



# Informe de gestión de Seguridad Cibernética

02 de noviembre 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 Tickets 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.....	14

## 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 octubre 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 octubre 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.



## 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 mes. 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<sup>1</sup> (falta de cifrado, CMS obsoletos, credenciales recuperadas, servidores desactualizados, puertos expuestos, phishing, defacement, 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 tickets para notificar a la entidad 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.

---

<sup>1</sup> 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 de 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	1158
2	Disponibilidad	6D00	340
3	Información de seguridad de contenidos	7S00	131
4	Otros	11O00	115
5	Fraude	8F00	78
6	Código Malicioso	2C00	21
7	Recopilación de Información	3R00	6
8	Intentos de Intrusión	4I00	2
9	Contenido Abusivo	1A00	1
10	Intrusión	5I00	1
<b>Total</b>			<b>1853</b>

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 octubre, respecto a septiembre de 2021.

Como se aprecia en la tabla, los tickets de las categorías de disponibilidad, Información de seguridad de contenidos, fraude y contenido abusivo presentan una baja (hay menos tickets), mientras que cinco categorías experimentan una tendencia creciente al comparar el mes de septiembre con el pasado mes de octubre.

Nº	Septiembre	Octubre	Tendencia	Variante
1	Vulnerabilidad	Vulnerabilidad	▲	→
2	Disponibilidad	Disponibilidad	▼	→
3	Información de seguridad de contenidos	Información de seguridad de contenidos	▼	→
4	Fraude	Otros	▲	↑
5	Otros	Fraude	▼	↓
6	Código Malicioso	Código Malicioso	▲	→
7	Contenido Abusivo	Recopilación de Información	▲	↑
8	Intrusión	Intentos de Intrusión	▲	↑
9	Recopilación de Información	Contenido Abusivo	▼	↓
10	Intentos de 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	33	1125	1158
Disponibilidad	26	314	340
Información de seguridad de contenidos	112	19	131
Otros	64	51	115
Fraude	69	9	78
Código Malicioso	18	3	21
Recopilación de Información	5	1	6
Intentos de Intrusión	0	2	2
Contenido Abusivo	1	0	1
Intrusión	0	1	1
<b>Total</b>	<b>328</b>	<b>1525</b>	<b>1853</b>

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

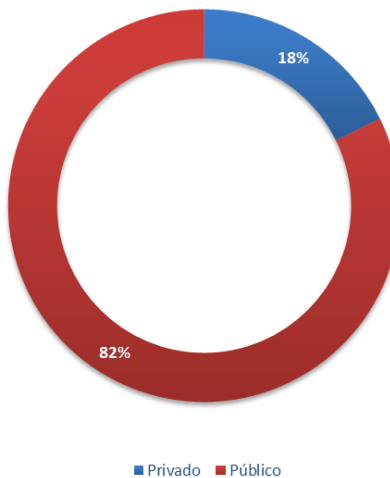


Ilustración 2— Tickets a Instituciones Públicas y Privadas



## 5. Estado de Tickets Procesados en el Presente Mes

En la siguiente tabla y gráfico de distribución se muestra el estado de los tickets procesados en octubre de 2021. Como se puede apreciar la cantidad de tickets abiertos o generados en el período son un total de 1853 unidades. De este total, 1309 tickets fueron cerrados exitosamente, lo que representa un 71% de eficacia, mientras que 544 tickets 29% siguen en desarrollo para terminar de ser procesados en el período siguiente.

Total estado Ticket	Total
En desarrollo	544
Cerrados	1309
<b>Total general</b>	<b>1853</b>

