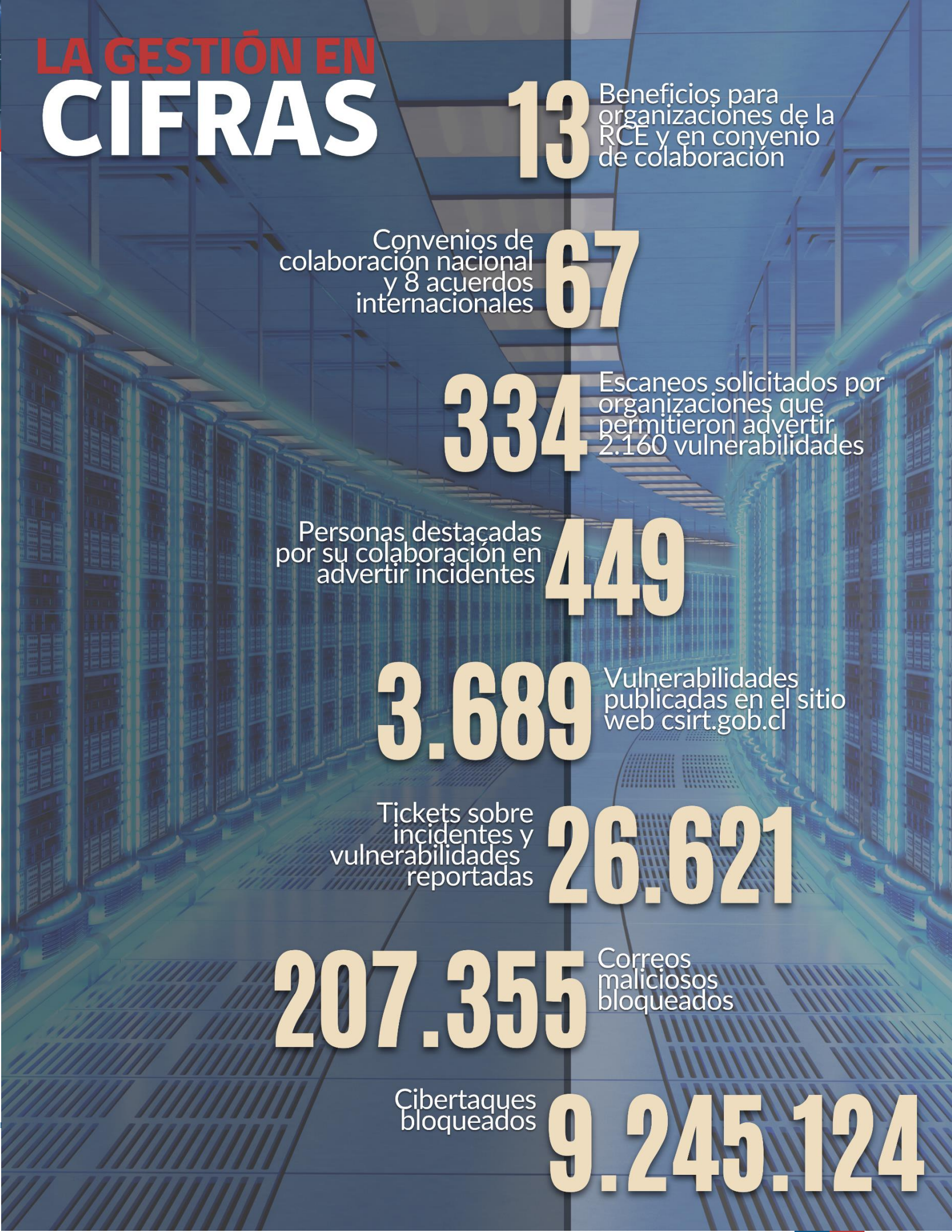
CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT

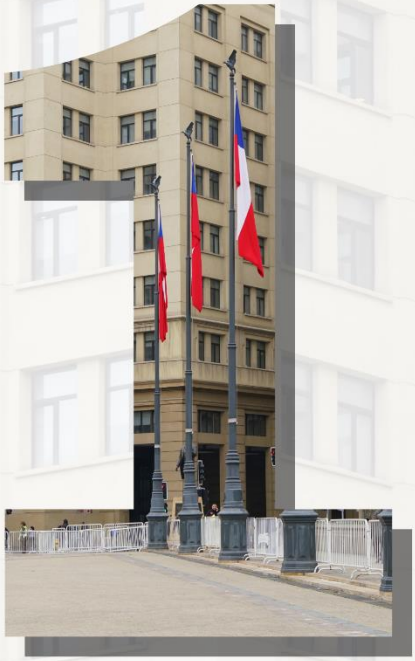
Equipo de Respuesta ante Incidentes de Seguridad Informática

INFORME ANUAL DE GESTIÓN 2022


LA GESTIÓN EN
CIFRAS
13
Beneficios para organizaciones de la RCE y en convenio de colaboración
Convenios de colaboración nacional y 8 acuerdos internacionales
67
334
Escaneos solicitados por organizaciones que permitieron advertir 2.160 vulnerabilidades
Personas destacadas por su colaboración en advertir incidentes
449
3.689
Vulnerabilidades publicadas en el sitio web csirt.gob.cl
Tickets sobre incidentes y vulnerabilidades reportadas
26.621
207.355
Correos maliciosos bloqueados
Cibertaques bloqueados
9.245.124

