INFORME ANUAL DE GESTIÓN 2021

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

División de Redes y Seguridad Informática
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Índice

1.- Introducción

El siguiente es un resumen de lo hecho como Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Gobierno a lo largo de 2021. 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.

Junto con esto, este informe anual 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 y esperamos también contar con su apoyo durante 2022, algo que, por lo demás, se volvió más fácil con el lanzamiento a fines del pasado año de nuestro nuevo número de emergencia 1510.

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 2021.

El contenido del siguiente informe reúne:

- ✓ El análisis de la gestión de tickets anual.
- ✓ La distribución de los tickets analizados durante el año.
- ✓ El análisis de los tipos de incidentes de acuerdo con 11 variables seleccionadas.
- ✓ Las tendencias de ciberseguridad que se espera destaquen en 2022.

3.- Resumen anual 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 entre el 1 de enero y el 31 de diciembre de 2021 generamos 22.473 tickets (un 47% más que en el año anterior) los que corresponden a 11 categorías definidas[1] según el tipo de incidente de seguridad informática al que corresponden, y ordenadas en la siguiente tabla:

N°	Tipos de Ticket	Código	2020	2021
1	Vulnerabilidad	9V00	3.353	**13.371**
2	Disponibilidad	6D00	624	**2.979**
3	Seguridad de los contenidos de información	7S00	1.231	**1.486**
4	Recopilación de Información	3R00	5.504	**1.160**
5	Fraude	8F00	2.211	**1.153**
6	Operaciones Ciberseguridad CSIRT	19OC	662	**646**
7	Otros	11O00	NA	**586**
8	Código Malicioso	2C00	1.468	**476**
9	Intentos de Intrusión	4I00	50	**320**
10	Intrusión	5I00	111	**165**
11	Contenido Abusivo	1A00	107	**131**
Total			15.321	**22.473**

Incidentes por mes durante 2021													
Código	**Ene**	**Feb**	**Mar**	**Abr**	**May**	**Jun**	**Jul**	**Ago**	**Sep**	**Oct**	**Nov**	**Dic**	**Total**
9V00	239	921	1.402	886	1.326	870	1.717	1.154	753	1.158	1.288	1.657	**13.371**
6D00	3	44	5	0	330	369	376	447	391	340	337	337	**2.979**
7S00	176	124	77	153	88	125	111	146	149	131	167	39	**1.486**
3R00	372	324	132	225	85	8	0	3	1	6	3	1	**1.160**
8F00	82	65	40	84	99	136	81	151	105	78	118	114	**1.153**
19OC	91	68	173	110	204	0	0	0	0	0	0	0	**646**
11O00	0	0	0	0	0	59	53	76	86	115	106	91	**586**
2C00	125	106	79	43	24	24	3	5	15	21	16	15	**476**
4I00	6	2	7	13	238	0	0	3	1	2	0	48	**320**
5I00	21	21	23	23	15	0	0	5	1	1	0	55	**165**
1A00	22	16	23	35	20	2	0	6	2	1	1	3	**131**
Total	1.137	1.691	1.961	1.572	2.429	1.593	2.341	1.996	1.504	1.853	2.036	2.360	**22.473**

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

3.1 Distribución de incidentes según tipo

Dentro de las 10 categorías antes descritas, las vulnerabilidades representan por lejos la más reportadas, con un 59% del total, contra el 22% que representaron en 2020. Los siguientes incidentes más comúnmente reportados fueron de disponibilidad y seguridad de los contenidos de información respectivamente.

Respecto de la categoría "Vulnerabilidad", recordamos lo esencial de realizar las actualizaciones de nuestros programas 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.

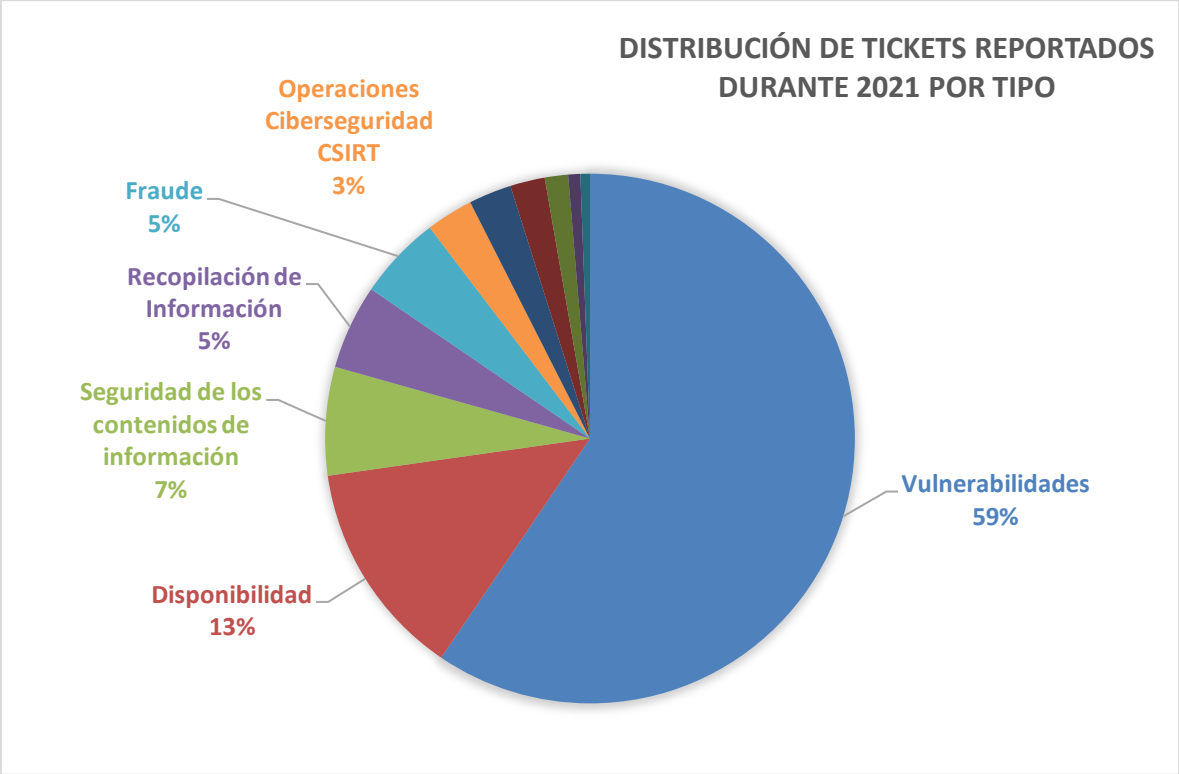


Imagen 1.- Distribución de tickets reportados durante 2021 por tipo.