Tabla 4 - Total Estado de Ticket

### Total Estado de Tickets

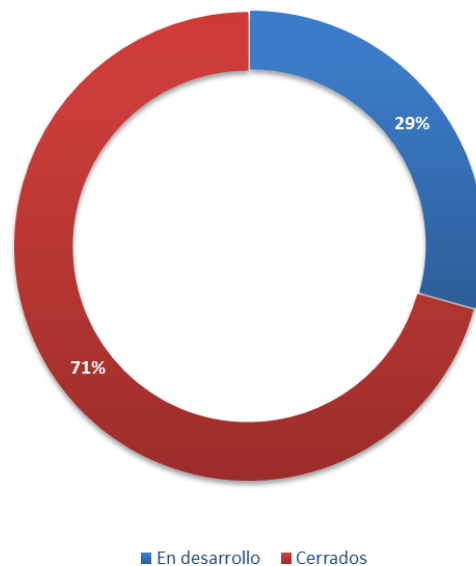


Ilustración 3 - Total Estado de Tickets





## 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 octubre 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	1642
Servicios Externos	211
<b>Total Fuentes de Tickets</b>	<b>1853</b>

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

Como se puede observar en el siguiente gráfico, un 89% de la demanda de trabajo que recibió CSIRT en el pasado mes de octubre tiene un origen interno, mientras que el 11% restante proviene de fuentes externas.

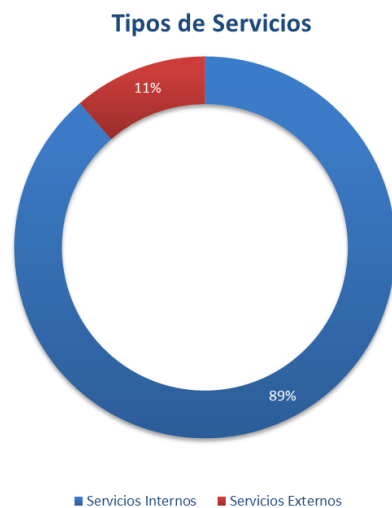


Ilustración 4- Distribución Porcentual de Origen de Tickets



## 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 octubre de 2021.

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Generados vía Formulario web	120
Generados vía Email	39
Generados vía Redes sociales	21
Generados vía Call center	16
Generados vía Internacionales	12
Generados vía Proveedor de servicio	3
<b>Total</b>	<b>211</b>

Tabla 6 - Fuentes de Origen Externo de Tickets

El siguiente gráfico de distribución muestra que en octubre de 2021 el porcentaje mayor de tickets externos son generados por aquellos tickets que provienen de “vía formulario web”, con un 56,9% de participación. En segundo lugar, se ubican aquellos tickets que provienen de “vía email” con un 18,5% de contribución.

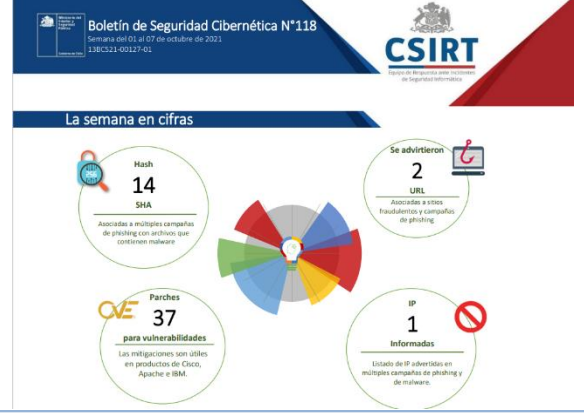



Ilustración 5- Tipos de servicios externo



## 8. Boletines con resúmenes de alertas y vulnerabilidades del mes


Los enlaces que se comparten a continuación corresponden a los boletines semanales publicados durante agosto, los que contienen el resumen de actividades realizadas por el CSIRT de Gobierno y que fueron publicadas en el sitio web [www.csirt.gob.cl](http://www.csirt.gob.cl).

