CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Informe anual de gestión 2020

División de Redes y Seguridad Informática

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Índice

1.- Presentación

2020 fue un año de múltiples desafíos. Aún no descendía la intensidad de la amenaza hacktivista cuando comenzó a brotar una campaña global de desinformación de la mano de la pandemia producto del covid-19. Internet se repletó de fake news en sitios web y redes sociales, y con ello se multiplicaron las campañas de phishing. CSIRT respondió con tres medidas prácticas para hacer frente a esta incesante ola de phishing: en primer lugar, puso en funcionamiento un desarrollo propio denominado "La Campana", que permitió advertir la potencial creación de sitios fraudulentos creados en NIC.CL; junto a lo anterior disponibilizó un manual de resolución de conflictos por nombres de dominios; y finalmente elaboró un protocolo frente a incidente de spear phishing.

En la medida que la sociedad comenzó a utilizar las cuarentenas como medidas sanitarias frente al coronavirus, se multiplicó el uso de herramientas de video-conferencia como Zoom. La imprevista y popularidad del uso de esta plataforma no solo brindó una enorme ventaja para la continuidad del trabajo, la educación y entrega de servicios. Lamentablemente también fue explotada por los atacantes para interrumpir transmisiones, obtener datos y provocar inseguridad. La inexperiencia en el uso de las video conferencias llevó a CSIRT a la generación de campañas educativas y de un informe recomendaciones para el uso adecuado y seguro de estas plataformas.

Cuando las medidas sanitarias pasaron de ser medidas transitorias a permanentes, el gobierno y el congreso realizaron un esfuerzo en tiempo record para facilitar el trabajo e distancia. Acompañando este importante logro, CSIRT compartió con la comunidad un protocolo para la implementación de un teletrabajo seguro, dirigido tanto a funcionarios públicos como a entidades privadas.

A partir de abril CSIRT inició una serie de publicaciones de perfil técnico-científico en la que se abordaron y analizaron incidentes recurrentes en el ámbito de la ciberseguridad. En total fueron 26 investigaciones sobre Análisis de Amenazas Cibernéticas, escritas por especialistas y colaboradores vinculados a nuestra institución, las que abordaron temas diversos y generales como phishing, ransomware, malware, defacement, emotet, DDoS, entre otros.

Durante todo el 2020 se realizaron campañas de concientización para educar preventivamente ante posibles riesgos cibernéticos, así como advertir sobre incidentes y reforzar recomendaciones de seguridad cibernética. La política de buenas prácticas aplicada en el CSIRT tuvo como eje central entregar un mensaje simple y didáctico a todos los grupos, enfatizando en algunas oportunidades el autocuidado en poblaciones más vulnerables en el uso de internet, como los niños, las mujeres y los adultos mayores. En el marco de esas iniciativas de concientización tuvo lugar la revista "Cibersucesos", la que está destinada a abordar en mayor profundidad algunos de los contenidos de esas campañas, así como a destacar aspectos relevantes de investigaciones, la acción de grupos que se dedican a la ciberseguridad, la cooperación internacional y la colaboración local en la materia.

En el inicio del segundo semestre, CSIRT firmó más de medio centenar de acuerdos de colaboración con entidades nacionales y firmas extranjeras presentes en nuestro país para acercar la ciberseguridad entre los sectores público y privado. Estos acuerdos buscaron fomentar y coordinar acciones en ciberseguridad, algunos de los cuales se vieron reflejados en medidas de evaluación, intercambio de indicadores de compromiso, información y buenas prácticas, así como la colaboración directa con entidades afectadas en algún incidente.

Septiembre fue el inicio de un período complejo en materia de ciberseguridad. Banco Estado, la institución bancaria más grande del país, fue víctima de un ataque cibernético. CSIRT cumplió un rol relevante en la advertencia y gestión comunicacional del incidente. La información transmitida en forma oportuna permitió a otras entidades revisar y activar sus protocolos de seguridad para evitar la propagación del mismo.

En seguida se precipitó otro incidente, esta vez dentro de Gobierno Digital, el cual fue coordinado con la propia institución a la que se le brindó asesoría y guía para mitigar y mejorar sus estándares, especialmente en la plataforma de Clave Única. El incidente derivó en la formalización de un atacante y la contención de la información exfiltrada.

CSIRT preparó un protocolo especial con miras a un posible estallido social 2.0 durante el mes de octubre, el cual se limitó finalmente a una serie de incidentes hacktivistas de menor visibilidad, lamentablemente algunos de ellos dirigidos a instituciones del área de salud. Durante todo el 2020, se ensayaron con las diferentes organizaciones del Estado diferentes protocolos de seguridad tanto para la transmisión de la información como para la activación de alertas, dependiendo del contexto.

CSIRT clausuró el año con un gran simposio en línea para los funcionarios públicos del Estado. Con la presencia del Subsecretario del Interior y el apoyo de panelistas invitados de Chile y el América Latina, se desarrolló esta novedosa actividad de casi 9 horas de duración, dirigido, producido y conducido por los miembros de la organización.

Durante los últimos meses se reactivó la plataforma MISP con las entidades en colaboración a nivel nacional, así como en el intercambio de información con el MISP de la OEA e Israel.

A nivel internacional se realizaron los primeros acercamientos con Reino Unido y Estonia, se reforzó el intercambio con España, Australia e Israel, y se estrecharon relaciones con países del concierto de América Latina, como República Dominicana, Colombia, Argentina, México, Uruguay y Paraguay.

Un año que cierra con la convicción y búsqueda permanente que estamos contribuyendo a la formación de un ecosistema más abierto más libre más seguro y más resiliente, pero sobre todo siendo parte de la formación permanente de una cultura de ciberseguridad

2.- Resumen ejecutivo

El presente informe tiene como objetivo presentar un resumen de la gestión del CSIRT durante el año 2020. Para esto, se entrega un reporte con el total de los tickets procesados, un análisis con el detalle de los tipos de incidentes reportados y se muestra el porcentaje de tickets que se reportaron al sector público y privado.

Junto con esto, el informe anual da cuenta de los informes de campañas de phishing, malware, creación de sitios fraudulentos, vulnerabilidades y ataques de fuerza bruta informados mediante los canales digitales del CSIRT a la ciudadanía. Para lograr informar oportunamente y las distintas amenazas a los que están expuestas las personas, el CSIRT de Gobierno recibe la colaboración de personas e instituciones que notifican estos incidentes. A todos ellos, queremos, a través de este medio, darles nuestros agradecimientos y reconocerlos.

El año 2020 estuvo marcado por nuevas amenazas cibernéticas. Los cambios vividos durante este año demostraron la importancia de la ciberseguridad y la visibiliza de una manera positiva para el ecosistema, pero sin olvidar nunca que las formas de ataque cada di son más sofisticadas dinámicas y dirigidas, por tanto, tenemos que representarnos las tendencias de los vectores de ataque. Por esta razón, el CSIRT realizó un análisis de los peligros que nos pueden deparar el 2021, los que les daremos a conocer en este documento.

3.- Alcances del Informe

La información contenida en este informe proviene del proceso de notificación de incidentes de ciberseguridad del CSIRT, del trabajo de investigación en el análisis de casos, de la proyección de esos resultados y de las medidas preventivas aplicadas internamente y a terceros como parte de la misión de esta institución, y de la colaboración entre organismos públicos y privados vinculados con CSIRT. De igual forma, la data expuesta contabiliza la información pública emitida durante el período 2020.

El contenido del siguiente informe reúne:

- ✓ El análisis de la gestión de tickets anual.
- ✓ La distribución de tickets analizados.
- ✓ El análisis de los tipos de incidentes de acuerdo a las 10 variables utilizadas seleccionadas.
- ✓ El reconocimiento a quienes colaboraron con información sobre campañas de phishing, malware, vulnerabilidades y sitios fraudulentos.
- ✓ Tendencias cibernéticas del año 2021.

4.- Análisis anual de los tickets y tipos de incidentes

Ante las diversas amenazas y peligros que abundan en el ciberespacio, el Equipo de Respuesta Ante Incidentes de Seguridad Informática, CSIRT, notifica a instituciones públicas y privadas de aquellos riesgos que pueden afectar a sus sistemas.
Entre el 1 de enero y el 31 de diciembre del año 2020, se generaron 15.321 ticket, aumentando la gestión del equipo CSIRT en un 56,8% respecto al año 2019. 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.

Ese total de tickets se desglosa en las siguientes categorías:

N°	Tipos de ticket	Código	Cantidad
1	Recopilación de Información	3R00	5504
2	Vulnerabilidad	9V00	3353
3	Fraude	8F00	2211
4	Código Malicioso	2C00	1468
5	Información de seguridad de contenidos	7S00	1231
6	Operaciones Ciberseguridad CSIRT	19OC	662
7	Disponibilidad	6D00	624
8	Intrusión	5I00	111
9	Contenido Abusivo	1A00	107
10	Intentos de Intrusión	4I00	50
	TOTAL		**15321**

*Matriz de clasificación de incidentes de ENISA, Agencia de la Unión Europea para la Ciberseguridad.