3.1.1 Distribución mensual de tickets según tipo de incidente reportado

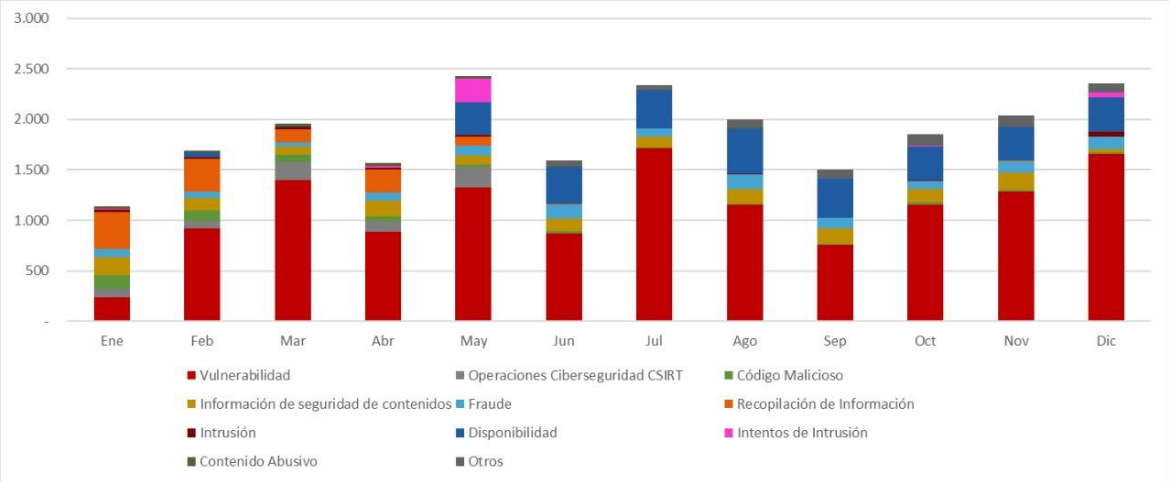


Imagen 2.- Distribución mensual de tickets por tipo.

3.1.2 Tipo de incidente: Vulnerabilidades

Las vulnerabilidades fueron el tipo de incidente más reportados por el CSIRT de Gobierno, llegando a un máximo de 1.717 incidentes y mostrando una tendencia al alza desde septiembre.

Esto nos recuerda que el reporte constante de las vulnerabilidades detectadas por el CSIRT es clave para que las instituciones afectadas parchen estas vulnerabilidades, principal vector de acceso para los ciberatacantes.

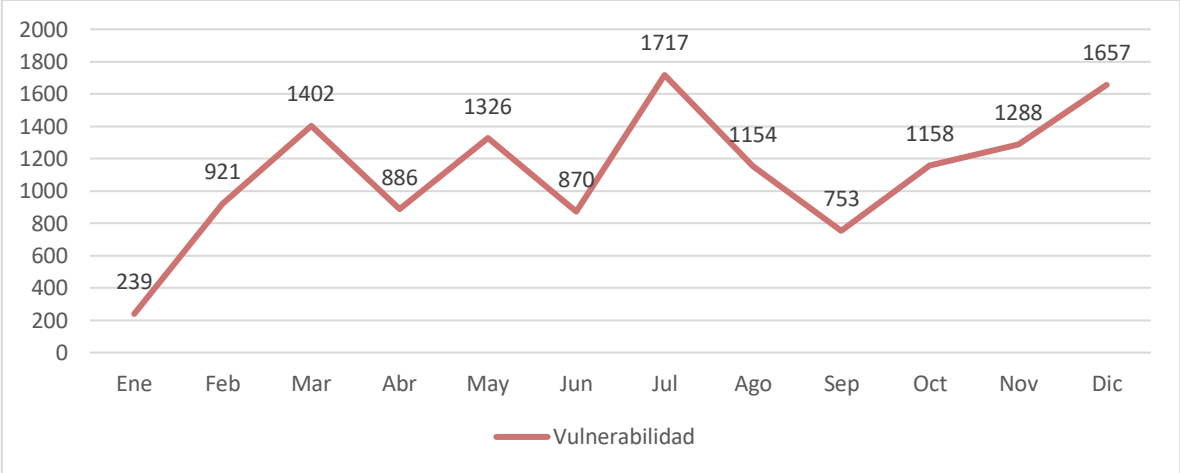


Imagen 3.- Distribución mensual de incidentes del tipo Vulnerabilidades.

3.1.2 Tipo de incidente: Operaciones de ciberseguridad del CSIRT de Gobierno

Estos son incidentes que el CSIRT de Gobierno reporta directamente a la Red de Conectividad del Estado (RCE), especialmente al bloqueo de IP de acuerdo con su reputación.

Se destaca en mayo un peak de este tipo eventos, mismo mes en que se terminó de usar este indicador, pasando a registrarse en la categoría "Otros" (3.1.11).