<b>Boletín de Seguridad Cibernética n°118</b> <a href="https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n118/">https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n118/</a>	<b>Boletín de Seguridad Cibernética n°119</b> <a href="https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n119/">https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n119/</a>
 <p><b>Boletín de Seguridad Cibernética N°118</b> Semana del 01 al 07 de octubre de 2021 138CS21-00127-01</p> <p><b>La semana en cifras</b></p> <ul style="list-style-type: none"> <li><b>Hash</b> 14 SHA Asociados a múltiples campañas de phishing con archivos que contienen malware</li> <li><b>Se advirtieron</b> 2 URL Asociadas a sitios fraudulentos y campañas de phishing</li> <li><b>Parches</b> 37 para vulnerabilidades Las mitigaciones son útiles en productos de Cisco, Apache e IBM.</li> <li><b>IP</b> 1 Informadas Estado de IP advertidas en múltiples campañas de phishing y de malware.</li> </ul>	 <p><b>Boletín de Seguridad Cibernética N°119</b> Semana del 08 al 14 de octubre de 2021 138CS21-00128-01</p> <p><b>La semana en cifras</b></p> <ul style="list-style-type: none"> <li><b>Hash</b> 72 SHA Asociados a múltiples campañas de phishing con archivos que contienen malware</li> <li><b>Se advirtieron</b> 1 URL Asociadas a sitios fraudulentos y campañas de phishing</li> <li><b>Parches</b> 114 para vulnerabilidades Las mitigaciones son útiles en productos de Dell, Apple y Microsoft.</li> <li><b>IP</b> 19 Informadas Estado de IP advertidas en múltiples campañas de phishing y de malware.</li> </ul>
<b>Boletín de Seguridad Cibernética n°120</b> <a href="https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n120/">https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n120/</a>	<b>Boletín de Seguridad Cibernética n°121</b> <a href="https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n121/">https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-n121/</a>
 <p><b>Boletín de Seguridad Cibernética N°120</b> Semana del 15 al 21 de octubre de 2021 138CS21-00129-01</p> <p><b>La semana en cifras</b></p> <ul style="list-style-type: none"> <li><b>Hash</b> 14 SHA Asociados a múltiples campañas de phishing con archivos que contienen malware</li> <li><b>Se advirtieron</b> 4 URL Asociadas a sitios fraudulentos y campañas de phishing</li> <li><b>Parches</b> 250 para vulnerabilidades Las mitigaciones son útiles en productos de Google, Oracle y Cisco.</li> <li><b>IP</b> 1 Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware.</li> </ul>	 <p><b>Boletín de Seguridad Cibernética N°121</b> Semana del 22 al 28 de octubre de 2021 138CS21-00130-01</p> <p><b>La semana en cifras</b></p> <ul style="list-style-type: none"> <li><b>Hash</b> 22 SHA Asociados a múltiples campañas de phishing con archivos que contienen malware</li> <li><b>Se advirtieron</b> 10 URL Asociadas a sitios fraudulentos y campañas de phishing y malware.</li> <li><b>Parches</b> 111 para vulnerabilidades Las mitigaciones son útiles en productos de Red Hat, Discourse, Apple y Adobe.</li> <li><b>IP</b> 15 Informadas Listado de IP advertidas en múltiples campañas de phishing y de malware.</li> </ul>



## 9. Síntesis de gestión sobre concientización y buenas prácticas

A continuación, las campañas de concientización y buenas prácticas publicadas por CSIRT de Gobierno durante octubre y disponibles en [csirt.gob.cl/recomendaciones](https://csirt.gob.cl/recomendaciones).