ÍNDICE

Dirección Ingrid Inda Camino | **Edición general** Carlos Silva Caffi | **Contenido** Patricio Quezada Andaur | **Colaboración** César López Hormazábal, Hernán Espinoza Medina, Sabina Torres Figueroa, Juan Moraga Andrades, Carolina Covarrubias Escudero, Felipe Quezada Valenzuela y Francisco Corona Caroca | **Diseño** Patricio Quezada Andaur | **Corrección de estilo** Ramón Rivera Notario | **Contacto** comunicaciones@csirt.gob.cl | Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, **CSIRT, 2023.**



PRESENTACIÓN

1. Presentación

Expresar en cifras la gestión de la ciberseguridad es una meta que anualmente nos proponemos en el CSIRT para medir el trabajo que realizamos. Y aunque las cifras son necesarias y objetivas, en este caso son una representación cuantitativa de la realidad, las que muchas veces dejan de lado las experiencias de un trabajo que, en lo cotidiano, está por sobre el compendio estadístico y se dedica a cumplir una misión prevista en la Política Nacional de Ciberseguridad, con énfasis en el Estado, la economía y la ciudadanía.

El CSIRT busca que el proceso de transformación digital que estamos atravesando como sociedad esté sustentado en un ecosistema digital seguro y resiliente, en el cual las capacidades de respuesta ante incidentes estén previstos en la gestión de los riesgos, y que cuando eso no ocurra, las organizaciones públicas y privadas tengan las competencias reactivas y proactivas suficientes para enfrentar los desafíos, limitando y mitigando la afectación de la integridad, disponibilidad y confidencialidad de los activos involucrados.

En este devenir de cambios y continuidades culturales asociados a los revolucionarios adelantos en las tecnologías de la información, la distancia entre los objetivos propuestos en la ciberseguridad y las diferentes realidades que enfrentan las organizaciones y la ciudadanía, todavía se perciben como amplias y confusas. Es ahí donde las cifras nos ayudan a comprender mejor el progreso de nuestro ecosistema. Y aunque para los críticos incluso las cifras puedan dar lugar a interpretaciones, lo que no se puede desconocer de ellas es que son una de las pocas constantes en un mundo de permanentes transformaciones.

El CSIRT nuevamente cumple con el compromiso autoimpuesto de medir la ciberseguridad, de la que se hace cargo en varios de sus aspectos por el mandato de la política nacional y en la práctica, por el rol de respuesta que se le asignó desde su creación y con el apoyo de las normativas que lo regulan.

El informe anual de gestión 2022 quiere dar cuenta de la gestión de la ciberseguridad en la mayor cantidad de aspectos posibles, y busca ser objeto de debate entre sus lectores, así como una fuente para las futuras evaluaciones sobre el progreso de esta materia.

IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS Y MEDIDAS DE MITIGACIÓN

2. Identificación y evaluación de riesgos y medidas de mitigación

La gestión del riesgo es uno de los principales objetivos de la ciberseguridad. Las organizaciones que logran coordinar actividades para dirigir y controlar el riesgo pueden comprender -a partir de su análisis-, la naturaleza de este y determinar niveles que permiten definir aquello entre lo que es aceptable de lo que no lo es.

Para gestionar el riesgo en ciberseguridad es necesario identificar qué representa un riesgo para la organización o negocio, y realizar un análisis para una posterior evaluación y la toma de decisiones sobre cómo tratarlo.

Una parte importante del trabajo del CSIRT es proveer y gestionar herramientas que permiten identificar y evaluar los riesgos de ciberseguridad de las organizaciones del Estado. Las áreas de auditoría y de prevención de vulnerabilidades, están trabajando en forma permanente y coordinada con las organizaciones que lo requieren, para identificar, analizar y evaluar los aspectos más sensibles en los activos informáticos de los servicios públicos que están expuestos a la internet, entregándoles reportes con las mitigaciones específicas que recomendamos realizar en esos activos y que puedan proteger sus activos y, sobre todo, a la organización.

2.2. Gestión de auditoría

Los instrumentos de autoevaluación han sido fijados por el CSIRT como una forma de apoyar a las organizaciones para detectar sus debilidades, así como sus fortalezas.

Esta evaluación se obtiene de un cuestionario voluntario que no exige evidencias probatorias. En consecuencia, su confiabilidad depende íntegramente de las respuestas otorgadas por las organizaciones entrevistadas.

La participación en estas auditorías no solo va en beneficio individual de las organizaciones, sino que permiten evaluar a los sectores de la economía en los que se desenvuelven, para así comparar experiencias y encontrar soluciones a desafíos transversales por las que atraviesan.

El documento final que se construye luego de esta autoevaluación sirve como diagnóstico para impulsar el desarrollo de planes y estrategias que buscan fortalecer aquellos temas y aspectos que se consideren vulnerables respecto de los ejes centrales de la ciberseguridad gubernamental, de ahí la importancia de esta gestión.

En específico, las auditorías permiten, en primer lugar, identificar oportunidades de mejora en torno a los sistemas de gestión de seguridad de la información (SGSI) basados en la norma ISO 27001, en las buenas prácticas y controles (CONTROLES) de la norma ISO 27002:2022, en las infraestructuras críticas (IC) o de importancia estratégica, y en los controles de ciberseguridad definidos (CIBERSEG) en la ISO 27032.