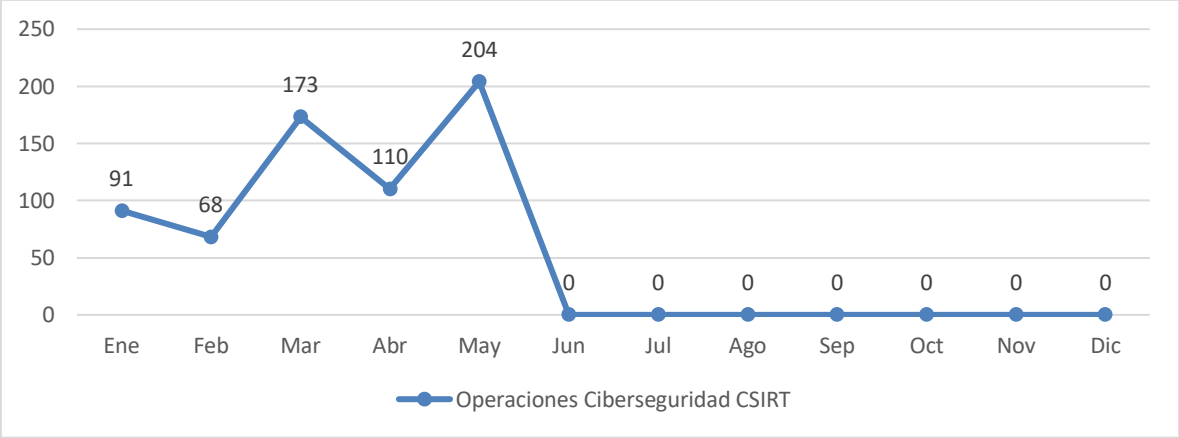


Imagen 4.- Distribución mensual de incidentes del tipo Operaciones Ciberseguridad CSIRT.

3.1.3 Tipo de incidente: Código malicioso

Afortunadamente los ataques de código malicioso (también conocido como software malicioso o "malware") reportados fueron cayendo fuertemente durante 2021, terminando en promedio casi 90% por debajo de la cifra de enero. En esta categoría se engloban virus, gusanos, troyanos, y spyware, entre otros ejemplos de malware.

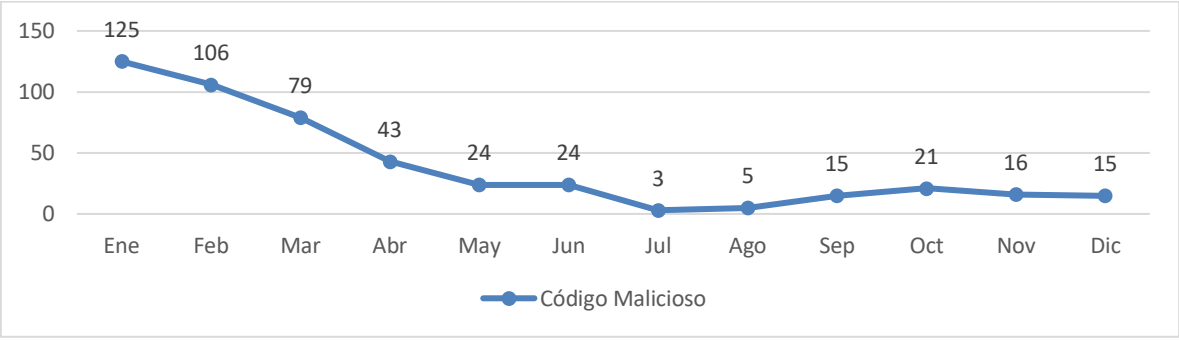


Imagen 5.- Distribución mensual de incidentes del tipo Código Malicioso.

3.1.4 Tipo de incidente: Seguridad del Contenido de Información

Esta clase de incidente reúne dos categorías: el acceso no autorizado a la información de un sistema vulnerado y la modificación no autorizada de la misma.

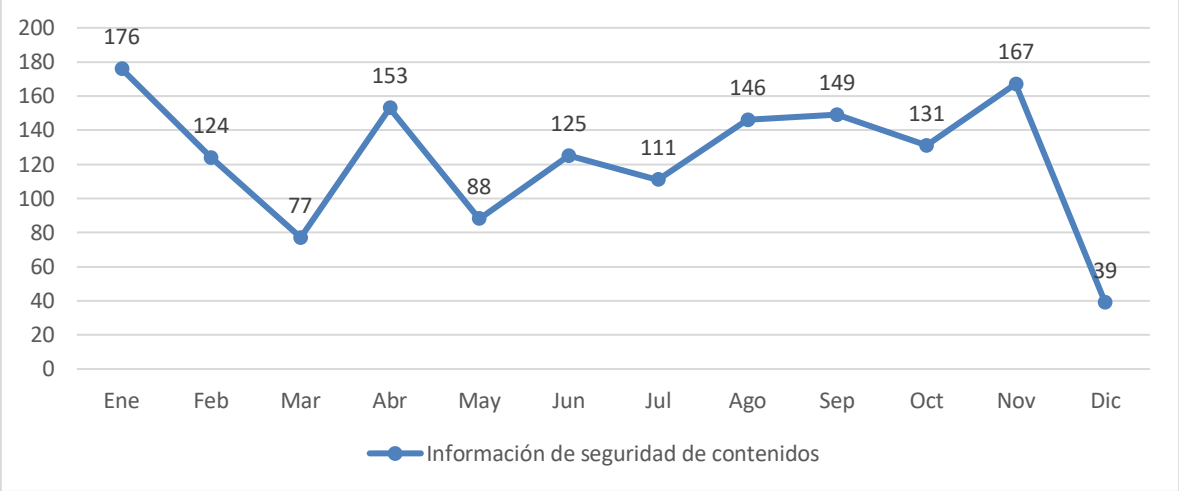


Imagen 6.- Distribución mensual de incidentes del tipo Seguridad del Contenido de Información.