Campaña de ciberconsejos junto a CSIRTAméricas   Semana 1: Navegación Segura	Campaña de ciberconsejos CSIRTAméricas   Semana 2: Niños, Niñas y Adolescentes
<p><a href="https://www.linkedin.com/posts/csirt-gob_mesdelaciberseguridad-csirtamericas-ciberconsejos-activity-6855840753751470081-1ku2">https://www.linkedin.com/posts/csirt-gob_mesdelaciberseguridad-csirtamericas-ciberconsejos-activity-6855840753751470081-1ku2</a></p>	<p><a href="https://www.linkedin.com/posts/csirt-gob_mesdelaciberseguridad-csirtamericas-ciberconsejos-activity-6855840753751470081-1ku2">https://www.linkedin.com/posts/csirt-gob_mesdelaciberseguridad-csirtamericas-ciberconsejos-activity-6855840753751470081-1ku2</a></p>
 <p><b>Cybertips for a new CYBERSECURITY AWARENESS MONTH SAFE INTERNET BROWSING</b></p> <p>To navigate the internet safely, follow these tips:</p> <ul style="list-style-type: none"> <li><b>CLEAR</b> your browser's cache and cookies to limit third-party tracking of what you visit on the internet</li> <li><b>USE</b> incognito mode or private browsing to prevent some websites from tracking your searches and browsing</li> <li><b>AVOID</b> connecting to public wifi, especially to make payments or share personal or financial data</li> </ul> <p>CSIRTAméricas Network</p> <p><b>Ciberconsejos para el MES DE LA CIBERSEGURIDAD NAVEGACIÓN SEGURA</b></p>  <p><b>EVITA</b> acceder a enlaces sospechosos, unos de los medios más utilizados para redirigir a las víctimas a sitios maliciosos son enlaces o hipervínculos</p> <p><b>CIERRA</b> la sesión cuando finalices una actividad en una página web a la que hayas accedido con tus credenciales (usuario y contraseña)</p> <p><b>NUNCA</b> realice descargas de aplicaciones desde páginas que no sean oficiales</p> <p>CSIRTAméricas Network</p>	 <p><b>Ciberconsejos para el MES DE LA CIBERSEGURIDAD NIÑOS, NIÑAS Y ADOLESCENTES</b></p> <ul style="list-style-type: none"> <li><b>HABLA</b> con tus hijos sobre el uso de internet y redes sociales.</li> <li><b>ACUERDA</b> en familia pautas para el uso de la tecnología en casa.</li> <li><b>CUIDA</b> la huella digital de tus hijos y lo que publicas sobre ellos en redes sociales.</li> </ul> <p>CSIRTAméricas Network</p> <p><b>Cybertips for a new CYBERSECURITY AWARENESS MONTH CHILDREN AND ADOLESCENTS</b></p> <p>Practice digital self-care with your young children on the Internet!</p> <ul style="list-style-type: none"> <li><b>TEACH</b> about safe use and risks on the internet.</li> <li><b>ACTIVATE</b> privacy options in social networks.</li> <li><b>AVOID</b> contact with strangers and REPORT in case of being a victim.</li> </ul> <p>CSIRTAméricas Network</p>
<p><b>Ciberconsejos para guiar a las personas mayores en el mundo digital</b></p>	<p><b>Siete Grandes Ciberriesgos para Niños, Niñas y Adolescentes</b></p>
<p><a href="https://csirt.gob.cl/recomendaciones/ciberconsejos-para-guiar-a-las-personas-mayores-en-el-mundo-digital-una-nueva-guia-del-csirt-de-gobierno-para-este-mes-de-la-ciberseguridad/">csirt.gob.cl/recomendaciones/ciberconsejos-para-guiar-a-las-personas-mayores-en-el-mundo-digital-una-nueva-guia-del-csirt-de-gobierno-para-este-mes-de-la-ciberseguridad/</a></p>	<p><a href="https://www.csirt.gob.cl/recomendaciones/siete-grandes-ciberriesgos-nna/">https://www.csirt.gob.cl/recomendaciones/siete-grandes-ciberriesgos-nna/</a></p>
 <p>En el Mes de la Ciberseguridad 2021</p> <p><b>CIBERCONSEJOS PARA GUIAR A LAS PERSONAS MAYORES EN EL MUNDO DIGITAL</b></p> <p>CSIRT</p>	 <p>En el Mes de la Ciberseguridad 2021</p> <p><b>Siete grandes ciberriesgos para Niños, Niñas y Adolescentes</b></p> <p>CSIRT</p>



## Campaña de ciberconsejos junto a CSIRT Americas | Semana 3: PYMES

[https://www.linkedin.com/posts/csirt-gob\\_mesdelaciberseguridad-csirtamericas-ciberconsejos-activity-6858402129074278400-Td6H](https://www.linkedin.com/posts/csirt-gob_mesdelaciberseguridad-csirtamericas-ciberconsejos-activity-6858402129074278400-Td6H)

### Cybertips for a new CYBERSECURITY AWARENESS MONTH

SMEs



When working from home, remember that the office's security perimeter now extends to your physical location:

**NEVER** connect to your enterprise network without a VPN. Always utilize the most secure means for connection to corporate networks.