La escala de evaluación para esta valoración es de 5 niveles. Cada uno de estos indicadores fueron evaluados por grupos e individualmente. En todos los casos se fijó un 75% de cumplimiento como piso adecuado en la escala de madurez, esto es, un nivel donde todos los incidentes relacionados con la seguridad de la información son gestionados y se aplica mejora continua a los procesos de ciberseguridad.

NIVEL	ASPECTO	CUMPLIMIENTO	DESCRIPCIÓN
0	Sin respuesta	0%	No se obtiene información al respecto
1	Inicial	0% - 20%	Existe este elemento clave, pero no está aprobado formalmente o no se ejecuta como parte del Sistema de Ciberseguridad.
2	Repetible o Planificado	20% - 40%	Se planifica y se aprueba formalmente. Se programa la realización de actividades.
3	Definido o Ejecutado	40% - 60%	Se ejecuta e implementa de acuerdo con lo aprobado y planificado.
4	Gestionado o Verificado	60% - 80%	Se realiza seguimiento y medición de las acciones asociadas a la ejecución.
5	Optimizado o Retroalimentado	80% - 100%	Se retroalimenta y se toman medidas para mejorar el desempeño.

De acuerdo con los resultados de las auditorías realizadas el pasado año 2022, el promedio global de avance alcanzado en el período evaluado llega a un 49,3% de logro, lo que sitúa a las organizaciones en general en el nivel 3 de la escala de valoración, de un máximo de 5. En este nivel las instituciones están logrando planificar acciones de ciberseguridad con cierto grado de formalidad interna, y están logrando ejecutar en parte los planes establecidos, pero no están realizando un seguimiento y medición de las acciones asociadas a la ejecución, aspecto relevante para el control de calidad y de objetivos.

De acuerdo con la evaluación, tampoco se está logrando incorporar el mejoramiento continuo sobre la ciberseguridad en los procesos institucionales vinculados a los objetivos estratégicos, aspecto clave para el descubrimiento de problemas en los procesos críticos vigentes y la aplicación de las respectivas soluciones. Esta situación es particularmente preocupante en virtud de los desafíos que se ha auto impuesto el Estado respecto de la transformación digital, que señala el uso obligatorio de plataformas electrónicas.[1]

Ahora bien, analizados los indicadores grupales, los promedios muestran diferentes porcentajes de avance, aunque todos siempre dentro de la misma categoría (nivel 3).

INDICADORES	PROMEDIO
Sistema de gestión de seguridad de la información (SGSI)	44,4%
Prácticas y controles (Controles)	50,4%
Infraestructura Crítica (IC)	46,3%
Controles de ciberseguridad (CIBERSEG)	53,5%
Global	49,3%

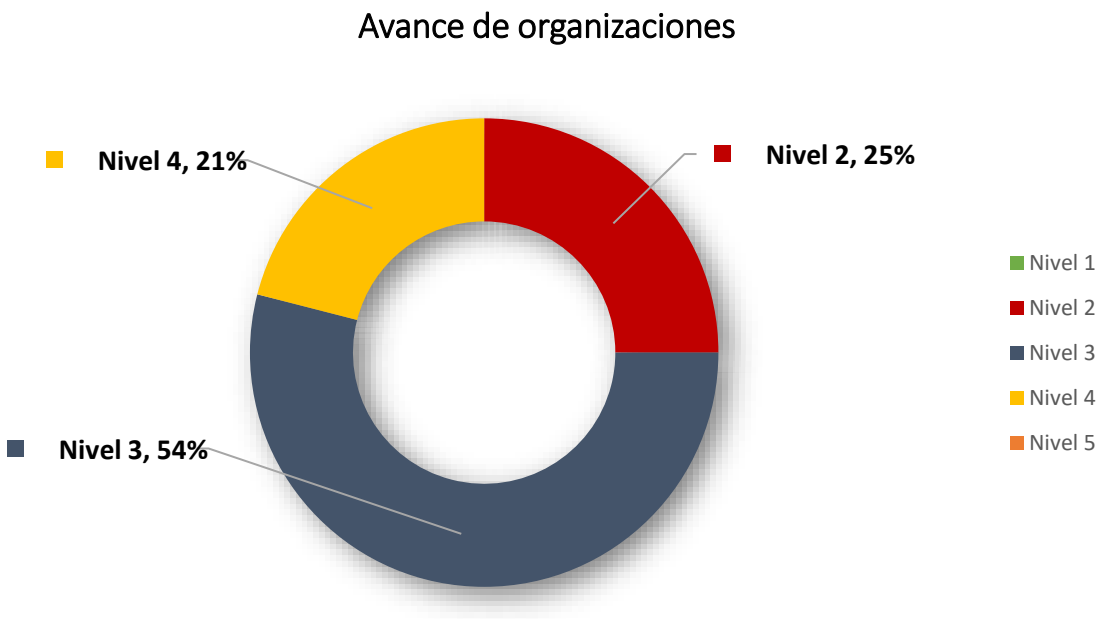
[1] https://bcn.cl/2naga

Dentro de los desempeños grupales se observa un mejor resultado en el ámbito de los controles de ciberseguridad, fenómeno que podría tener relación con la aplicación de directivas presidenciales hacia las instituciones (Instructivo Presidencial N°8 de 2018), instrumento que imparte instrucciones urgentes en materia de ciberseguridad para la protección de redes, plataformas y sistemas informáticos de los órganos de la administración del Estado y que incluye, entre otros, la designación de encargados de ciberseguridad por institución.