3.1.5 Tipo de incidente: Fraude

Los fraudes, principalmente de tipo phishing y spear phishing, son las principales técnicas para penetrar a un sistema sin autorización. Con ellos, los ciberdelincuentes se aprovechan de la falta de conocimiento y exceso de credulidad de los usuarios para conseguir que éstos les entreguen acceso a sus instituciones. Son el fuerte de la mayoría de las campañas destinadas a aumentar la conciencia de seguridad digital de los empleados de las organizaciones, ya que un clic equivocado de una persona dentro de la red corporativa puede comprometerla completamente.

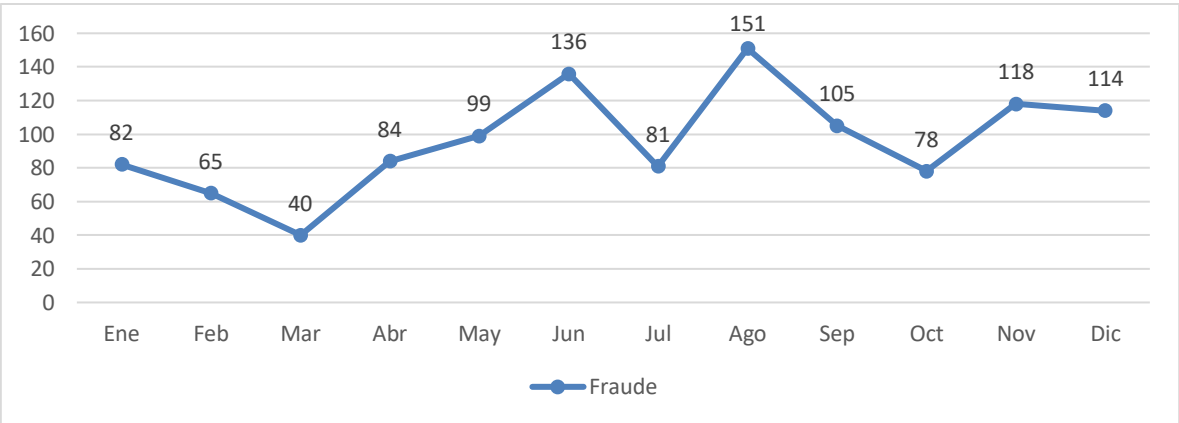


Imagen 7.- Distribución mensual de incidentes tipo Fraude.

3.1.6 Tipo de incidentes: Recopilación de Información

La recopilación de información incluye ataques de exploración, es decir, el envío por delincuentes de solicitudes a un sistema para descubrir puntos débiles, como la recopilación de información sobre hosts, servicios y cuentas, la observación del tráfico de una víctima y la ingeniería social.

Su cantidad baja debido a cambios en la forma en que se clasifican dentro del CSIRT de Gobierno.

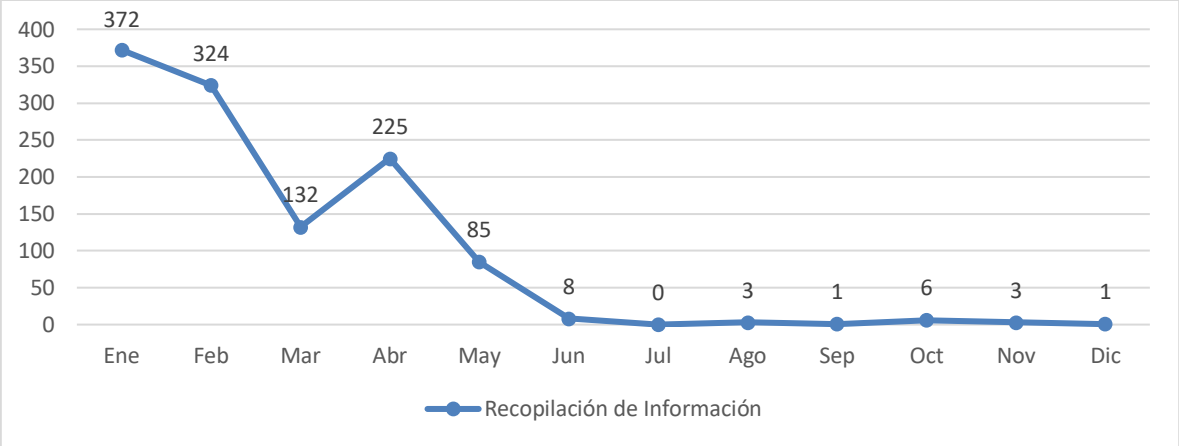


Imagen 8.- Distribución mensual de incidentes del tipo Recopilación de Información

3.1.7 Tipo de incidentes: Intrusión

La categoría Intrusión se refiere principalmente al acceso no autorizado a través del uso de credenciales robadas. Esta categoría muestra solo las intrusiones que fueron detectadas, y se debe tener en cuenta que esta detección puede suceder mucho tiempo después de que este ingreso no autorizado comenzó a suceder dentro de una red.

