsApp</p>



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

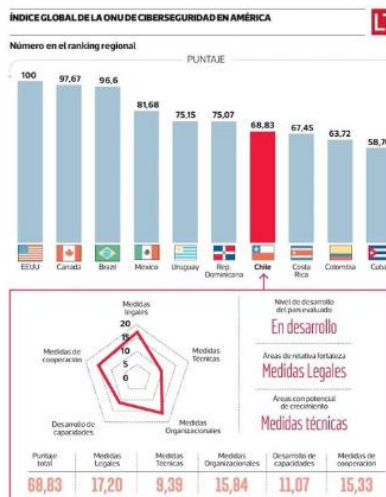


En la cuarta edición del prestigioso ranking de ciberseguridad mundial Global Cybersecurity Index, desarrollado por la Unión Internacional de Telecomunicaciones (ITU, agencia de las Naciones Unidas especializada en la coordinación de las telecomunicaciones a nivel global), el cual refleja los avances 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



TREND MICRO **OEA** **Canada** **Citi Foundation** **CSIRT**

OEA CYBERWOMEN CHALLENGE

4ta edición online 2021

CHILE 2021

ÚLTIMOS CUPOS PARTICIPA

Jueves 8 de julio
08:40 a 17:45

Con el apoyo de **aws** **WOMCY**

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](https://www.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>