Incidentes distribuidos por mes

Código	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Total
3R00	899	772	475	371	295	322	353	237	198	402	575	605	**5504**
9V00	270	357	386	422	435	417	299	129	142	167	228	101	**3353**
8F00	203	135	204	236	189	115	323	310	256	107	95	38	**2211**
2C00	217	195	103	24	87	133	129	104	56	158	131	131	**1468**
7S00	88	119	119	179	92	92	71	123	91	49	82	126	**1231**
19OC	6	7	17	27	25	46	65	134	69	98	90	78	**662**
6D00	149	88	122	45	15	16	28	18	38	94	6	5	**624**
5I00	0	0	17	56	5	4	4	2	1	17	2	3	**111**
1A00	5	2	1	0	0	3	2	3	11	20	12	48	**107**
4I00	2	26	4	7	3	2	1	2	1	0	1	1	**50**
Total	1839	1701	1448	1367	1146	1150	1275	1062	863	1112	1222	1136	**15321**

Tabla 1.- Incidentes distribuidos por mes

4.1 Tipos de incidentes

Para complementar la información entregada, presentamos distintos gráficos que muestran los tipos de incidentes que fueron registrados por el CSIRT durante 2020, y su comportamiento.

Así, dentro de las 10 categorías, "Recopilación de Información" y "Vulnerabilidad" representaron el mayor porcentaje de incidentes con un 35,9% y un 22%, respectivamente. En el contexto de las sucesivas crisis social y sanitaria, la información adquirió un carácter crítico, no solo en su esencia por tratarse de datos que pueden revelar información relevante de una entidad y de las personas vinculadas a ésta para un eventual ataque, sino como un medio que puede ser manipulado para crear incertidumbre y confusión entre los usuarios de sistemas informáticos, lo que permite explotar vulnerabilidades o infiltrar organizaciones.

En el caso de "Vulnerabilidades", es fundamental tomar consciencia de que la falta de actualizaciones en aplicativos y la deficiencia de las políticas de seguridad o la ausencia de éstas, llevan a las instituciones a ser blanco fácil de ataques cibernéticos. Por lo tanto, para evitar que continúe aumentando el número de incidentes de seguridad informática, el CSIRT recomienda tomar las medidas preventivas correspondientes y de forma oportuna.

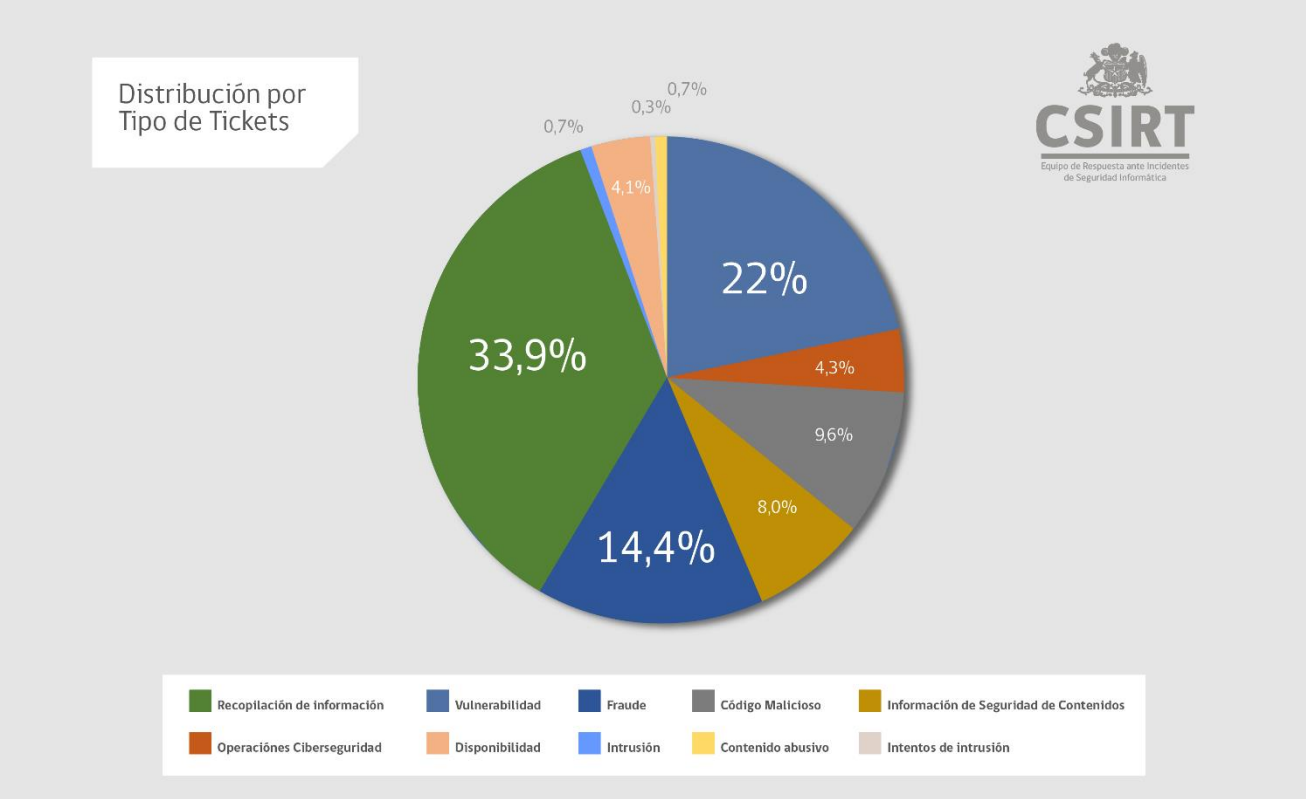

Imagen 1.- Distribución por tipo de tickets

3.1.1 Tickets mensuales

En el siguiente gráfico podemos apreciar cómo fue el comportamiento de los incidentes mensualmente. Cabe destacar que, a raíz del estallido social, se produjo durante el último trimestre del año 2019 un incremento de ciberataques a instituciones del Estado, lo que puede explicar las cifras de enero y que luego disminuyen y vuelven a aumentar desde la llegada del Coronavirus a nuestro país.

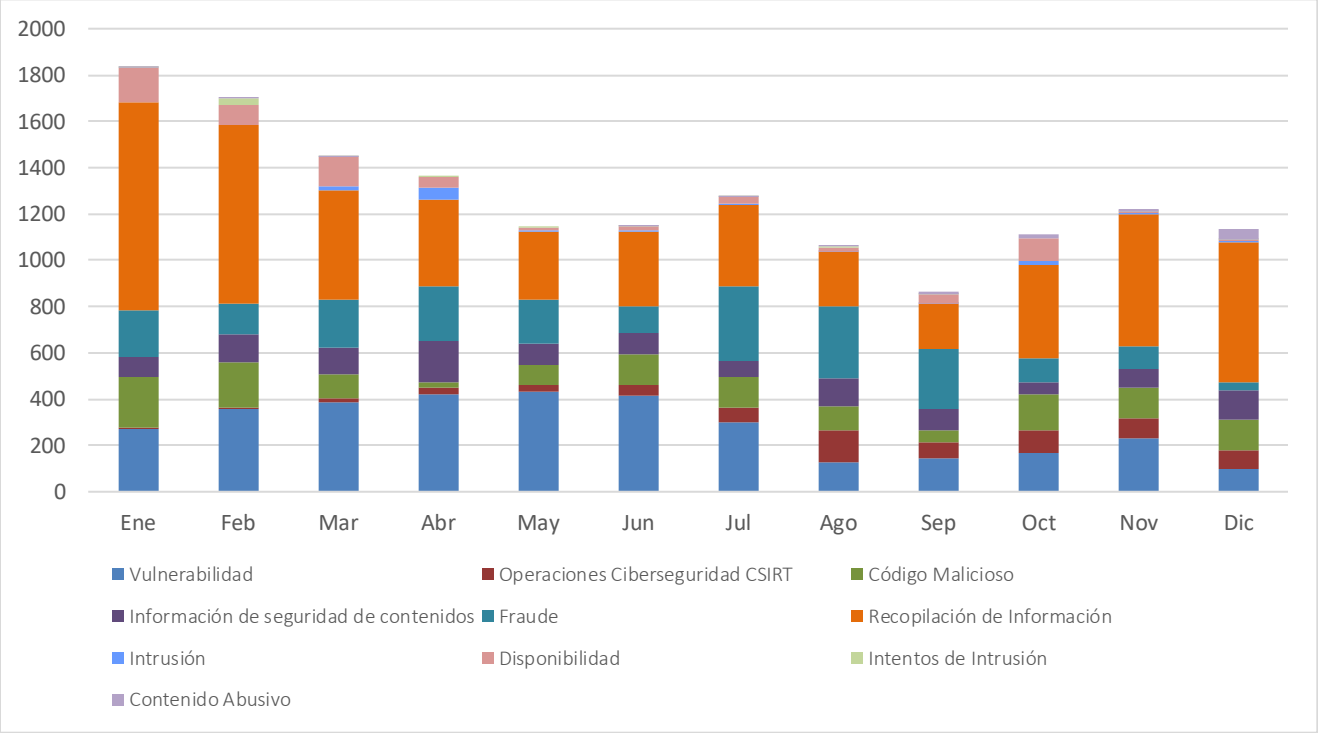

Imagen 2.- Distribución tendencial de tickets

3.1.2 Tipo de incidente: Vulnerabilidades

Las vulnerabilidades fueron uno de los incidentes más frecuentemente reportados por el CSIRT, siendo detectadas producto de un permanente trabajo de monitoreo. Llegando a un máximo de 435 incidentes y un mínimo de 101. El comportamiento en esta curva hace suponer que a principios de año existía una falta de actualización de los sistemas. Por esto, es clave recordar la importancia de descargar las respectivas actualizaciones y parches de los proveedores para evitar que los sistemas sean vulnerados.
CSIRT, durante el 2020, reporto más de 2.300 vulnerabilidades de distinta criticidad a las instituciones de Gobierno por la vía de informes de vulnerabilidad.