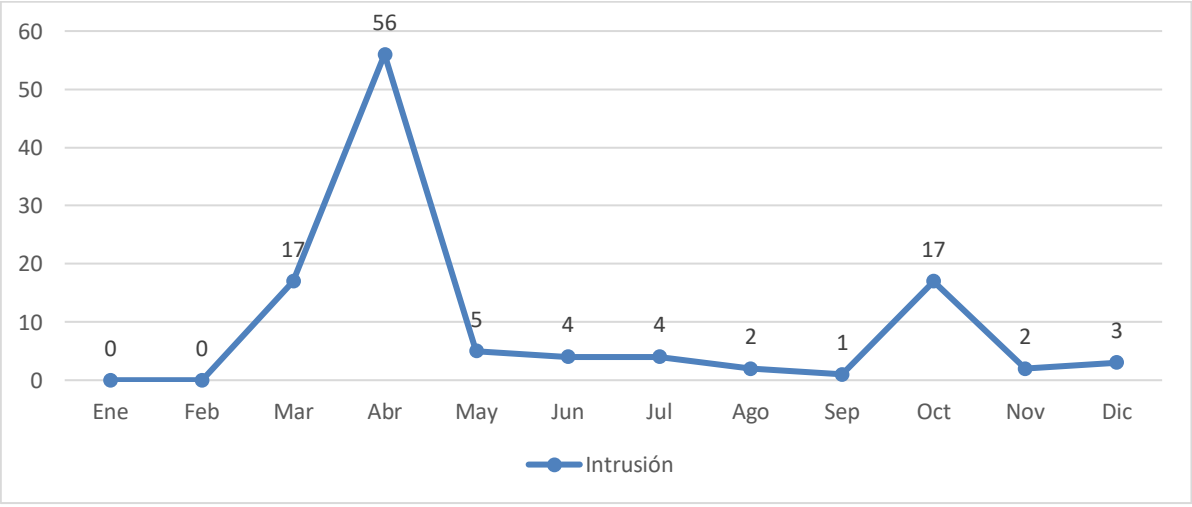


Imagen 9.- Distribución mensual de Intrusión

3.1.8 Tipo de incidente: Disponibilidad

Asociados a los ataques de denegación de servicio, este año se observó un descenso de los registros, potencialmente debido a una baja de la actividad hacktivista contra instituciones de gobierno, lo que explicaría que los incidentes aumenten en octubre.

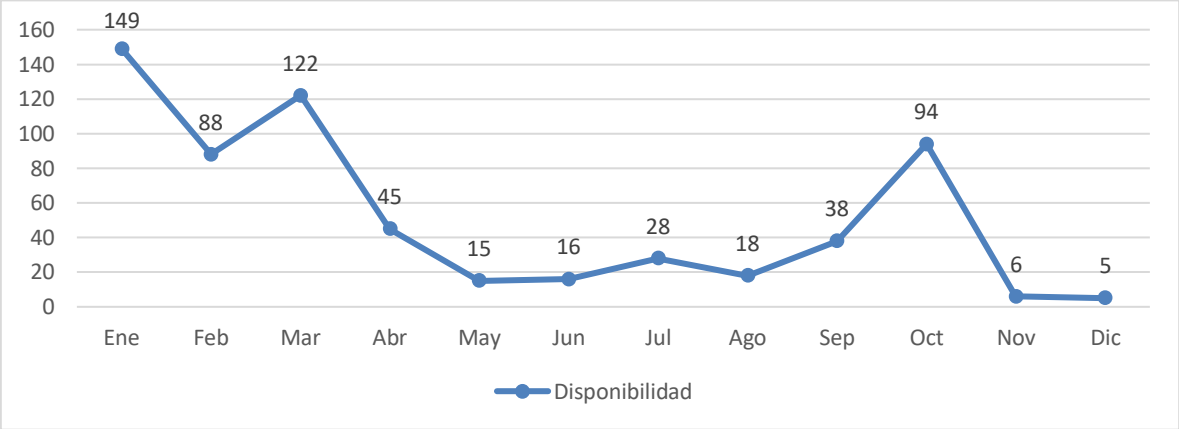


Imagen 10.- Distribución mensual de incidentes tipo Disponibilidad.

3.1.9 Tipo de incidente: Intentos de Intrusión

Se trata de los intentos fallidos de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas, siendo relativamente poco comunes. No confundir con las intrusiones exitosas (punto 3.1.7.). Su cantidad registrada baja debido a cambios en la forma en que se clasifican dentro del CSIRT de Gobierno.

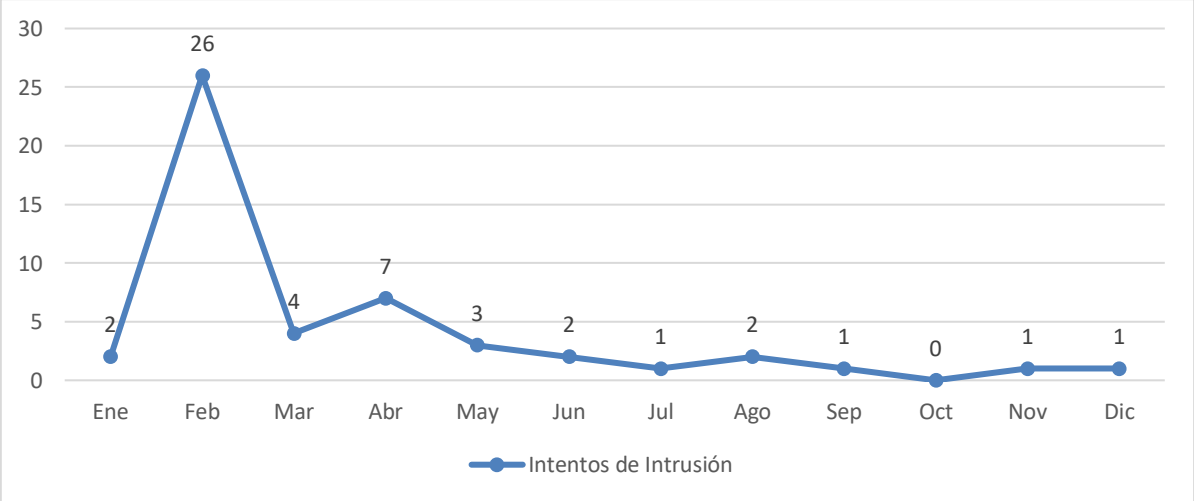


Imagen 11.- Distribución mensual de Intentos de Intrusión

3.1.10 Tipo de incidentes: Contenido abusivo

El alza de este tipo de incidente a fines de año muestra que sigue habiendo instituciones que no están tomando las suficientes medidas preventivas para evitar estos ataques, en los que agentes maliciosos alteran las páginas web de sus víctimas y redirigen el tráfico hacia contenido abusivo como pornografía, violencia u otros.