Por contraste, el indicador más débil corresponde al SGSI, cuyo porcentaje promedio es de 44,4%. Este es uno de los aspectos más desafiantes que entrega este diagnóstico, precisamente porque el SGSI es particularmente relevante para articular las medidas necesarias en la institución frente a los escenarios de riesgos, amenazas y sus impactos probables en los activos de información críticos.

Un mejor desempeño obtuvo el IC. Este marco referencial de resiliencia, de gran importancia para para lograr niveles superiores de madurez y clave para enfrentar los desafíos de calidad establecidos y requeridos por el proceso de transformación digital, logró un 46,3% de avance. Este nivel de avance se debe vincular a la implementación de consideraciones de resiliencia vinculados a los planes de continuidad de negocios (BCP) y a los planes de recuperación de desastres (DRP).

Entre las 24 organizaciones que se sometieron a la autoevaluación, los resultados muestran que el 54% de ellas se encuentran dentro del promedio general, el nivel 3, y un 21% está en el nivel 4, lo que es bastante positivo.



Existen casos sobresalientes en lo individual. Al menos 1 organización está por encima del piso mínimo en el indicador SGSI (nivel 4, y en 79% de logro, solo 1% por debajo del nivel 5), y otras 4 también comparten el nivel 4, por sobre un 60% de logro; otras 3 organizaciones logran el piso de evaluación de 75% en el indicador de planificación y controles, a las que se suman otras 2 organizaciones que se sitúan en el nivel 4; en cuanto a la resiliencia, ninguna organización logra el

piso mínimo, pero 5 de ellas están en un nivel 4; por último, hay 5 organizaciones en el nivel 4 de controles de ciberseguridad, y 3 de ellas están muy cerca del umbral de 75% fijado.

En este sentido, el grueso de las instituciones se encuentra en un buen pie para transitar hacia el próximo nivel y, en lo posible, alcanzar el objetivo de 75%. Para ello las organizaciones deben considerar los controles con baja evaluación e incluirlos en los planes de acción a modo de elevar su madurez, apoyándose en un SGSI que cuente con el compromiso de las jefaturas e incluyendo una capacidad operativa suficiente para articular los desafíos que enfrenta respecto de los riesgos tecnológicos, tanto para su funcionamiento administrativo como para su operación.

El compromiso del CSIRT es entregar los resultados individuales a cada organización participante, con las respectivas propuestas de mejora, todo lo anterior con la debida reserva de sus alcances. Pero a la vez, queremos contribuir con estas cifras generales de avance, de modo que el diagnóstico global pueda servir al debate público y sea un modelo de gestión para otras organizaciones, tanto públicas y privadas, que se dedican a la ciberseguridad.

2.3. Gestión de escaneo de vulnerabilidades a organizaciones

Uno de los beneficios más importantes que otorga el CSIRT a las organizaciones de la administración pública del Estado es la gestión de escaneo de vulnerabilidades. Este beneficio, que desde diciembre pasado está respaldado en el de Decreto 273, es una gestión preventiva realizada por el CSIRT en colaboración con la organización interesada y busca robustecer la seguridad informática de éstas al encontrar anticipadamente vulnerabilidades en los sitios y aplicativos webs de los servicios expuestos a la internet.

El escaneo de vulnerabilidades ha permitido detectar diferentes tipos de debilidades o errores de implementación en los activos informáticos analizados y evaluados, advirtiendo en cada reporte sobre la severidad y la más probable vía de explotación por parte de los actores de amenaza.

Tanto los reportes preliminares, que pueden estar disponibles dentro de 24 horas desde que se coordina el escaneo, así como en los informes finales, cuya entrega promedio es de 7 días hábiles desde el inicio del proceso, son herramientas de enorme valor para la gestión de la ciberseguridad de las organizaciones. El reporte final, además de analizar y evaluar en detalle sobre la vulnerabilidad encontrada, incluye de una serie de recomendaciones tendientes a mitigar las vulnerabilidades allí señaladas.

Una vez entregado el reporte final a la organización, CSIRT inicia un proceso de seguimiento de la gestión de mitigación el que se formaliza a través de la apertura de tickets individuales por cada una de las vulnerabilidades detectadas.

Cuando las organizaciones lo requieren, CSIRT entrega orientación específica sobre cómo mitigar las vulnerabilidades informadas. Sin embargo, dado que cada organización cuenta con sistemas y plataformas distintos, siempre será la organización la responsable final de éxito en la gestión de mitigación de las vulnerabilidades.

La valoración de este beneficio a nivel de las organizaciones de la administración pública del Estado ha permitido que se normalice su uso a través del ya mencionado Decreto 273, el que puede ser esgrimido por todos los órganos del Estado centralizados y descentralizados para que el CSIRT pueda ejecutar esta tarea en los sitios y aplicativos webs que las organizaciones estimen necesarios, con la sola exigencia de mínimos técnicos y protocolos específicos para otorgar este beneficio.