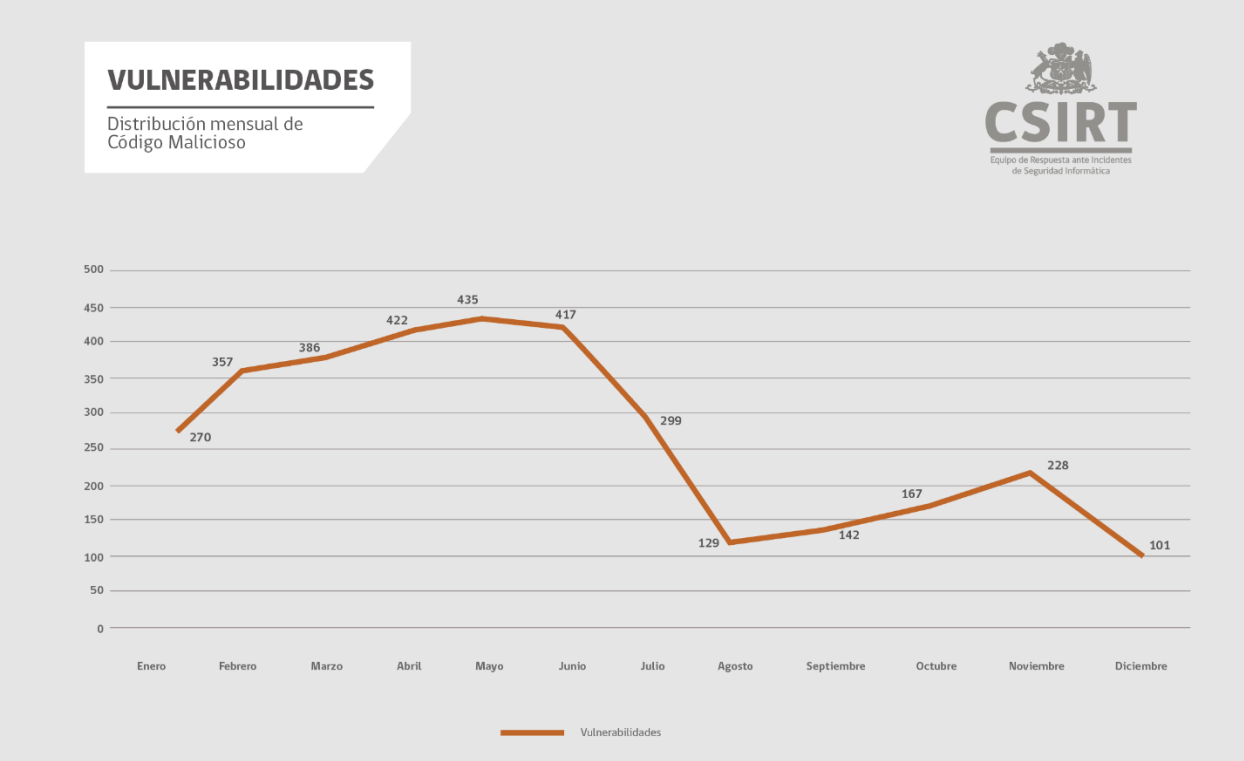

Imagen 3.- Distribución mensual de vulnerabilidades

3.1.2 Tipo de incidente: Operaciones Ciberseguridad CSIRT

Esta categoría contiene incidentes que están directamente vinculados a la operación interna del CSIRT sobre la Red de Conectividad del Estado, especialmente con el bloqueo y desbloqueo de IP de acuerdo a su reputación. Su operación, limitada al sector público, se manifiesta en acciones mayoritariamente coordinadas, destacándose en agosto el peak de eventos.

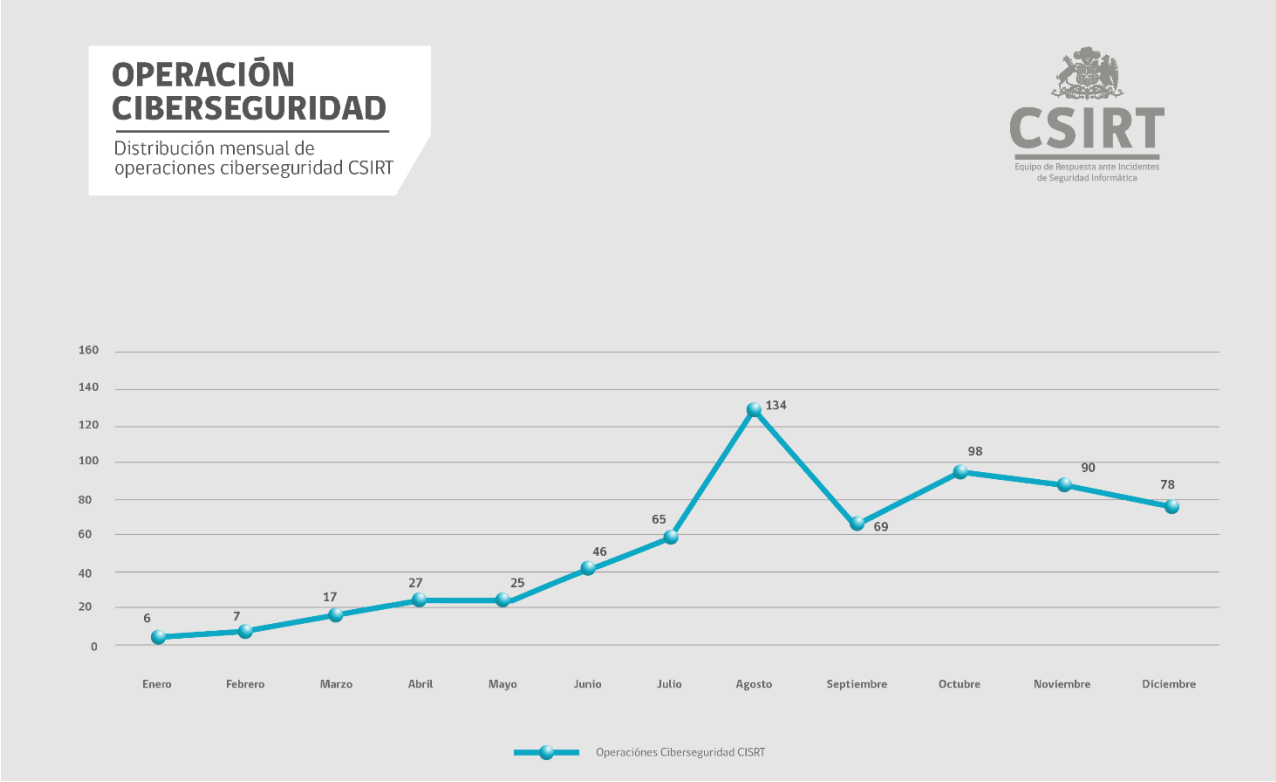

Imagen 4.- Distribución mensual de Operaciones Ciberseguridad CSIRT

3.1.3 Tipo de incidente: Código malicioso

Una caída en los ataques de código malicioso se vio reflejada a partir de febrero, indicador que continuó a la baja durante los siguientes meses, hasta abril. Lamentablemente, se aprecia un leve repunte en octubre, que puede ser a causa del primer aniversario de la crisis social.