### Ciberconsejos para el MES DE LA CIBERSEGURIDAD

PYMES



Para fortalecer la ciberseguridad en tu empresa, recuerda los siguientes consejos:

**REALIZA y VERIFICA** tus copias de seguridad de forma periódica.

**MANTEN** actualizadas tus activos informáticos recurrentemente.

**FOMENTA** una cultura de ciberseguridad en tu organización.



## Campaña de ciberconsejos junto a CSIRT Americas | Semana 4: Personas mayores

[https://www.linkedin.com/posts/csirt-gob\\_mesdelaciberseguridad-csirtamericas-ciberconsejos-activity-6861288721086521344-tvBp](https://www.linkedin.com/posts/csirt-gob_mesdelaciberseguridad-csirtamericas-ciberconsejos-activity-6861288721086521344-tvBp)

### Ciberconsejos para el MES DE LA CIBERSEGURIDAD

ADULTOS MAYORES



**RECUERDA** lo que publicas dura para siempre, cuando publicas algo en internet, comparte inadvertidamente detalles personales con extraños.

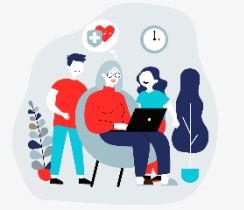
**IGNORA** Los emails y mensajes que crean una sensación de urgencia y requieren que respondas a una crisis. Suelen ser estafas.

**SIEMPRE** Utiliza diferentes contraseñas para cada cuenta, construye tu clave combinando letras, números y símbolos y no la relaciones con información personal.



### Cybertips for a new CYBERSECURITY AWARENESS MONTH

SENIORS



Every senior should consider the following:

**VERIFY** web pages you visit to access medical appointments, banks, pensions, among others.

**NEVER** publish family information, ID numbers or address on sites such as Whatsapp, Facebook or YouTube.

**BE AWARE** you may suffer fraud if you click on links from emails, Whatsapp or SMS.





## Actualidad

Director del CSIRT resalta urgencia de nueva institucionalidad en Cuarto Seminario de Ciberseguridad de la PDI y la Universidad Santa María



Durante octubre tuvo lugar el Cuarto Seminario Internacional de Ciberseguridad, organizado por la Policía de Investigaciones y la Universidad Técnica Federico Santa María, que bajo el título «Hiperconectados: Riesgos, desafíos y responsabilidades» reunió a destacadas personalidades de la ciberseguridad en nuestro país, como el senador Kenneth Pugh, el académico Xavier Bonaire y el director del CSIRT de Gobierno, Carlos Landeros. Este seminario se realiza cada año en el marco del Mes de la Ciberseguridad (<https://www.mesdelaciberseguridad.cl/seminario/>).

Landeros entregó en su presentación «Evolución del ecosistema de la ciberseguridad en Chile» una muestra de cómo el ambiente en esta materia ha ido cambiando en los últimos años, en medio de un crecimiento exponencial de los ataques informáticos y el avance de la transformación digital y la inteligencia artificial, entre otros cambios que exigen la creación de una Agencia Nacional de Ciberseguridad (ANC) como la que busca generar el proyecto de Ley Marco de Ciberseguridad.

Más información sobre el evento y la presentación de Carlos Landeros para descargar en PDF, aquí: <https://www.csirt.gob.cl/noticias/cuarto-simposio-pdi-2021/>.



Ministerio de Ciencia presenta primera Política Nacional de Inteligencia Artificial del país, con un importante componente de ciberseguridad



El Ministerio de Ciencia, Tecnología, Conocimiento e Innovación presentó ayer la nueva Política Nacional de Inteligencia Artificial (disponible para su descarga aquí [Política Nacional de Inteligencia Artificial \(minciencia.gob.cl\)](http://Política Nacional de Inteligencia Artificial (minciencia.gob.cl))), iniciativa inédita en el país y que define los lineamientos estratégicos que seguirán las decisiones de la autoridad en términos de inteligencia artificial por la próxima década.