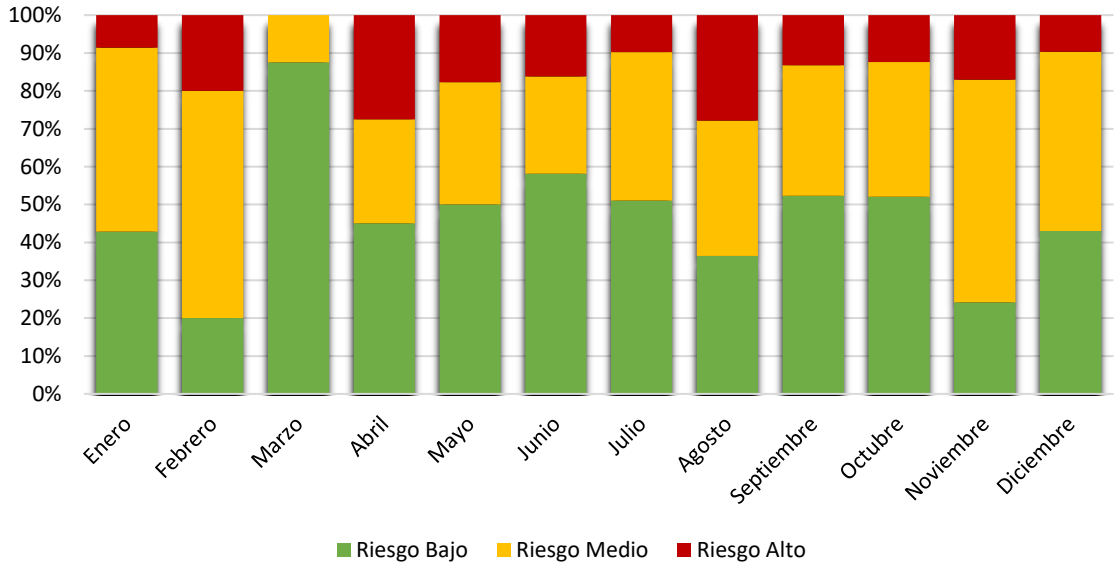
Conocer las vulnerabilidades y mitigarlas oportunamente, es una de las medidas preventivas complementarias a la gestión de ciberseguridad de las organizaciones que más ayudan a proteger los sistemas informáticos.

Durante el año recién pasado, CSIRT realizó un total de 334 escaneos solicitados por organizaciones del Estado. En total, fueron 48 instituciones las que recibieron este beneficio. Este trabajo permitió detectar 343 vulnerabilidades de rango alto, 837 de rango medio y 980 de rango bajo.

En 30 de las 48 organizaciones que recibieron el beneficio (63%) fue detectada, al menos, una vulnerabilidad de riesgo alto, mientras que en 43 se encontraron vulnerabilidades de riesgo medio y en 47 de las 48 se reportaron algún tipo de vulnerabilidad de riesgo bajo.

Es importante destacar que cada organización tiene la obligación de priorizar sus vulnerabilidades, sin importar que estas sean evaluadas en distintos tipos de severidad. Es así como, si una organización es informada de vulnerabilidades de rango medio, si estas son esenciales para la continuidad operativa de sus servicios, las organizaciones deben abocarse a su mitigación en el menor tiempo posible, porque una eventual exposición de esa vulnerabilidad, aún sin ser de severidad alta, puede ser explotada por un actor de amenaza.

Proporción anual de vulnerabilidades por criticidad



Si analizamos proporcionalmente las vulnerabilidades encontradas el año 2022, nos encontramos con un escenario inestable comparando cada mes. Hay varios factores que explican el fenómeno, desde la metodología del trabajo, las variables proporcionadas por nuevas vulnerabilidades, así como la demanda de escaneo por parte de las organizaciones.

En cuanto a la metodología, mientras las constantes van por el lado de las herramientas y las métricas que se utilizan, las variables dependen del descubrimiento de nuevas vulnerabilidades y de la clasificación de riesgos. A ello debemos sumar la gran cantidad de vulnerabilidades acumuladas y no tratadas oportunamente por las organizaciones. En consecuencia, estamos hablando de una gran cantidad de vulnerabilidades, cada una con diferentes riesgos.

Lo anterior se hace aún más complejo en la medida que las organizaciones no siempre son conscientes de la exposición de los activos informáticos que poseen y que, por acción derivada de la solicitud de un análisis específico, puede ser descubierto al momento del proceso de escaneo.

GESTIÓN DE CONTENIDOS, COMUNICACIÓN Y COOPERACIÓN

3. Gestión de contenidos, comunicación y cooperación

El intenso intercambio de información entre organizaciones públicas y privadas, así como el reporte de amenazas e incidentes que emana desde la ciudadanía, es posible gracias a la creación de un ambiente basado en la confianza.

Construir y mantener la confianza pública es una gestión que depende de la cooperación y de una fluida comunicación entre los actores interesados en la prevención y respuesta de los incidentes.

En el CSIRT utilizamos diferentes canales de comunicación y cooperación. Estos canales sirven para compartir indicadores de compromiso que son útiles a la gestión de la ciberseguridad de las organizaciones, así como material de concientización, investigaciones, comunicados, reportes de vulnerabilidades y alertas de seguridad.

En líneas generales, existen tres canales de comunicación de ciberseguridad: las que están dirigidas a la ciudadanía y en medios de comunicación; las que ponen énfasis en la gestión de ciberseguridad de los órganos del Estado; y las que suscriben acuerdos de cooperación.

Adicionalmente, el CSIRT interactúa formalmente con otras organizaciones como parte de su gestión cotidiana, como las entidades que componen el Comité Interministerial de Ciberseguridad, otros CERT's y CSIRT's, proveedores de servicios, entre otras.