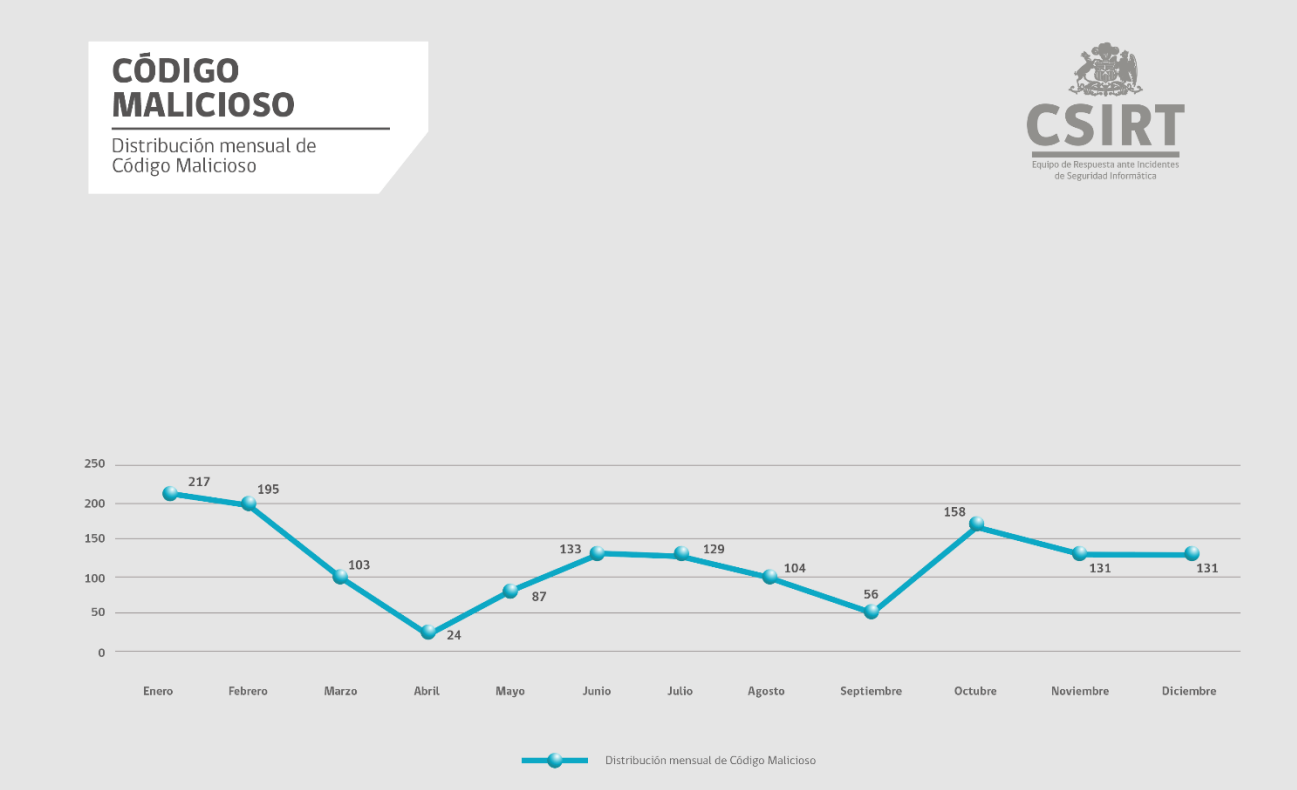

Imagen 5.- Distribución mensual de Código Malicioso

3.1.4 Tipo de incidente: Información de Seguridad de Contenidos

Este tipo de incidente representa una proporción baja de las amenazas que afectan a las instituciones del Estado, según los tickets registrados. No obstante, se presenta una importante alza en abril (de cerca de 50% contra el mes anterior), para luego retomar una tendencia descendente.

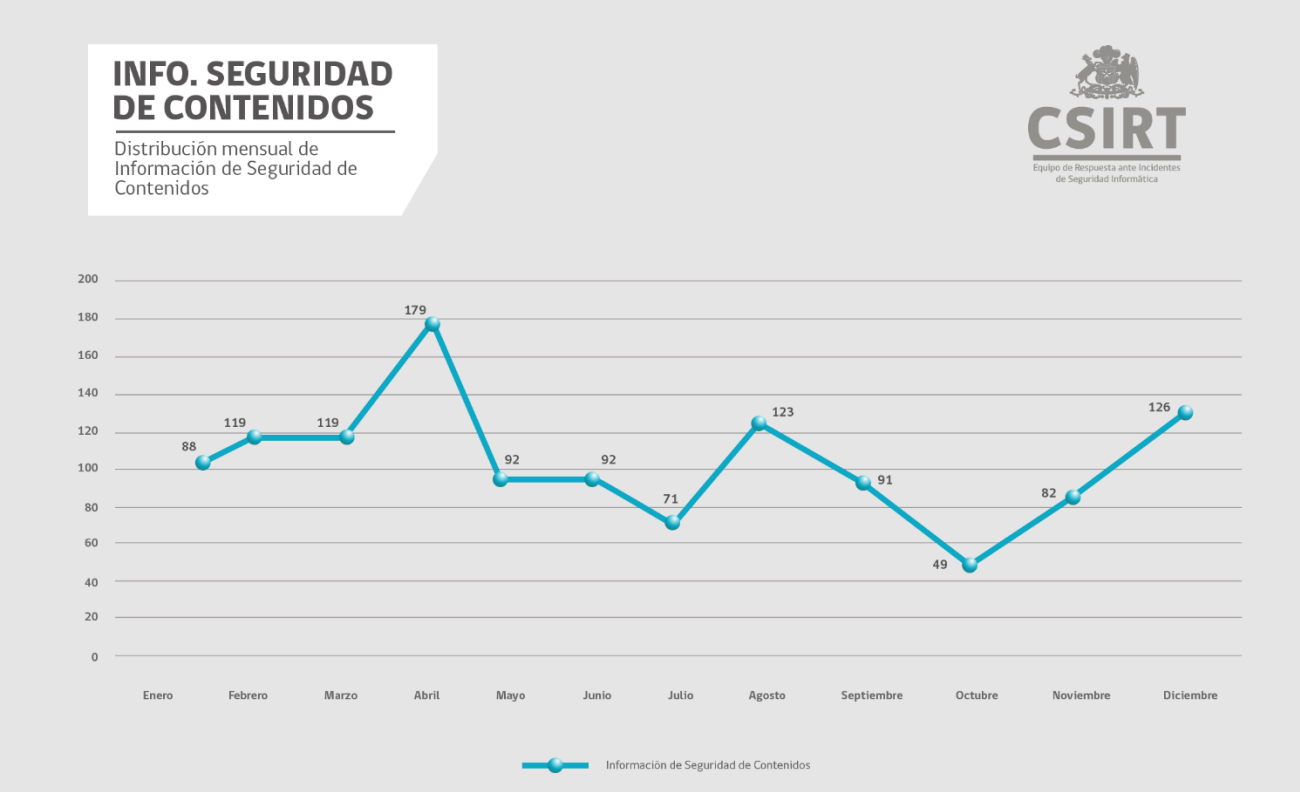

Imagen 6.- Distribución mensual de Información de Seguridad de Contenidos

3.1.5 Tipo de incidente: Fraude

Los fraudes como los phishing y spear phishing son las principales técnicas para penetrar a un sistema. Los ciberdelincuentes se aprovechan de la falta de conocimiento de los usuarios para acceder a sus instituciones. Este año, la tendencia demuestra un peak en julio, que corresponde al momento más álgido del coronavirus, lo que permitió desplegar campañas de phishing relacionadas con la pandemia.

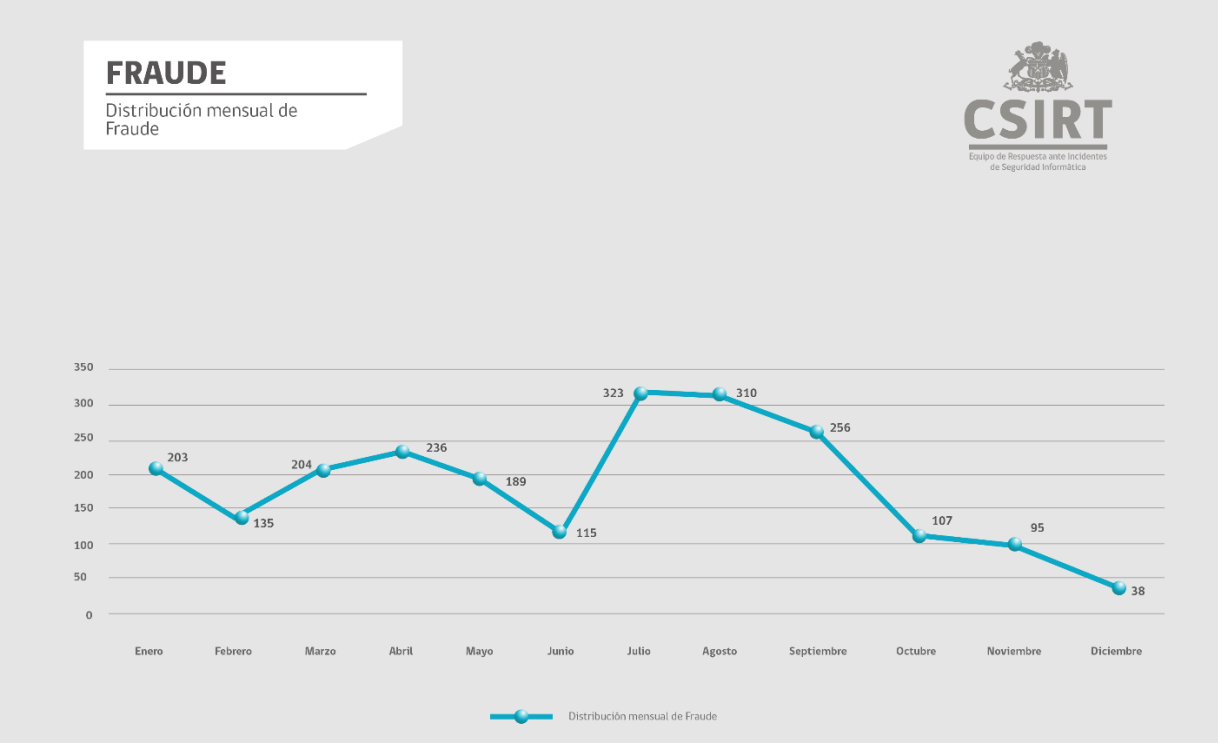

Imagen 7.- Distribución mensual de Fraude

3.1.6 Tipo de incidentes: Recopilación de Información

La recopilación de información se relaciona con ataques de exploración, es decir, se envían solicitudes a un sistema para descubrir puntos débiles, incluyendo algún tipo de proceso de prueba para recopilar información sobre hosts, servicios y cuentas. Durante 2020 este fue el tipo de incidente más recurrente. Los registros fueron disminuyendo desde enero, fecha en que se observaron 899 incidentes.

