



# Informe de gestión de Seguridad Cibernética

## Mayo 2022



```

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.- Introducción.....	3
2.- Alcances del Informe .....	3
3. Resumen mensual de tickets y tipos de incidentes reportados.....	4
3.1. Distribución mensual de tickets según tipo de incidente reportado.....	5
3.2. Tickets emitidos a instituciones públicas y privadas .....	5
3.3. Estado de procesamiento de tickets durante mayo .....	6
3.4. Procedencia de tickets .....	6
4. Boletines de Seguridad Cibernética del mes .....	7
5. Campañas de concientización durante mayo 2022 .....	8



## 1.- Introducción

En el siguiente documento resumimos la labor del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Gobierno durante mayo de 2022. Se compendian así los tickets que procesamos, incluyendo el detalle de los tipos de incidentes reportados y datos como el porcentaje de tickets que se reportaron al sector público y privado.

Además, este informe mensual da cuenta de las alertas sobre campañas de phishing, malware, creación de sitios fraudulentos, vulnerabilidades y ataques de fuerza bruta informados mediante los canales digitales del CSIRT de Gobierno a la ciudadanía.

Para lograr informar oportunamente y las distintas amenazas a los que están expuestas las personas, el CSIRT de Gobierno recibe la invaluable colaboración de personas e instituciones que notifican estos incidentes en cuanto los descubren. A todos ellos, les entregamos nuestros más sinceros agradecimientos. Esperamos seguir contando con su apoyo.

## 2.- Alcances del Informe

La información contenida en este informe proviene del proceso de notificación de incidentes de ciberseguridad del CSIRT de Gobierno, del análisis de casos, de las medidas preventivas aplicadas internamente y a terceros como parte de la misión de esta institución, y de nuestra colaboración con organismos públicos y privados. De igual forma, los datos expuestos incorporan la información pública emitida durante el mes.

El siguiente informe reúne:

- El análisis de la gestión de tickets mensual.
- La distribución de los tickets analizados durante el mes.
- El análisis de los tipos de incidentes de acuerdo con 10 variables seleccionadas.



### 3. Resumen mensual de tickets y tipos de incidentes reportados

Ante las diversas amenazas y peligros que abundan en el ciberespacio, el CSIRT de Gobierno notifica a instituciones públicas y privadas de aquellos riesgos que considera más probables de afectar a sus sistemas. Es así como este mes generamos **2.602 tickets**, un **5% más que en abril**. Estos tickets de mayo corresponden a las siguientes categorías, definidas<sup>1</sup> según el tipo de incidente de seguridad informática al que corresponden, y ordenadas a según su frecuencia:

N°	Tipos de Tickets	Código	Mayo 2022
1	Vulnerabilidad	9V00	1989
2	Disponibilidad	6D00	257
3	Otros	11O00	134
4	Código Malicioso	2C00	103
5	Fraude	8F00	74
6	Información de seguridad de contenidos	7S00	36
7	Intentos de Intrusión	4I00	6
8	Intrusión	4I00	2
9	Recopilación de Información	5I00	1
10	Contenido Abusivo	1A00	0
Total			2602

Imagen 1.- Distribución de tickets reportados durante el mes por tipo.

#### Prevalencia de los distintos tipos de tickets

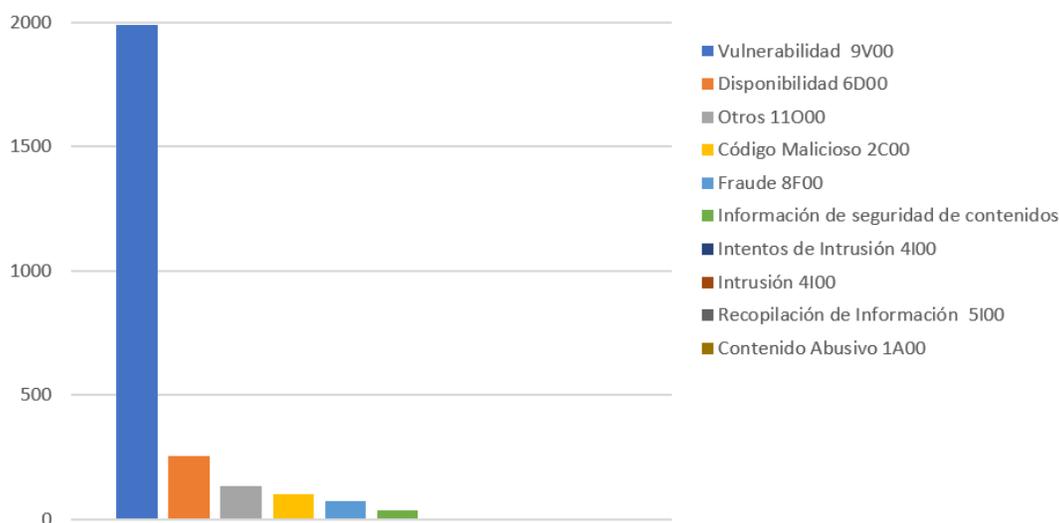


Imagen 2.- Prevalencia de tickets reportados durante el mes por tipo.