Pero tan importante como los canales de gestión de comunicación, es la información que se comunica y la oportunidad con que se realiza esa comunicación. Ese insumo depende fundamentalmente del equipo humano y técnico que recibe y recolecta la información, la analiza, la evalúa y genera diversos productos en forma de documentos.

3.1. Sobre la información que se comunica

Con la implementación del área de comunicaciones, el CSIRT comenzó a organizar e incorporar los productos y los canales de comunicación que permiten, en la actualidad, gestionar el intercambio de información y cooperación con otras entidades y con la ciudadanía.

En este período se han consolidado un conjunto de productos que se comunican de forma cotidiana, como:

- Alertas reactivas, que advierten métodos, vectores de infección e indicadores de compromiso de campañas de phishing, malware, ataques de fuerza bruta y falsificación de registros;
- Alertas de vulnerabilidades, que informan sobre los parches liberados por los fabricantes, así como información de gestión en casos de vulnerabilidades de día cero;
- Comunicados de alertas especificas o información general, que ponen énfasis en algún incidente en particular o advierten de una situación que podría convertirse en relevante en el corto o mediano plazo, entregando siempre recomendaciones sobre el fenómeno en particular;

- Boletines de ciberseguridad semanales, que compilan antecedentes de la información gestionada cada semana e incorpora el resumen del trabajo de concientización y el aporte ciudadano y de otras organizaciones;
- Resúmenes de ciberseguridad, que compilan la información de gestión semanal del CSIRT
- Material de concientización, que incluye campañas temáticas y generales, promoción de buenas prácticas y consejos, productos audiovisuales de apoyo y piezas gráficas;
- Investigaciones y reportes estadísticos, que organiza en un trabajo específico algunas de las temáticas de relevancia contextual o para ser un aporte al conocimiento general de la ciberseguridad;

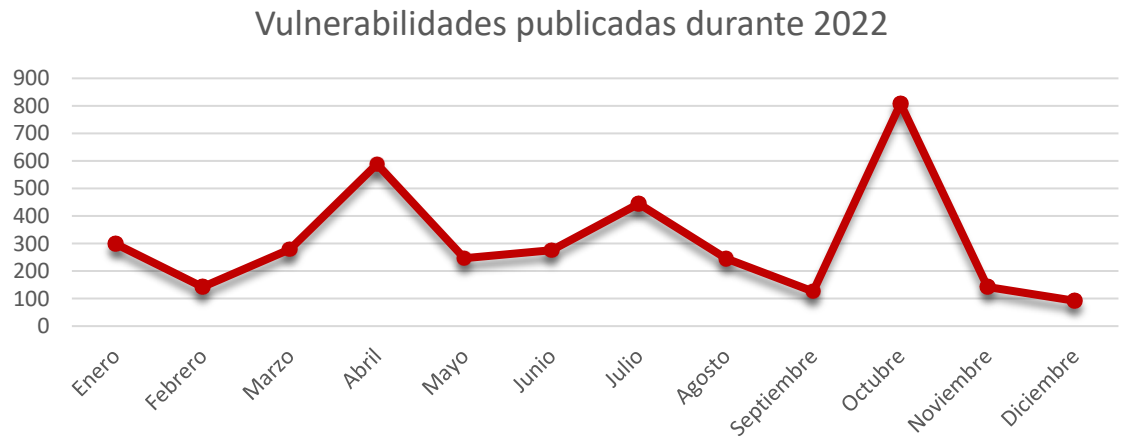
3.2. Plataformas de gestión de la comunicación

La comunicación ha sido, desde un principio, uno de los pilares de la gestión del CSIRT. Esa gestión se realiza a través de diferentes plataformas: sitio web, formulario de contacto, correo electrónico, teléfono y redes sociales.

La web www.csirt.gob.cl es la principal herramienta de compilación de información, que sirve por igual a la gestión ciudadana como organizacional. Las redes sociales, por otra parte, facilitan la difusión de la información, así como campañas de concientización y del trabajo del CSIRT. Por su parte, el teléfono como el correo se han consolidado como medios de comunicación oficial, intra e interinstitucional.