Esta «hoja de ruta» presenta 180 iniciativas y 70 acciones prioritarias, organizadas alrededor de tres ejes: factores habilitantes, uso y desarrollo de Inteligencia Artificial en Chile y aspectos de ética y seguridad, y fue desarrollada con la participación de 9 mil personas, indica el ministerio, liderados por un comité asesor multidisciplinario de 12 expertos.

La Política nace de una solicitud efectuada por el Presidente Sebastián Piñera en agosto de 2019, y hace mención explícita y reiterada a la ciberseguridad, y a las implicancias para bien y para mal que tiene la extensión del uso de inteligencia artificial (IA) para estas materias.

Así, la ciberseguridad y sus ramificaciones vienen analizadas directamente en su propia sección del capítulo sobre Ética, Aspectos Legales y Regulatorios. Es indispensable ignorar la ciberseguridad como parte de la discusión sobre IA, explica el documento, ya que «el significativo aumento y complejidad de los ciberataques ejecutados diariamente se suma a los diversos propósitos e intereses que ellos persiguen, así como también a la multiplicidad de brechas, vulnerabilidades y vectores de ataque. Un ciberataque puede llegar a ser tan efectivo y perjudicial como un ataque armado, y más aún ante posibles usos bélicos de estos sistemas automatizados».

Estos riesgos aumentan con la aplicación de IA, agrega el texto, algo que ya está sucediendo. Pero al mismo tiempo «la IA se presenta como una nueva herramienta para mantener el ciberespacio libre, abierto, seguro y resiliente y, con ello, cumplir los objetivos señalados en nuestra actual Política Nacional de Ciberseguridad. De ahí la vinculación entre ambas Políticas. La IA, en general, puede contribuir optimizando los tiempos de respuesta, la identificación de vulnerabilidades, la detección de intrusiones, fraudes o identificación de malwares, además de identificar tendencias y/o elaborar rankings de los riesgos relevantes en la red y analizar grandes volúmenes de información de contexto reduciendo al mismo tiempo la intervención humana».

Más detalles sobre lo estipulado por la Política Nacional de IA respecto de la ciberseguridad, y un enlace para descargar y leer la política, aquí: <https://www.csirt.gob.cl/noticias/politica-nacional-ia/>.





CSIRT de Gobierno participa con columna sobre ciberseguridad en especial de El Mercurio



**ALIANZA CHILENA DE CIBERSEGURIDAD**



EDICIONES ESPECIALES@MERCURIO.CL SANTIAGO DE CHILE JUEVES 28 DE OCTUBRE DE 2021 2

AVANCES:

## En la carrera de la ciberseguridad, mantener el ritmo depende de todos

**POR CARLOS LANDEROS,**  
director nacional CSIRT de Gobierno, Ministerio del Interior y Seguridad Pública.

Nuestro trabajo en el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de la Subsecretaría del Interior es una tarea de nunca acabar. Pero, de todos modos, no puedo sino sentirme muy orgulloso de lo que hemos logrado avanzar en la historia del CSIRT, que dio origen desde su nacimiento, en marzo de 2018. Nos ha tocado crear y fortalecer el marco institucional de la ciberseguridad en tiempos en que esta se vuelve cada día más importante, dada la transformación digital en la que nos encontramos inmersos, y el salto hacia la digitalización que ha supuesto la pandemia.

Así, la formalización del propio CSIRT (realizada en 2019) y la creación de la División de Redes y Seguridad Informática del Ministerio del Interior, junto a la definición de normas urgentes de ciberseguridad para el sector público en el Instructivo Presidencial No.8 de 2018, fueron eventos clave en el fortalecimiento de nuestro marco institucional de ciberseguridad, algo que ha hecho a Chile avanzar en rankings internacionales como el Global Cybersecurity Index 2021 de la ITU, en el que avanzamos nueve lugares a nivel mundial y dos en América, y el Reporte Regional de Ciberseguridad 2020 de la OEA, que reconoció un importante avance en relación con la edición 2016.