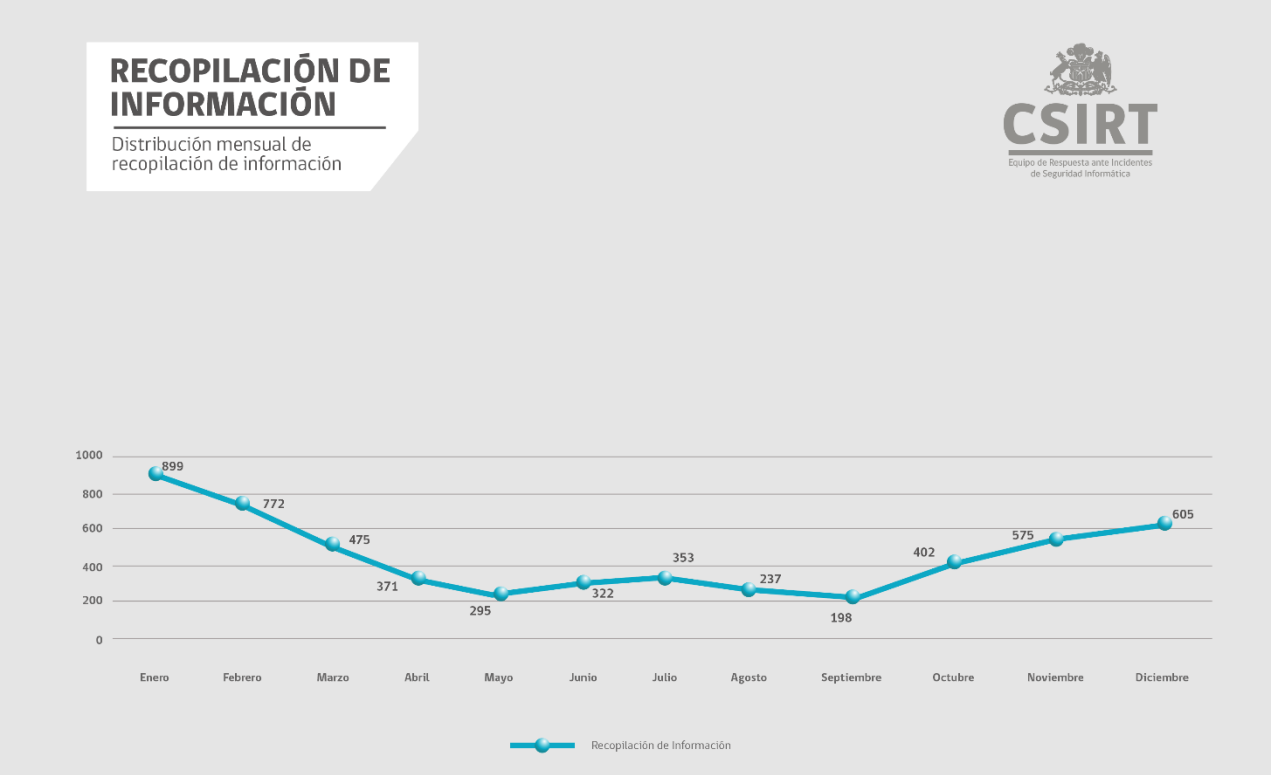

Imagen 8.- Distribución mensual de Recopilación de Información

3.1.7 Tipo de incidentes: Intrusión

La Intrusión se refiere principalmente a "Credenciales Recuperadas". Esta categoría muestra solo las que fueron detectadas, y esto puede suceder mucho tiempo después de que la intrusión comenzó. Diferentes factores explican esto, entre otros, la forma en que se realiza el monitoreo de seguridad (aleatorio, en clusters o por requerimiento), y si fue registrado por una institución o una persona, entre otros.

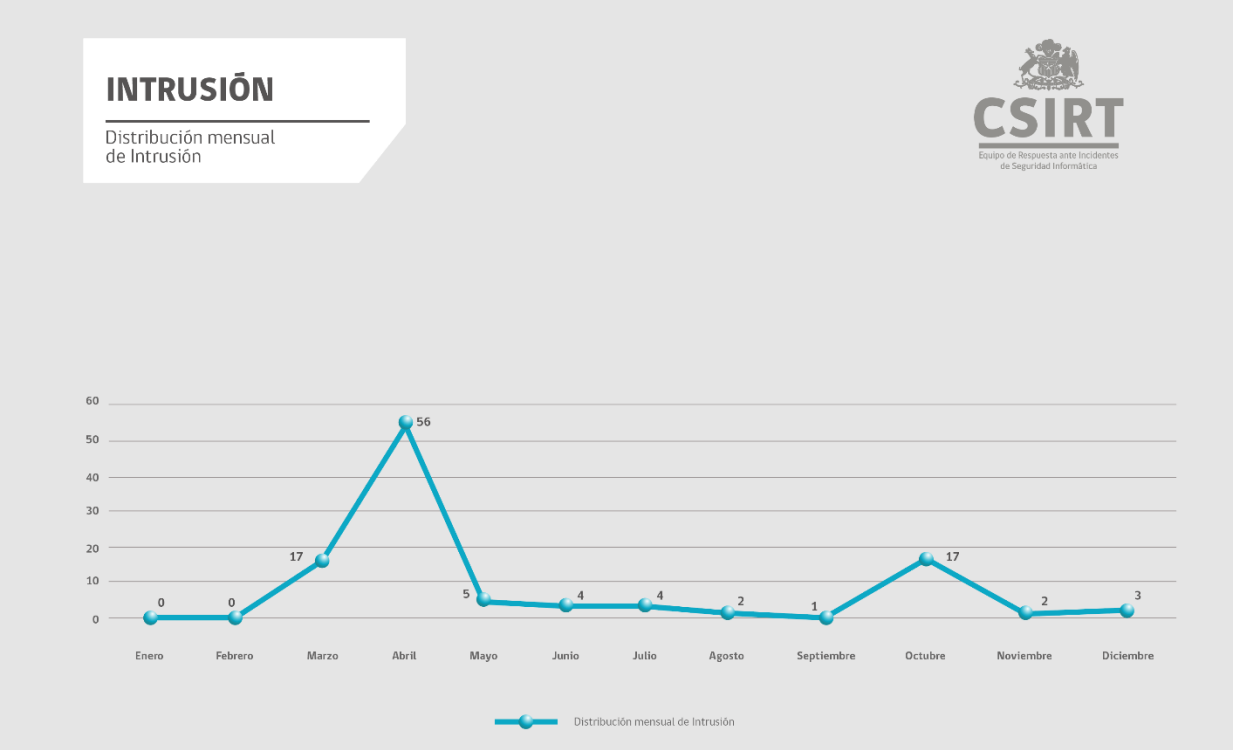

Imagen 9.- Distribución mensual de Intrusión

3.1.8 Tipo de incidente: Disponibilidad

Asociados a los ataques de denegación de servicio, en enero se registraron los índices más altos de este tipo de incidente, debido probablemente a la actividad hacktivista contra instituciones de gobierno entre octubre de 2019 y que se arrastró hasta principios de 2020. Posteriormente, hay un leve aumento en octubre, aunque en este caso el mayor porcentaje de estos incidentes están asociados al sector privado.