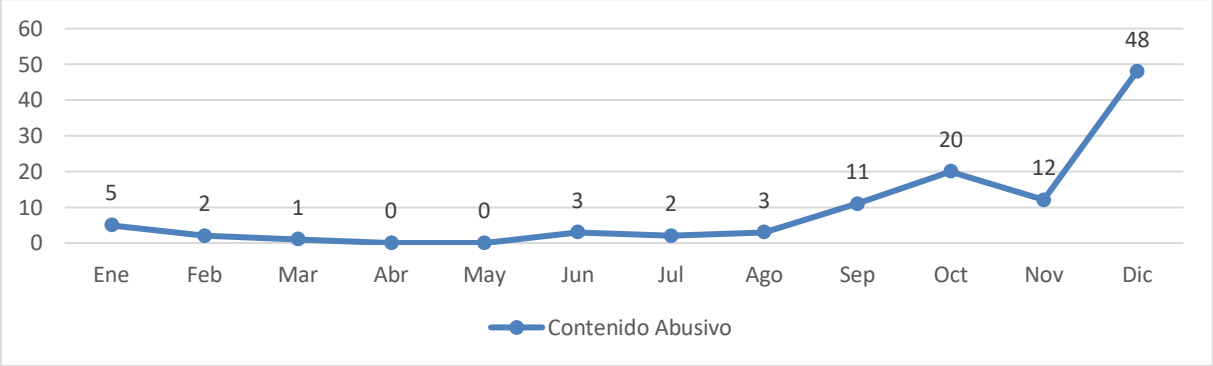
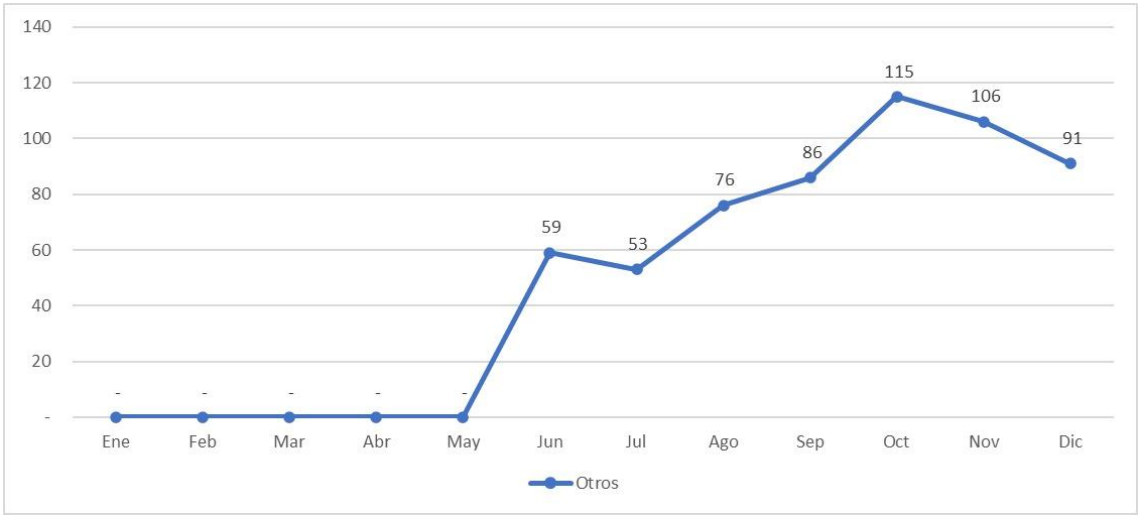


Imagen 12.- Distribución mensual de Contenido Abusivo

3.1.11 Tipo de incidentes: Otros

En esta categoría se reúnen desde junio tickets que se considera no calzan dentro de las demás categorías definidas por Enisa[2]. En el caso del CSIRT de Gobierno, se tratan principalmente de reportes de tráfico que las entidades nos solicitan para analizar potenciales amenazas, los tickets avisando de escaneos preventivos realizados por el CSIRT a las instituciones, y los bloqueos preventivos realizados por el CSIRT de Gobierno.



[2] Matriz de clasificación de incidentes de ENISA, Agencia de la Unión Europea para la Ciberseguridad: https://www.csirt.gob.cl/matriz-clasificacion-incidentes/

3.2 Tickets emitidos a instituciones públicas y privadas

Desde la creación del CSIRT de Gobierno, la vinculación con el sector privado ha sido fundamental para contribuir a mantener un ciberespacio más seguro, además de proteger los sistemas e información de todos los chilenos.

Para esto, el intercambio de información y buenas prácticas juegan un rol fundamental. Por lo que adquirimos el compromiso de también alertar de situaciones o incidentes riesgosos que se detectan en organizaciones privadas. Es así como de 18% (4.061) de los 18.412 tickets totales corresponde al sector privado, lo que de todas formas representa una proporción menor al 30% de 2020.