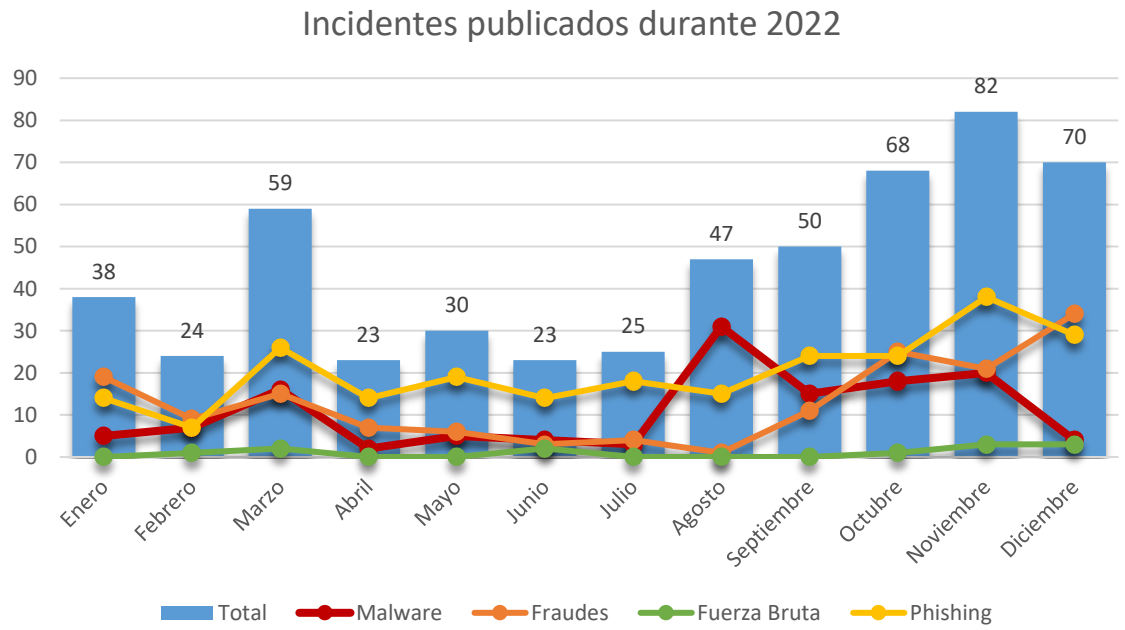
3.2.1. Sitio web

El sitio web es uno de los repositorios más completos sobre ciberseguridad disponibles para las organizaciones y la ciudadanía, el que incluye información para la gestión cotidiana, además de alertas, vulnerabilidades, noticias, comunicados, investigaciones, concientización, estadística e información general.



En lo que concierne al sitio web, su estructura privilegia la publicación de vulnerabilidades y alertas. En el caso de las vulnerabilidades, el criterio es publicar información sobre riesgos relacionados a plataformas que son utilizadas frecuentemente entre las organizaciones del Estado y que además son de elevada criticidad, para que las organizaciones puedan implementar los parches correspondientes.

Durante 2022 se publicaron 220 informes para advertir unas 3.689 vulnerabilidades. La gran mayoría de estas vulnerabilidades contaba con el respectivo parche elaborado por el proveedor, sin embargo, hubo una excepción que corresponde a la vulnerabilidad de Microsoft Exchange Server de día cero, en el que la empresa tardó más de un mes en resolverlo. En ese contexto, y a partir de la información entregada por el proveedor, así como otras agencias de ciberseguridad, el CSIRT generó una serie de comunicados con recomendaciones con el objetivo de reducir la superficie de ataque ante una potencial explotación.



En el caso de los incidentes, que incluyen campañas de malware, falsificación de registros, phishing y ataques de fuerza bruta, CSIRT publicó en su sitio web y difundió en redes sociales un total de 539 alertas.

Del total de alertas públicas de incidentes, el 44,9% de ellas correspondieron a campañas de phishing (242 muestras obtenidas de correos). Le siguieron la falsificación de registros (28,8%), las campañas de malware (24,1%), y los ataques de fuerza bruta (2,2%).

Al revisar el comportamiento anual de las alertas de incidentes publicados, entre los meses de octubre a diciembre acumula la mayor cantidad de publicaciones un 40,8% siendo noviembre el mes con la mayor cantidad de incidentes del año, un total de 82.

Cada uno de los informes publicados entrega información relevante para los especialistas de seguridad de las organizaciones. Entre los antecedentes compartidos, los indicadores de compromiso como la URL, el hash o la dirección IP, son de un importante valor estratégico. El pasado año 2022 se informaron 830 URL, 794 hashes y 874 direcciones IP sospechosas. El CSIRT siempre recomienda que los especialistas evalúen la aplicación de una cuarentena sobre estos indicadores y su revisión posterior para un eventual levantamiento de la medida.

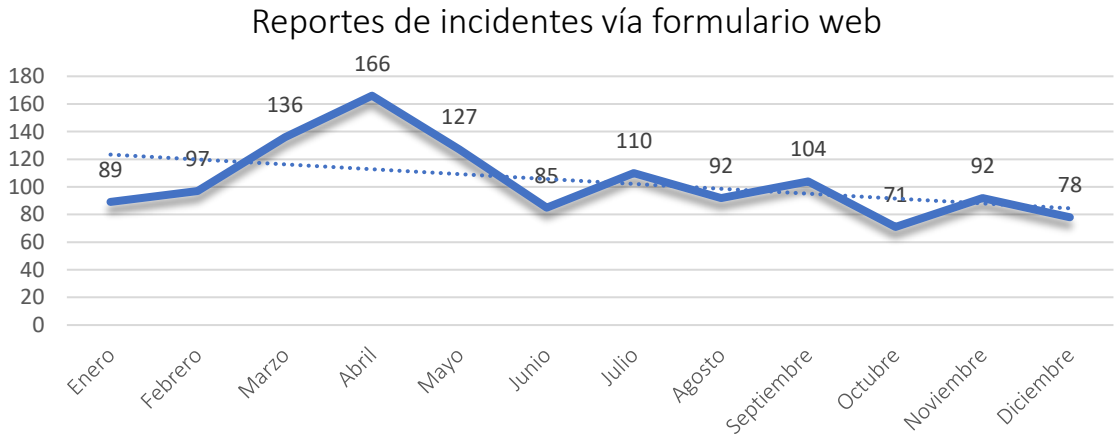
Además de indicadores de compromiso, el informe de alertas, en el caso de los phishing, advierte sobre el método utilizado por el atacante para ejecutar esta acción. En la medición de las alertas de phishing publicadas el 2022 (240 campañas) el 82,1% de los ataques se realizaron a través de un correo electrónico, el 9,6% a través de WhatsApp y un 8,3% vía Smishing.