<sup>1</sup> Matriz de clasificación de incidentes de ENISA, Agencia de la Unión Europea para la Ciberseguridad: <https://www.csirt.gob.cl/matriz-clasificacion-incidentes/>



Respecto de la categoría “Vulnerabilidad”, recordamos lo esencial de realizar las actualizaciones de nuestros programas y sistemas en cuanto están disponibles, ya que no hacerlo, en conjunto con la deficiencia de las políticas de seguridad de muchas instituciones, aumentan su exposición a ataques cibernéticos. Una fuente sobre nuevas actualizaciones a estas vulnerabilidades la ponemos disponible en nuestra propia web: <https://www.csirt.gob.cl/vulnerabilidades/>.

### 3.1. Distribución mensual de tickets según tipo de incidente reportado

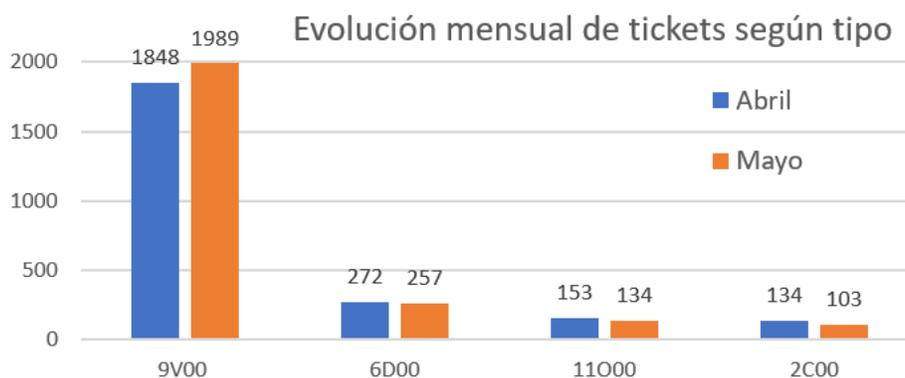


Imagen 3.- Distribución mensual de tickets por tipo.

### 3.2. Tickets emitidos a instituciones públicas y privadas

Nuestra vinculación con el sector privado es fundamental para contribuir a mantener un ciberespacio más seguro, además de proteger los sistemas e información de todos los chilenos. Y para lograr esa vinculación, el intercambio de información y buenas prácticas juegan un rol fundamental. Debido a lo anterior, adquirimos el compromiso de alertar de situaciones o incidentes riesgosos que se detectan en organizaciones privadas (que corresponden al **25%** de los tickets).

Tickets	Privado	Público	Total
Vulnerabilidad	199	1790	1989
Disponibilidad	20	237	257
Otros	107	27	134
Código Malicioso	88	15	103
Fraude	65	9	74
Información de seguridad de contenidos	28	8	36
Intentos de Intrusión	5	1	6
Intrusión	0	2	2
Recopilación de Información	1	0	1
Contenido Abusivo	0	0	0
<b>Total</b>	<b>513</b>	<b>2089</b>	<b>2602</b>



### 3.3. Estado de procesamiento de tickets durante mayo

Este mes, el **59%** de los tickets generados en el período logró ser cerrada exitosamente (contra un 51% en abril), mientras el resto seguirá siendo procesado en junio.

Total estado Ticket	Total
En desarrollo	1081
Cerrados	1521
<b>Total general</b>	<b>2602</b>

### 3.4. Procedencia de tickets

Los tickets que procesa el CSIRT de Gobierno se pueden originar tanto interna como externamente. Aquellos de origen interno (**93,1% en mayo**) fueron generados por sistemas propios del Ministerio del Interior y Seguridad Pública, mediante software utilizado por el CSIRT, que también considera los sensores que dan aviso o reportan desde otros servicios públicos y las Fuerzas Armadas.

Por otro lado, los tickets de origen externo (**6,9%**) se originan en proveedores vinculados al CSIRT vía contractual o que se generan a través de reportes ciudadanos, via nuestro call center y por formulario web, alerta desde otros CSIRT internacionales, o por correos electrónicos de empresas privadas.