Es claro que aún tenemos grandes pendientes: necesitamos que el Congreso apruebe, cuanto antes, proyectos que ya se encuentran en sus manos, como la nueva Ley de Delitos Informáticos y la Ley de Protección de Datos Personales, los cuales son



La ciberseguridad es una carrera constante y de nunca acabar.

proyectos transversales e indispensables para mejorar la seguridad digital del país, por lo que no se entiende que sigamos esperando que sean ley. Prontamente, presentaremos al Congreso la Ley Marco, que creará además una nueva Agencia Nacional de Ciberseguridad que profundizará el rol del CSIRT con nuevas atribuciones, combatiendo la gobernanza en la materia, y la regulación del sector privado y la protección de las infraestructuras críticas de información del país. Sin perjuicio de estos proyectos, como CSIRT decidimos impulsar la

adopción de mejores prácticas de ciberseguridad en sectores privados estratégicos, a través de la Subtel, el Coordinador Eléctrico, la CMF y superintendencias como la de Casinos y la de Seguridad Social. Así hemos podido implementar las principales normas que contempla la Ley Marco a sectores económicos clave, para tener a nuestras principales industrias listas para cuando la ley sea promulgada y avanzar en la mejora de estándares, lo que, además, las hace más competitivas en mercados extranjeros, donde adoptan normas

estrictas de ciberseguridad es un requisito. Esta labor refleja la importancia que para nuestro gobierno tiene la colaboración público-privada como vehículo para avanzar en ciberseguridad, adelantándose incluso al trabajo legislativo. Y nos recuerda que contar con estándares comunes es clave, porque el ecosistema de la ciberseguridad es uno solo, y los incidentes de una empresa o industria terminan afectando a las demás y a la población en general. Esto es válido no solo a nivel de empresas, sino de cada chileno.

Por eso, nuestra institución publica cada mes una revista de difusión sobre temas de ciberseguridad y, cada semana, distintos consejos ilustrados y explicados en simple, a través de nuestra web y redes sociales en Twitter, Instagram y LinkedIn. Junto con este material para el público general, el CSIRT ha elaborado y publicado miles de alertas sobre campañas de fraude, phishing y vulnerabilidades, entre otras amenazas informáticas, que tienen como público objetivo a los encargados de ciberseguridad de todo Chile. A propósito de llegar a todos los



Carlos Landeros, director nacional CSIRT de Gobierno, Ministerio del Interior y Seguridad Pública.

chilenos, el CSIRT forma parte de la iniciativa Cybenwomen Challenge de la OEA, que reúne una vez al año a mujeres con habilidades en ciberseguridad, quienes compiten, generan contactos y motivan a sus pares para dedicarse a este rubro con enorme potencial y un gran déficit de profesionales, especialmente mujeres. Ya que hablamos de cooperación internacional, hemos avanzado en el intercambio de información y buenas prácticas, a través de la suscripción de acuerdos con Argentina, la OEA, España, Ecuador, Israel, Colombia, el Reino Unido y Estonia, además de organismos internacionales especializados como CSIRT Americas, Meridian y First.

En definitiva, hemos avanzado mucho, pero aún queda bastante trabajo por delante, ya que la ciberseguridad es una carrera constante y de nunca acabar. Esto nos obliga, como país, a profundizar nuestra institucionalidad, a fomentar la cooperación público-privada y a formar cada año a más encargados de ciberseguridad y expertos en campos como la inteligencia artificial, que entienden la necesidad de mantenerse siempre actualizados con lo último en tecnología, y que antes de incorporar cualquier nuevo proceso tecnológico, debemos considerar cómo afectará esta implementación a nuestra ciberseguridad.

Con motivo del Mes de la Ciberseguridad, la Alianza Chilena de Ciberseguridad lideró un especial en El Mercurio donde reunió la opinión de los principales actores de la materia en el país. Entre ellos estuvo, por supuesto, el CSIRT de Gobierno, que aportó con una columna de su Director Nacional, Carlos Landeros.

Pueden leer el texto en su totalidad en nuestro sitio web: <http://csirt.gob.cl/noticias/csirt-especial-de-el-mercurio>.