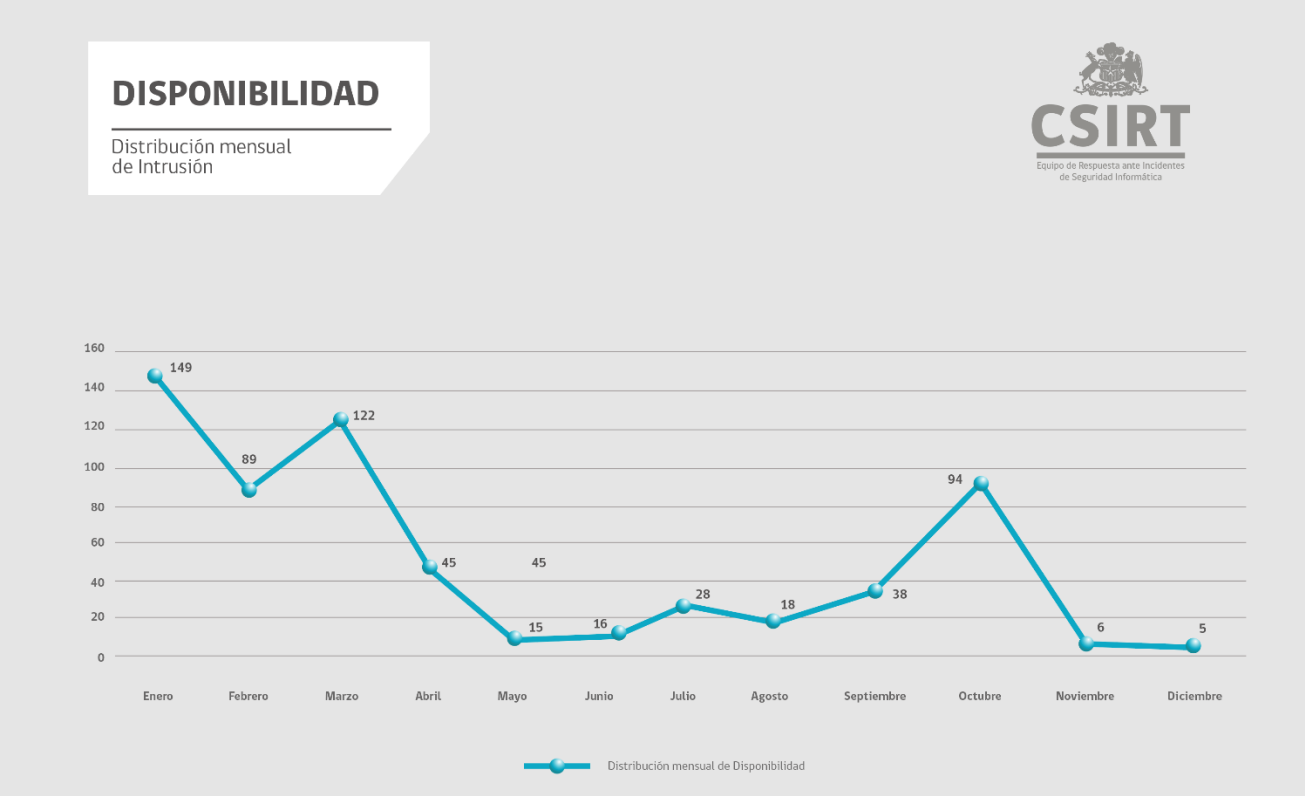

Imagen 10.- Distribución mensual de Disponibilidad

3.1.9 Tipo de incidente: Intentos de Intrusión

Se tratan de los intentos de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas. Representa uno de los ataques menos utilizados, especialmente en el sector privado, donde no se registran tickets asociados. De igual manera, las instituciones públicas no reciben frecuentemente ataques de este tipo.

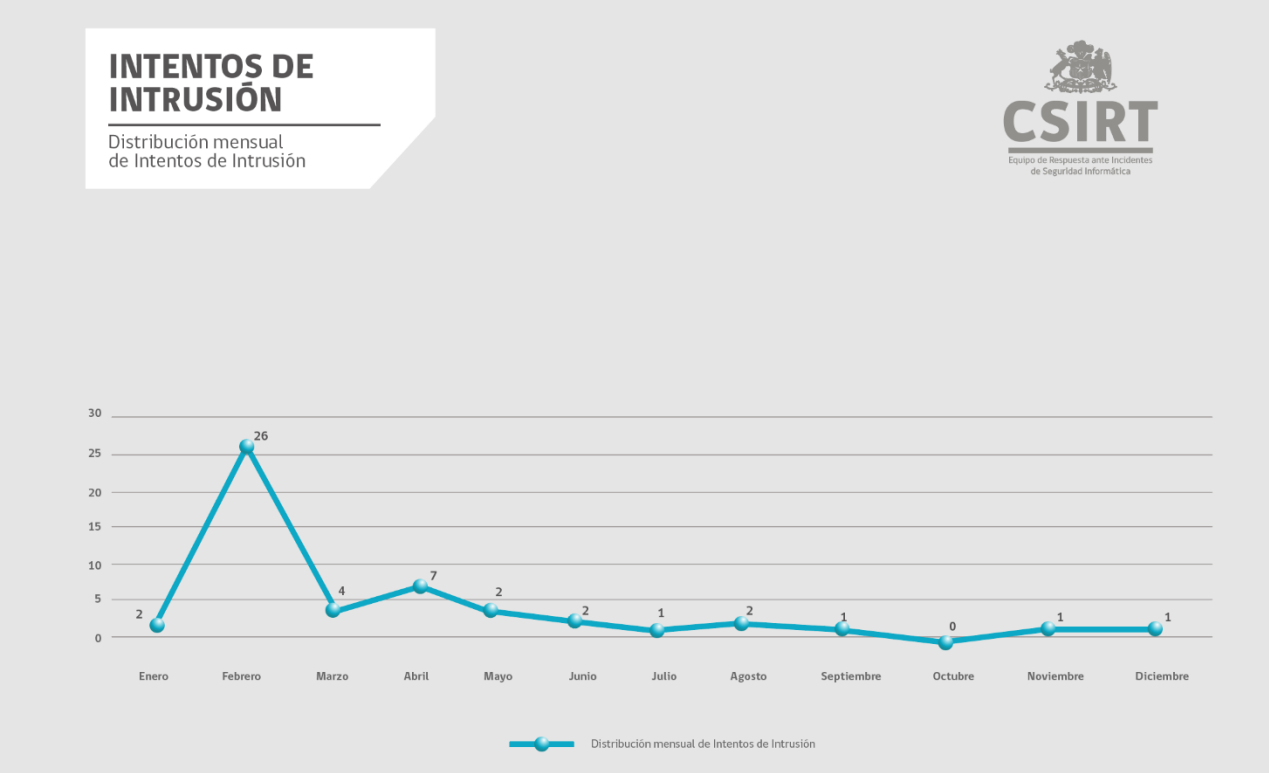

Imagen 11.- Distribución mensual de Intentos de Intrusión

3.1.10 Tipo de incidentes: Contenido abusivo

Este tipo de incidente no representa una gran amenaza en términos numéricos, sin embargo, al experimentar un alza en el último trimestre se podría suponer que las instituciones no están tomando las suficientes medidas preventivas para evitar estos ataques, que afectan directamente su imagen. Los tickets ingresados están relacionados al redireccionamiento de alguna URL que tenga contenido como abusivo como pornografía, violencia u otros.

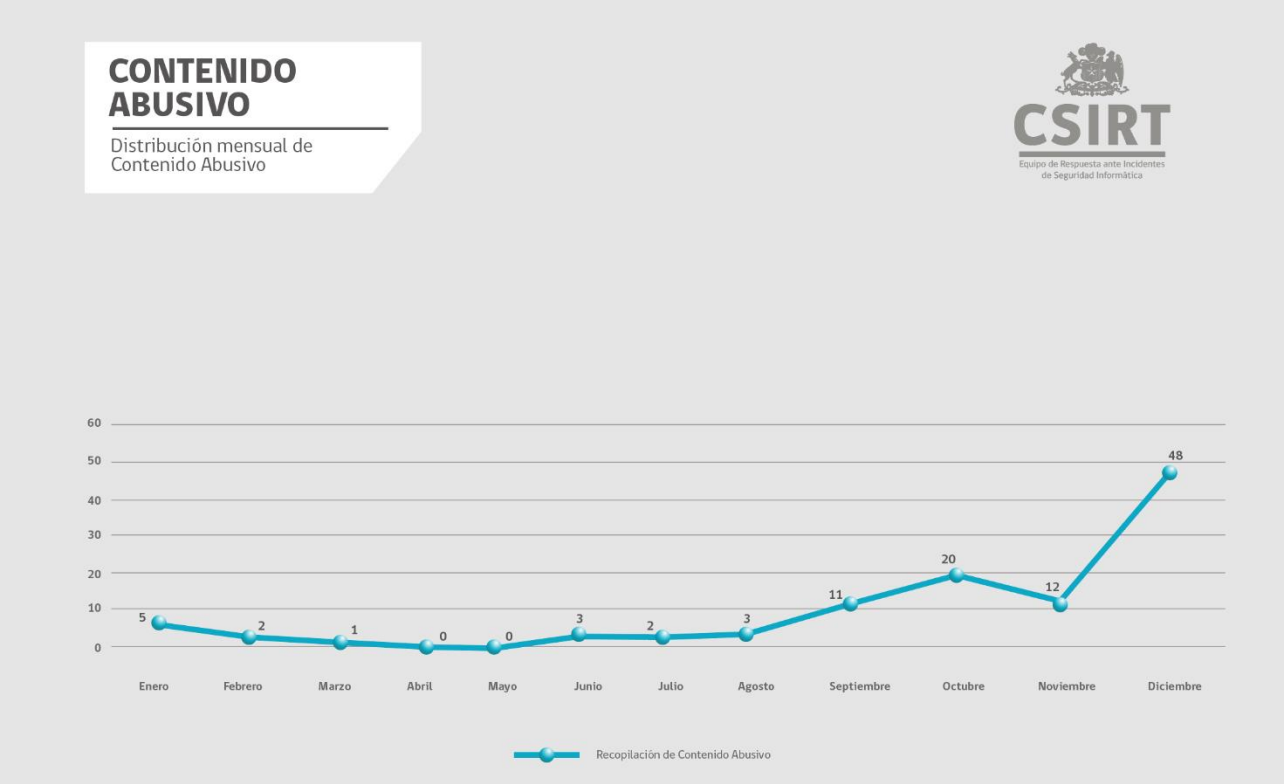

Imagen 12.- Distribución mensual de Contenido Abusivo

3.2 Tickets públicos y privados

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, se han impulsado una serie de iniciativas que permitan fortalecer esta relación, comunicación y trabajo en equipo.