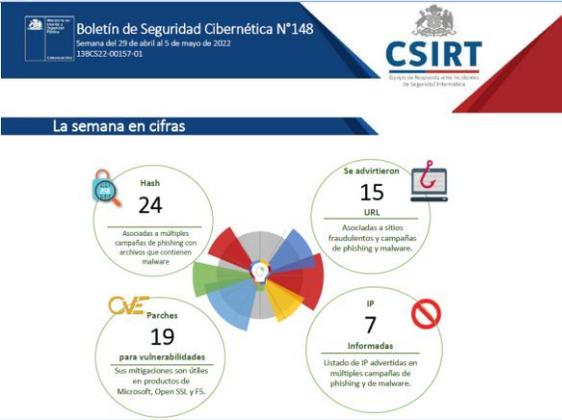
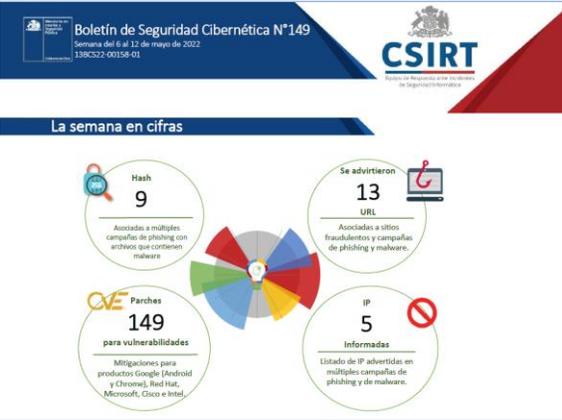
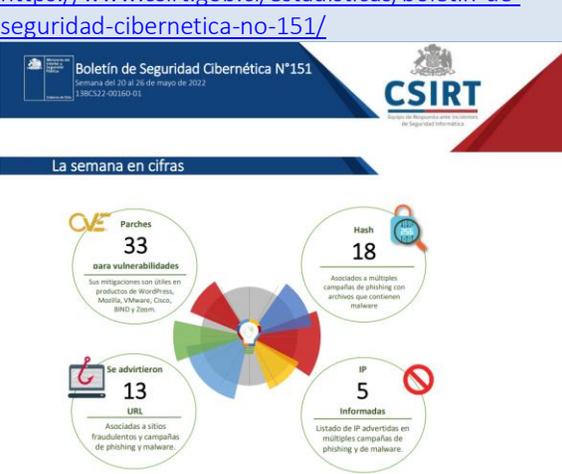
Tipo de Fuente	Cantidad de Tickets
Servicios Internos	2422
Servicios Externos	180
<b>Total Fuentes de Tickets</b>	<b>2602</b>

Fuentes de Origen Externo de Tickets	Cantidad de Tickets
Formulario web	127
Call center	6
Redes sociales	1
Internacionales	0
Proveedor de servicio	0
Email	46
<b>Total</b>	<b>180</b>



## 4. Boletines de Seguridad Cibernética del mes

Los enlaces a continuación corresponden a los boletines semanales publicados durante mayo de 2022. Cada uno resume las actividades, alertas y vulnerabilidades comunicadas por el CSIRT de Gobierno esa semana.

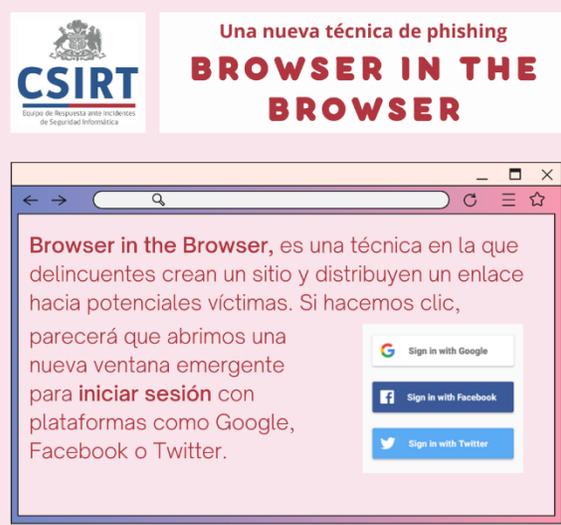
Boletín de Seguridad Cibernética n°148	Boletín de Seguridad Cibernética n°149
<a href="https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-148/">https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-148/</a>	<a href="https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-149/">https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-149/</a>
 <p><b>Boletín de Seguridad Cibernética N°148</b> Semana del 28 de abril al 5 de mayo de 2022 138CS22-00157-01</p> <p><b>La semana en cifras</b></p> <ul style="list-style-type: none"> <li><b>Hash 24</b>: Asociadas a múltiples campañas de phishing con archivos que contienen malware.</li> <li><b>Se advirtieron 15 URL</b>: Asociadas a sitios fraudulentos y campañas de phishing y de malware.</li> <li><b>Parches 19 para vulnerabilidades</b>: Sus mitigaciones son útiles en productos de Microsoft, Open SSL, y F5.</li> <li><b>IP 7 Informadas</b>: Listado de IP advertidas en múltiples campañas de phishing y de malware.</li> </ul>	 <p><b>Boletín de Seguridad Cibernética N°149</b> Semana del 6 al 12 de mayo de 2022 138CS22-00158-01</p> <p><b>La semana en cifras</b></p> <ul style="list-style-type: none"> <li><b>Hash 9</b>: Asociadas a múltiples campañas de phishing con archivos que contienen malware.</li> <li><b>Se advirtieron 13 URL</b>: Asociadas a sitios fraudulentos y campañas de phishing y de malware.</li> <li><b>Parches 149 para vulnerabilidades</b>: Mitigaciones para productos Google (Android y Chrome), Red Hat, Microsoft, Cisco e Intel.</li> <li><b>IP 5 Informadas</b>: Listado de IP advertidas en múltiples campañas de phishing y de malware.</li> </ul>