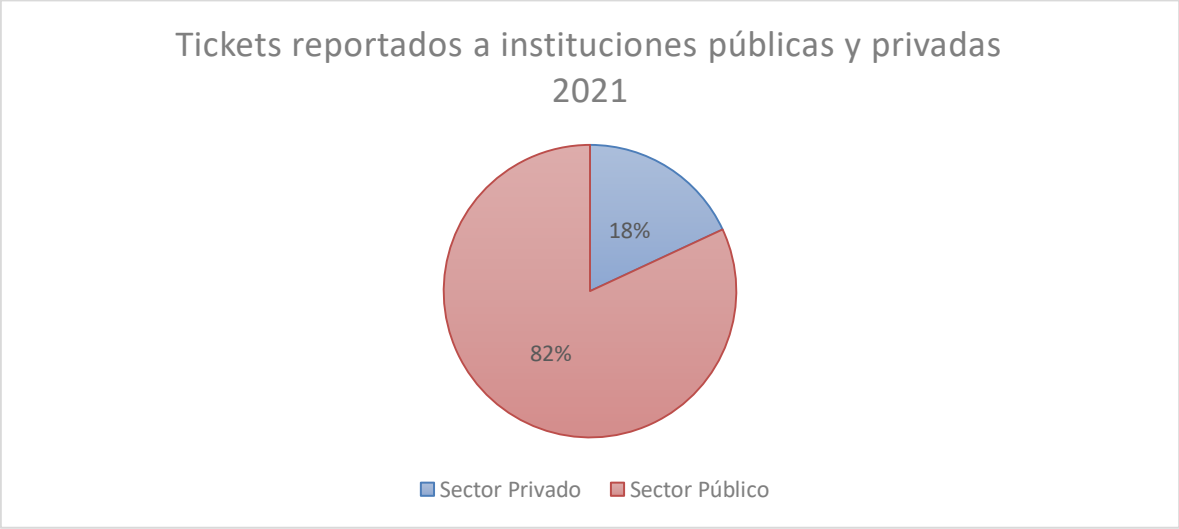


Imagen 3.- Distribución de tickets reportados a instituciones públicas y privadas

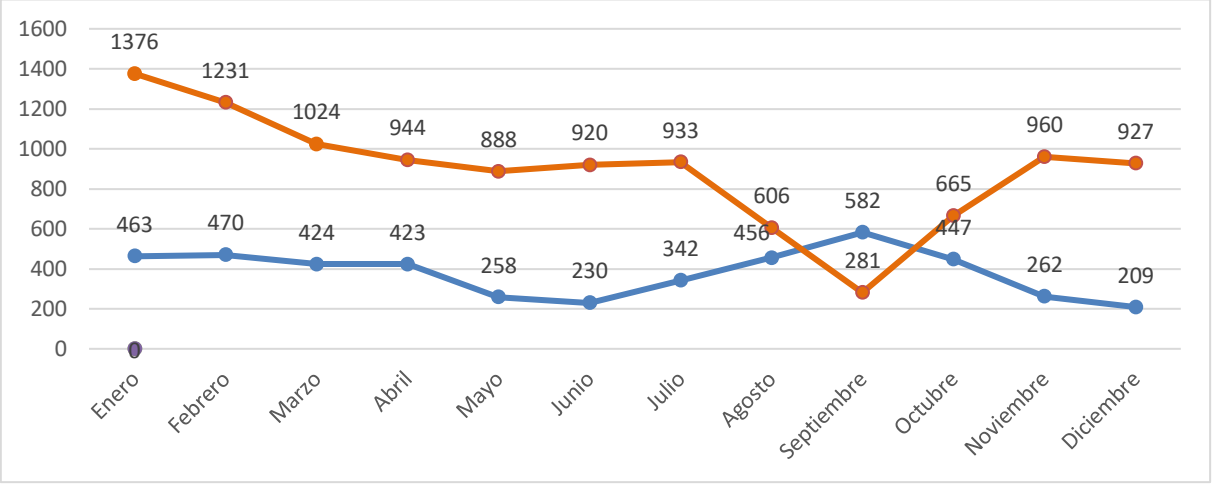
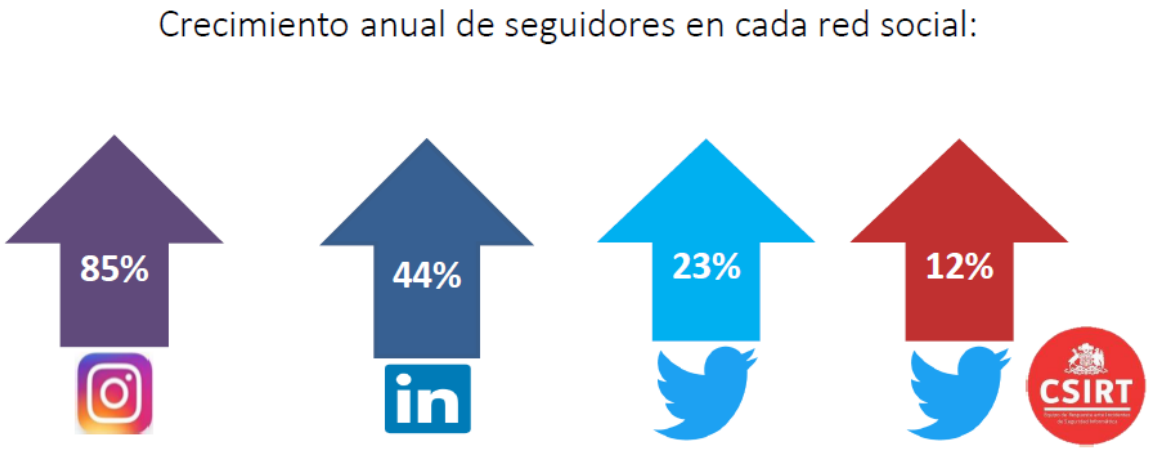


Imagen 13.- Reporte de tickets a instituciones públicas y privadas por mes.

4. Campañas de Concientización durante 2021

Con el fin de crear más conciencia sobre los riesgos, amenazas y tendencias que existen en el mundo digital, cada semana difundimos en nuestra web y las cuentas del CSIRT de Gobierno en redes sociales (Instagram, Linkedin y Twitter), campañas educativas sobre variados temas acordes a la contingencia nacional e internacional, además de seguir con el lanzamiento de nuestra revista mensual Cibersucesos.



Además, organizamos una nueva cuenta de Twitter apuntada a difundir datos a la ciudadanía en general, https://twitter.com/CSIRTConciencia, que complementa a nuestra cuenta ya establecida, https://twitter.com/CSIRTGOB, que se dirige a un público más especializado.

Algunos temas abordados durante 2021 fueron las estafas digitales, las precauciones que se deben tener antes de escanear códigos QR, el egourfing, el malvertising, los keyloggers y el secuestro de Whatsapp.

Puede encontrar todas las campañas en sección recomendaciones de la página web del CSIRT de Gobierno: https://www.csirt.gob.cl/recomendaciones/.