El intercambio de información y buenas prácticas juegan un rol fundamental. Por eso, alertar de situaciones o incidentes riesgosos que se detectan en organizaciones privadas es un compromiso que adquirió el CSIRT. Es así como de los 15.321 tickets registrados, un 30% de ellos corresponde al sector privado, como muestra el siguiente gráfico:

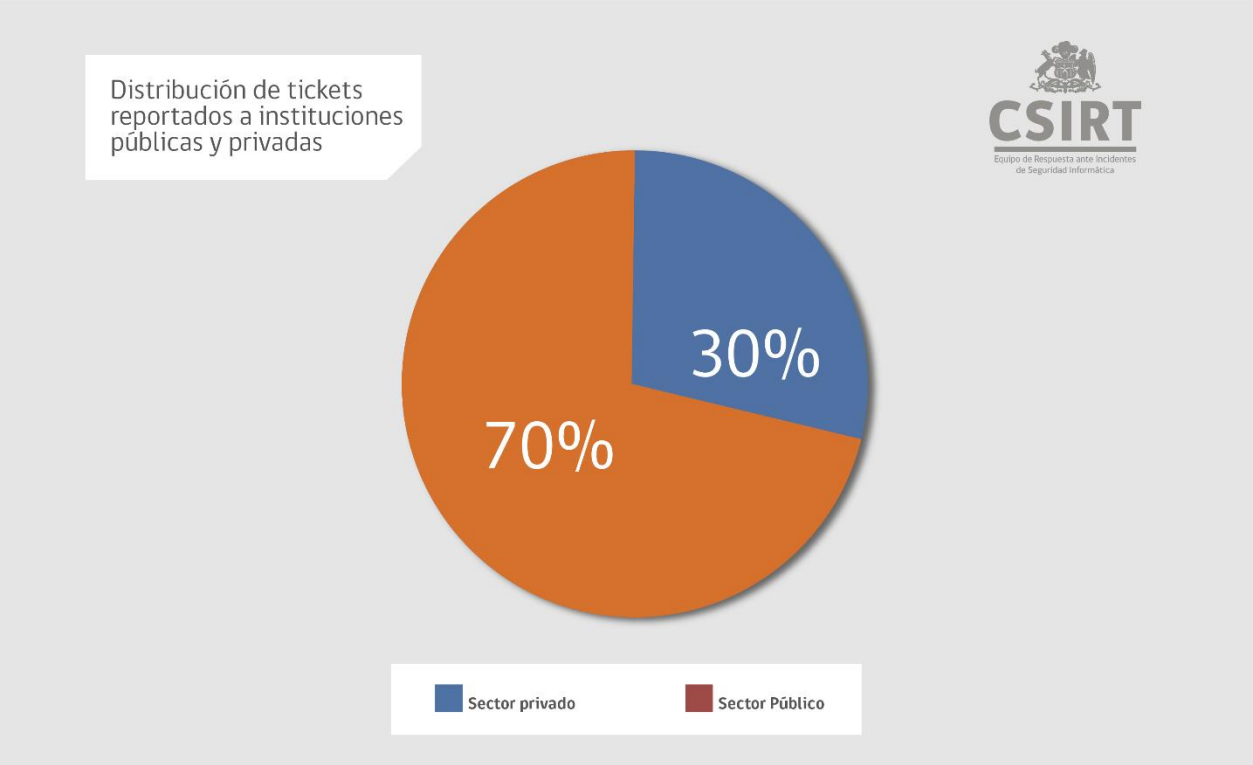

Imagen 13.- Distribución de tickets reportados a instituciones públicas y privadas

A continuación, detallamos el número de incidentes que corresponden a cada sector y entregamos un gráfico comparativo del comportamiento mensual.

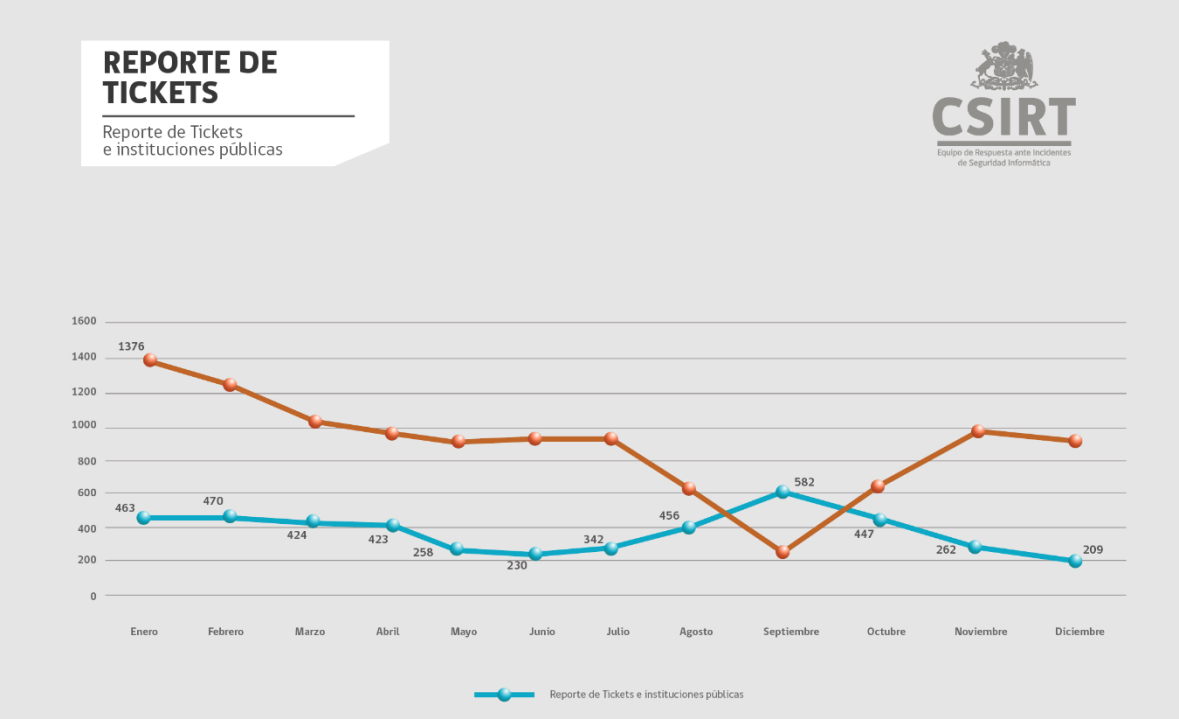

Imagen 14.- Reporte de tickets a instituciones públicas y privadas

Mes	Sector Privado	Sector Público	Total
Enero	463	1376	1839
Febrero	470	1231	1701
Marzo	424	1024	1448
Abril	423	944	1367
Mayo	258	888	1146
Junio	230	920	1150
Julio	342	933	1275
Agosto	456	606	1062
Septiembre	582	281	863
Octubre	447	665	1112
Noviembre	262	960	1222
Diciembre	209	927	1136
Total	**4566**	**10755**	**15321**

Tabla 15.- Tickets mensuales por sector

4. Reconocimiento colaboradores del año

Durante todo el 2020, como lo lleva haciendo desde sus inicios, el CSIRT informa regularmente a la ciudadanía de campañas de phishing, malware, creación de sitios fraudulentos, ataques de fuerza bruta y entrega el reporte de vulnerabilidades. Es así, como durante todo este año, se publicaron 1.297 alertas, las que se desglosan de la siguiente manera:

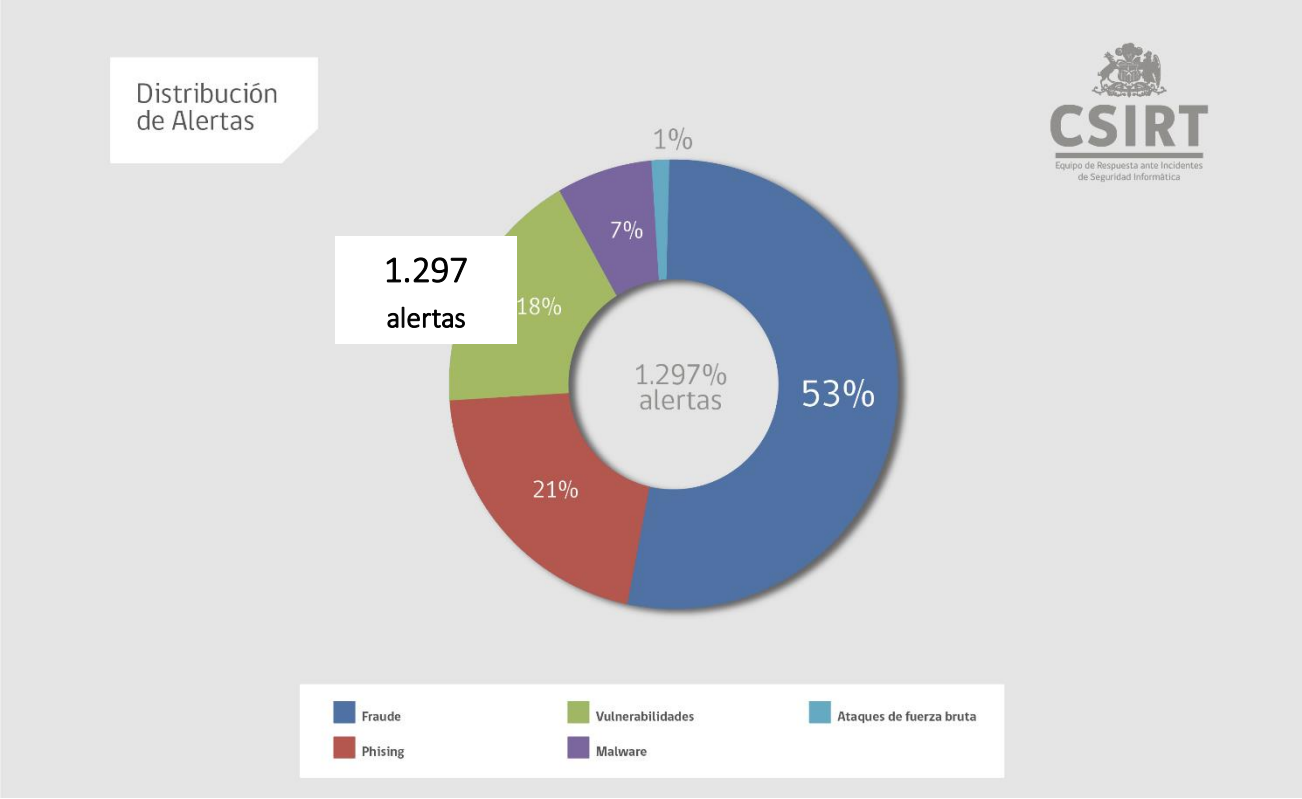

Imagen 16.- Distribución alertas

Tipos de alertas	
Fraude	693
Phishing	267
Vulnerabilidades	239
Malware	85
Ataques de Fuerza Bruta	13
Total	**1.297**

Esta información es obtenida mediante distintas fuentes y análisis propios del CSIRT. El siguiente es un listado de las 20 personas que más han colaborado para mejorar la seguridad informática en instituciones y organismos públicos del Estado, y que damos a conocer cada semana en nuestro Boletín de Seguridad Cibernética.