<b>Boletín de Seguridad Cibernética n°150</b> <a href="https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-150/">https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-150/</a>	<b>Boletín de Seguridad Cibernética n°151</b> <a href="https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-151/">https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-151/</a>
 <p><b>Boletín de Seguridad Cibernética N°150</b> Semana del 13 al 19 de mayo de 2022 138CS22-00159-01</p> <p><b>La semana en cifras</b></p> <ul style="list-style-type: none"> <li><b>Parches 30 para vulnerabilidades</b>: Sus mitigaciones son útiles en productos de Cisco, WordPress, VMware, Zynel, Sonos, Web y Apple.</li> <li><b>Se advirtieron 11 URL</b>: Asociadas a sitios fraudulentos y campañas de phishing y de malware.</li> <li><b>IP 10 Informadas</b>: Listado de IP advertidas en múltiples campañas de phishing y de malware.</li> </ul>	 <p><b>Boletín de Seguridad Cibernética N°151</b> Semana del 20 al 26 de mayo de 2022 138CS22-00160-01</p> <p><b>La semana en cifras</b></p> <ul style="list-style-type: none"> <li><b>Parches 33 para vulnerabilidades</b>: Sus mitigaciones son útiles en productos de WordPress, Mozilla, VMware, Cisco, BIND y Zoom.</li> <li><b>Hash 18</b>: Asociadas a múltiples campañas de phishing con archivos que contienen malware.</li> <li><b>Se advirtieron 13 URL</b>: Asociadas a sitios fraudulentos y campañas de phishing y de malware.</li> <li><b>IP 5 Informadas</b>: Listado de IP advertidas en múltiples campañas de phishing y de malware.</li> </ul>



Boletín de Seguridad Cibernética n°143	
<a href="https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-152/">https://www.csirt.gob.cl/estadisticas/boletin-de-seguridad-cibernetica-no-152/</a>	
	
<p>La semana en cifras</p>	
	
	

## 5. Campañas de concientización durante mayo 2022

Para crear conciencia de los riesgos, amenazas y tendencias en el mundo digital, cada semana difundimos en nuestra web y las cuentas del CSIRT de Gobierno en redes sociales, campañas educativas, las que se encuentran disponibles en la sección Recomendaciones de la página web del CSIRT de Gobierno: <https://www.csirt.gob.cl/recomendaciones/>.