Cooperación panamericana

El CSIRT de Gobierno desarrolló una campaña para conmemorar el Mes de la Ciberseguridad a nivel panamericano, junto a CSIRT y CERT del continente, asociados a CSIRTAmericas, de la Organización de los Estados Americanos (OEA). Fue compartida en 12 países de América durante todo el mes.

Cuentos para niños y adolescentes

Otra iniciativa novedosa del CSIRT de Gobierno fue publicar una compilación de cuentos de ciberseguridad para niños y adolescentes, escritas por los propios miembros del CSIRT y entregada a bibliotecas públicas para su mayor decisión.

5. Nuevos acuerdos de colaboración público-privada

Durante 2021, el CSIRT de Gobierno firmó acuerdos de colaboración con las siguientes entidades de los mundos público y privado, incluyendo empresas, universidades, superintendencias y gremios.

Aguas Andinas
Esval y Aguas del Valle
Mutual de Seguridad
Andes Salud
Masisa
AFC
IRADE
SAAM
SB Pay
Instituto Nacional de Normalización
Universidad de Concepción
BHP
Bolsa de Santiago
Universidad Autónoma
Essbio
Empresas Eléctricas AG
Aguas Antofagasta
Corporación de Universidades Privadas
Corporación Alta Ley
Trend Micro

Asimismo, y en la misma línea de extender la protección del ciberespacio nacional a través de los organismos públicos, el CSIRT de Gobierno participó de la elaboración de la normativa de ciberseguridad de la Superintendencia de Casinos de Juego.

6. Posibles tendencias en amenazas para 2022

Por supuesto que nadie puede saber qué pasará durante 2022, y todos los actores de la esfera digital debemos estar preparados para cualquier táctica y tipo de ataque. Pero en el ambiente de la ciberseguridad, estas son algunas de las tendencias que se mencionan bastante entre los expertos y firmas del rubro para el próximo año.

Continuará el crecimiento de los ataques a las cadenas de suministro. Esta modalidad de ataque permite comprometer a varias organizaciones, por lo que los cibercriminales pueden acceder a cientos o incluso miles de víctimas con ingresar a los sistemas de una empresa y, por ejemplo, infectar una actualización de seguridad, la que será descargada con toda confianza por parte de sus clientes. Para reducir este riesgo, es necesario administrar accesos y permisos diferenciados según el tipo de usuario, buscando llegar lo más cerca posible hacia una arquitectura de confianza cero, minimizar el acceso a datos sensibles, identificar riesgos internos y crear reglas estrictas para el uso de dispositivos.

Aumenta la digitalización del mundo físico y con ella, los riesgos: La creciente integración entre los ámbitos de las tecnologías de la información (IT) y operativas (OT) representa una fuente de automatización y eficiencia para muchas tareas productivas, pero también involucra riesgos, ya que hace posible la entrada de ciberdelincuentes procesos productivos clave, como servicios básicos, o el control de maquinaria peligrosa, por ejemplo, pudiendo provocar lesiones o muerte. Es clave, por ende, que las organizaciones entiendan estos riesgos e implementen estrategias que consideren la integración entre los mundos digital y físico, además de mantener siempre sus sistemas actualizados y contemplar zonas de seguridad especiales para los sistemas que controlan maquinaria física.

Mayor penetración del phishing a través de redes sociales: El phishing, o sea, cuando los delincuentes le hacen creer a un usuario que un mensaje malicioso es legítimo, y así logran extraer información o dinero, es el ciberataque más común y exitoso. Sin embargo, no por eso deja de sofisticarse, y expertos en el mundo de la ciberseguridad prevén que cada vez serán más y mejores los ataques de phishing que lleguen a las personas a través de redes como Twitter o Linkedin, por ejemplo, con falsas ofertas de empleo, para convencer a los trabajadores de una empresa de hacer clic o descargar programas maliciosos, dando acceso a los delincuentes a una compañía en específico. Con la ayuda del *machine learning*, los mensajes peligrosos pueden ser cada día más convincentes y por eso tenemos siempre que estar muy atentos cuando recibamos mensajes no solicitados.

Ransomware sigue siendo tendencia, pero se volverá más dirigido: Otra tendencia a la que apuntan varios expertos es a una sofisticación del ransomware (tipo de ataque que "secuestra" la información o datos valiosos de una persona o empresa, los cifra, y exige un rescate para entregar la clave para poder volver acceder a ellos). Estos ataques han sido noticia los últimos años, siendo

víctimas empresas grandes y pequeñas, e incluso algunos gobiernos locales en ciudades de EE.UU. La apuesta es a que esto seguirá, pero que veremos una especialización de algunos delincuentes en ataques de ransomware menos masivo y mejor diseñado para apuntar a grandes empresas y gobiernos puntuales, de forma de resultar más exitosos con estos "peces gordos". Además, se cree que estos ataques dirigidos aprovecharán mejor todas las formas de extorsión posibles, combinando amenazas como la destrucción de los datos secuestrados con la divulgación de información confidencial de los clientes y proveedores de la empresa

La actualización e instalación de parches sigue siendo demasiado lenta: Si bien todos los días sitios especializados, desarrolladores de software, expertos y empresas de ciberseguridad identifican vulnerabilidades de seguridad y desarrollan parches y estrategias para mitigarlas (muchas de las cuales compartimos también nosotros en nuestro sitio csirt.gob.cl), ha sido demostrado en numerosas ocasiones y con casos muy bullados (como vulneraciones en el último año a Solarwinds y Exchange) que las organizaciones tardan demasiado en instalar las actualizaciones y parches que eliminan estas vulnerabilidades, existiendo así numerosas víctimas que perfectamente pudieron haber estado protegidas. Como es la tendencia, creemos que lamentablemente estos retrasos solo se incrementarán, por lo que reiteramos el llamado a mantener siempre su software actualizado.