Agradecemos el trabajo de cada una de estas personas que contribuyen a mantener un ciberespacio más ciberseguro. Para reportar algún incidente se pueden utilizar los siguientes canales: www.csirt.gob.cl / +(562) 2486 3850

5. Tendencias de amenazas para 2021

Durante 2020, las amenazas cibernéticas han observado un aumentado considerable que perjudican transversalmente a todas las organizaciones y personas que tiene acceso a internet. Las amenazas no se circunscriben a naciones específicas. Traspasan con facilidad las fronteras y explotan los riesgos que encuentran sin discriminar la infraestructura digital a la que se enfrentan.

Para 2021, se supone que la cantidad de incidentes relacionados a la seguridad informática irán en aumento tanto en cantidad como en sofisticación. A continuación, analizaremos cada una de las principales amenazas del año que se espera cobren mayor relevancia este año que comienza.

5.1 Deepfakes para el fraude y el chantaje

Consiste en un video en que se reemplaza o crea un rostro distinto y altamente realista a través de machine learning (específicamente, al principio eran realizados usando deep learning, de ahí su nombre).

Esta técnica se puede usar para diseminar noticias falsas, haciendo parecer que una persona dijo algo que no, o para crear contenido pornográfico sin autorización de la persona dueña de la cara que se superpone al video original, lo que puede ser usado para humillarla y chantajearla.

5.2 Peligros de las configuraciones erradas en la nube

Debido a que los servicios de infraestructura en la nube se han convertido en una gran opción para mantener las operaciones durante la pandemia, Gartner estima para el año 2021 un crecimiento del 29% en las ventas de este servicio. Por tanto, las filtraciones de información desde la nube podrían crecer, debido a malas configuraciones y protecciones asignadas.

5.3 Malware en trabajadores remotos

Los usuarios que trabajan remoto desde sus hogares ya son objetivo de los ciberdelincuentes, quienes ingresan a través de ellos a las redes corporativas. Las vulnerabilidades de los RDP (protocolos de escritorio remoto), ampliamente usados para las conexiones VPN, fueron la principal vía de acceso del ransomware en la primera mitad de 2020, de acuerdo con Coveware, Emsisoft y Recorded Future. Esta tendencia viene en crecimiento incluso antes de la pandemia.

5.4 Continua alza del ransomware

Kaspersky espera que crezca aún más la cantidad de ataques de extorsión a través del ransomware y ataques DDoS, además de exploits de día cero. Por su parte, desde Eset esperan un auge del ransomware que no solo impide el acceso a los datos de la víctima, sino que va publicando de a poco la información privada de la empresa y sus socios y clientes, para aumentar la presión para obtener el pago.

En Chile estos ataques han sido muy sonados en los últimos años, afectando famosamente en 2020 al Banco Estado (Sodinokibi) y a Cencosud (Egregor), por ejemplo

5.5 Ataques de Ingeniería Social apoyados por el internet de las cosas

Los dispositivos que interactúan con los usuarios como los dispositivos inteligentes u otros sistemas en el hogar (IoT), serán utilizados para realizar ataques más sofisticados. La información que se logre extraer puede incluir las rutinas diarias, hábitos, información financiera, entre otras, la cual será de ayuda para realizar ataques más precisos basados en ingeniería social.

Los ataques "inteligentes" pueden además ser más certeros para apagar sistemas de seguridad, deshabilitar cámaras o secuestrar dispositivos, además de posible extorsión por información sensible o confidencial, robo de credenciales o rescate de sistemas.

5.6 Robo de bitcoin y skimming digital a servidores

Entre las tendencias en ciberdelitos financieros para 2021, se mencionan el webskimming, el cual afectó, por ejemplo, de parte solo del grupo criminal Keeper, a más de 570 sitios de e-*commerce* en el mundo, con un total de 250 mil clientes, incluyendo negocios en Chile.

En el mismo ámbito, Kaspersky advierte un posible mayor riesgo del robo de bitcoin, a medida que personas en economías frágiles y alta inflación podrían ser más proclives a realizar fraudes en criptodivisas que en la moneda local, especialmente bitcoin.

5.7 Proliferación del malware "fileless"

Los ataques con códigos maliciosos que no usan un archivo para atacar, conocidos como fileless, deberán aumentar este 2021, según la apreciación de Eset. Durante el año 2020 se vio un aumento en su popularidad, según entidades como la ONU y el NCSC del Reino Unido. Al no requerir de la descarga de un archivo y funcionar en base a programas ya existentes en los sistemas, estos ataques son más difíciles de detectar.

6. Campañas concientización 2020

Uno de los desafíos propuestos por el CSIRT durante el 2020 fue crear más conciencia sobre los riesgos, amenazas y tendencias que existen en el mundo digital. Para esto, cada semana se difundieron, a través de las redes sociales y sitio web de la institución, 30 campañas educativas sobre variados temas acordes a la contingencia nacional e internacional.

Algunos tópicos abordados fueron: vacaciones ciberseguras, sexting, ciberdelitos en época de Coronavirus, consejos de seguridad para utilizar plataformas de videoconferencias, explicamos qué es el malware y los tipos que existen, entregamos consejos para evitar fraudes ante el retiro del 10% de la AFP, preparamos guías como, por ejemplo, de mediación parental y violencia de género, y también se reforzó la importancia de contar contraseñas seguras, cómo crearlas y qué persiguen los ciberdelincuentes con esta información.

Encuentra las campañas en sección recomendaciones de la página del CSIRT: www.csirt.gob.cl

Junto con esto, y para promover aún más la educación en materia de ciberseguridad, desarrollamos protocolos, guías e informes sobre los peligros cibernéticos que a causa de la crisis sanitaria venían impactando de distintas formas al mundo, como el teletrabajo, el uso seguro de las plataformas de videoconferencias, spear phishing, entre otros.

Así también, y de forma novedosa, el CSIRT elaboró dos cuentos originales para niños entre 5 y 12 años llamados: "Amigos por Internet" y "Benkid, pro gamer 147", para explicar de forma dinámica y simple a los niños cómo cuidarse al navegar por internet ante el ciberbullying y el grooming.

Del mismo modo, elaboramos dos guías para ahondar en dos temas relevantes y de contingencia en la actualidad. Uno de ellos fue la mediación parental, en la que explicamos en qué consistía, los riesgos a los que están expuestos los menores si no hay una supervisión por parte de los padres, cómo prevenir y cómo apoyar en cada etapa de los niños. Posteriormente, en noviembre, para conmemorar el "El Día Internacional de la Eliminación de la Violencia de Género" preparamos un material educativo sobre los tipos de violencia presentes en internet, entregamos algunas cifras de las plataformas más utilizadas por donde se agrede a las mujeres, cuáles son los tipos de agresores y en qué está la legislación chilena al respecto.

7. Investigaciones 2020

Análisis de Amenazas Cibernéticas es un trabajo creado desde las inquietudes e intereses de quienes están comprometidos directamente en la primeria línea de la ciberseguridad. Durante sus 27 ediciones esta publicación brindó un espacio de expresión a los analistas y especialistas que administran, gestionan, crean, educan, fomentan y se forman en esta materia. En principio fueron investigaciones de nuestros profesionales en el CSIRT con el apoyo del área de comunicaciones de nuestra unidad, pero luego extendimos la invitación a quienes estaban vinculados con nosotros en convenios de colaboración, así como a investigadores cercanos y especialistas reconocidos. Nuestro objetivó fue involucrar a la comunidad cibernética de la que somos parte para que los especialistas pudieran reflejar en estas páginas el estado de la ciberseguridad nacional. Fue un gran esfuerzo que involucró muchas voluntades y nos permitió conocer fenómenos y tipos específicos de amenazas cibernéticas, así como herramientas que nos pueden ayudar a contenerlas. Pero además nos dio la posibilidad de explorar por primera vez nuestras propias capacidades de investigación. Fue un reto muy especial que abrió un espacio público para compartir y debatir, en forma escrita, sobre los riesgos cibernéticos que enfrentamos como sociedad. En síntesis, esta publicación buscó crear conciencia del enorme esfuerzo que realizamos y nos queda por delante como país.

Encuentra las investigaciones en sección reportes de la página del CSIRT: www.csirt.gob.cl