Ciberconsejos   Browser In The Browser (BITB), técnica que dificulta identificar un phishing	Decálogo de Ciberseguridad
<a href="https://www.csirt.gob.cl/recomendaciones/ciberconsejos-bitb/">https://www.csirt.gob.cl/recomendaciones/ciberconsejos-bitb/</a>	<a href="https://www.csirt.gob.cl/recomendaciones/decalogo-de-ciberseguridad/">https://www.csirt.gob.cl/recomendaciones/decalogo-de-ciberseguridad/</a>
	



<p>Ciberdiccionario Vol. IV</p>	<p>Ciberconsejos   ¿Cómo prevenir la escalabilidad de privilegios?</p>
<p><a href="https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-4/">https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-4/</a></p>	<p><a href="https://www.csirt.gob.cl/recomendaciones/ciberconsejos-escalabilidad-de-privilegios/">https://www.csirt.gob.cl/recomendaciones/ciberconsejos-escalabilidad-de-privilegios/</a></p>
 <h2>Ciberdiccionario</h2> <p><b>1.- CRACKER:</b></p> <p>Persona que consigue ingresar sin autorización a sistemas informáticos, con fines maliciosos, como robar datos o suplantar a otra persona.</p> <p>Incluye a los hackers maliciosos, ya que el concepto de hacker como tal puede tener buenas o malas intenciones.</p> 	<h2>Ciberconsejos</h2> <h3>¿Cómo prevenir la Escalabilidad de privilegios?</h3> <p><b>¿Qué es?</b></p> <p>Tipo de ataque con el que los ciberdelinquentes logran, tras acceder sin autorización a un sector relativamente poco sensible de un sistema, alcanzar otros, explotando fallas en la configuración del mismo o vulnerabilidades de software.</p> <p>O sea, pueden conseguir mayores privilegios definidos en computación como la capacidad de realizar cambios en el sistema y ver y modificar datos contenidos en él de los que tenían al penetrar el sistema.</p> 
<p>Ciberdiccionario Vol. V</p>	<p>Día Mundial de Internet: Hitos de la llegada de internet a Chile</p>
<p><a href="https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-5/">https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-5/</a></p>	<p><a href="https://www.csirt.gob.cl/recomendaciones/dia-mundial-de-internet/">https://www.csirt.gob.cl/recomendaciones/dia-mundial-de-internet/</a></p>
 <h2>Ciberdiccionario</h2> <p><b>1.- COOKIE:</b></p>  <p>Archivos que se transmiten al navegar por internet y que pueden ser almacenados tanto por nuestro navegador como por la página que visitamos.</p> <p>Dependiendo del sitio y las cookies, pueden recolectar información de sitios visitados, búsquedas realizadas, permitiendo que los sitios web reconozcan al usuario, recuerden sus preferencias y personalicen la publicidad que le muestran.</p>	 <h2>La Historia de Internet en Chile</h2> <p><b>1985. Primer e-mail chileno:</b></p> <p>Como parte de un proyecto entre la Universidad de Chile y la Universidad de Santiago se envió el primer correo electrónico con este mensaje: "si este mail te llega, abramos una botella de champaña".</p> 



<p>Ciberdiccionario Vol. VI</p> <p><a href="https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-6/">https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-6/</a></p>  <p><b>Ciberdiccionario</b>   <b>CSIRT</b> Equipo de Respuesta ante Incidentes de Seguridad Informática</p> <p><b>1.- ATAQUE DE DENEGACIÓN DE SERVICIOS DISTRIBUIDO O DDoS:</b></p> <p>Este tipo de ataque cibernético busca lograr que un servicio o página web no siga estando disponible (o sea, para “botarlo” o hacer “que se caiga”), para lo que el atacante satura el servidor objetivo de solicitudes, logrando que colapse.</p>	<p>Ciberconsejos: Vulnerabilidades informáticas</p> <p><a href="https://www.csirt.gob.cl/recomendaciones/ciberconsejos-vulnerabilidades/">https://www.csirt.gob.cl/recomendaciones/ciberconsejos-vulnerabilidades/</a></p>  <p><b>Qué son y cómo protegernos Vulnerabilidades informáticas</b></p> <p>Las vulnerabilidades informáticas son fallas de un programa, un “punto débil” que permite a un ciberdelincuente acceder a nuestros equipos o sistemas sin autorización.</p> <p>El intruso puede, dependiendo de la vulnerabilidad, acceder a nuestros datos, tomar control total de un computador o smartphone, o encriptarlo y exigir recompensa, entre otros.</p>
<p>Subsecretaría del Interior y Cámara de Comercio de Santiago coordinan medidas de seguridad para primer CyberDay de 2022</p>	
<p><a href="https://www.csirt.gob.cl/recomendaciones/consejos-cyberday-2022/">https://www.csirt.gob.cl/recomendaciones/consejos-cyberday-2022/</a></p>	
 <p>Ministerio del Interior y Seguridad Pública</p> <p><b>CIBERCONSEJOS PARA UN CYBERDAY SEGURO</b></p> <p>#Cybercl</p> <p><b>SI BUSCAS</b> una buena oferta, hazlo directamente en los sitios web oficiales de las tiendas comerciales.</p> <p><b>SI RECIBES UN CORREO</b> inesperado con enlaces o archivos adjuntos sobre una oferta especial, descártalo, podría tratarse de una estafa de phishing.</p> <p>CYBERDATO: 795 comercios serán parte del evento</p> <p>Verifica todas las webs oficiales en <a href="http://www.cyber.cl">www.cyber.cl</a></p> <p>CCS</p>	