Las publicaciones de alertas y vulnerabilidades ayudan a la gestión preventiva entre las organizaciones. En el caso de las vulnerabilidades, el aviso temprano tiene como objetivo que las organizaciones implementen los parches de seguridad, las instrucciones del proveedor y las recomendaciones del CSIRT, antes de que un atacante tenga la oportunidad de explotarlas. En el caso de las alertas, el objetivo es advertir a las organizaciones sobre campañas masivas o ataques dirigidos, cuyas consecuencias podrían afectar la continuidad, integridad o disponibilidad de los sistemas y activos informáticos de la organización.

3.2.2. Formulario de contacto

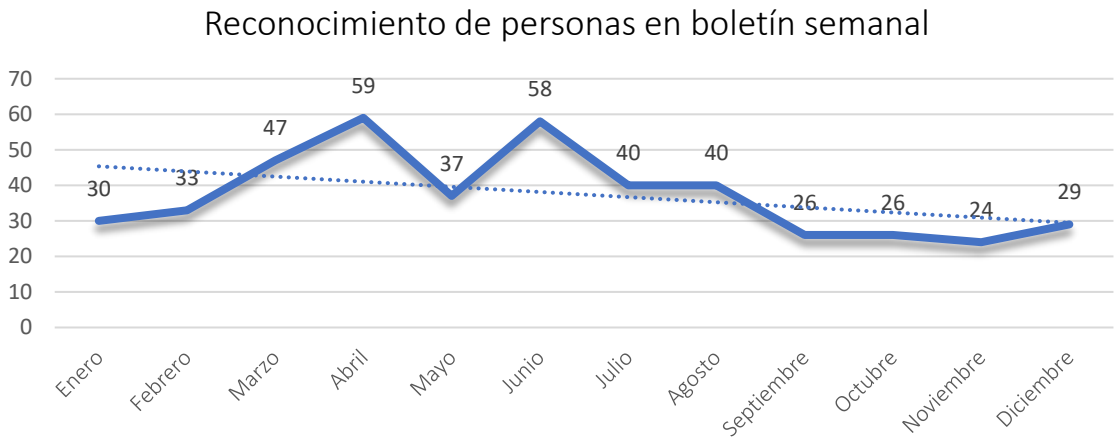
Con la entrada en vigencia del Decreto 273 (2 de diciembre de 2022), sobre notificación de incidentes, el formulario de reporte se institucionalizó como el mecanismo digital que las organizaciones deben utilizar para comunicarse con el CSIRT

Lo anterior no desconoce el hecho de que el formulario web se ha consolidado paulatinamente como una herramienta expedita y eficaz para reportar o notificar incidentes tanto para la ciudadanía como para las organizaciones.



Esta herramienta permite la apertura automática de un ticket sobre un incidente lo que permite iniciar el proceso de gestión de respuesta y su seguimiento hasta el cierre del mismo.

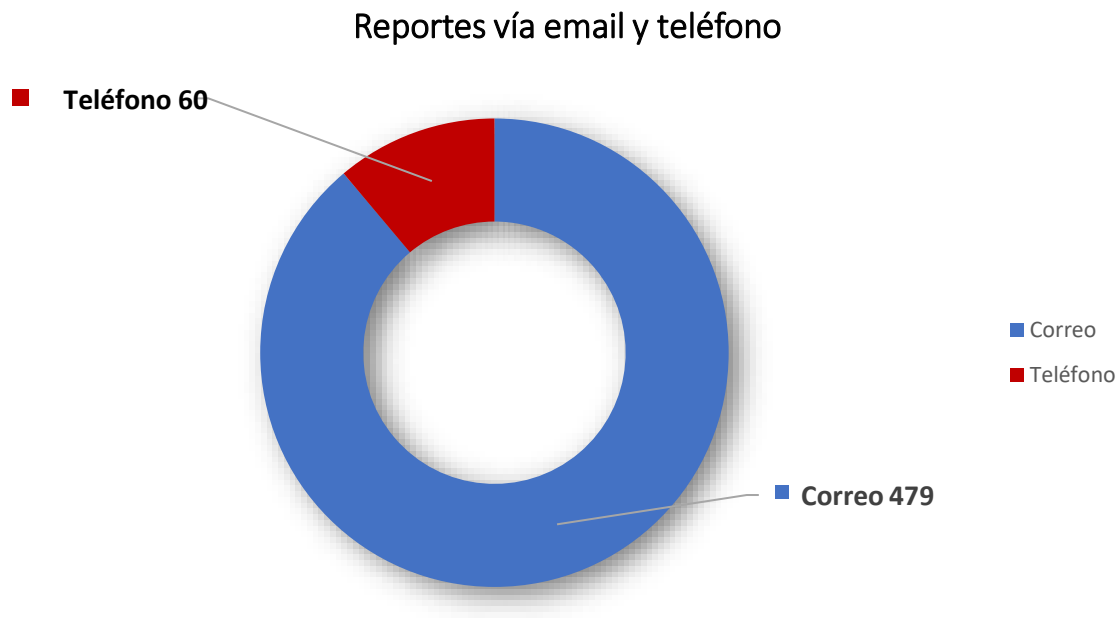
El 2022 el formulario web sirvió para realizar 1.247 reportes de incidentes. Una parte importante de estos reportes fue advertida por la ciudadanía y organizaciones externas. Si bien esta herramienta aún constituye una exigua proporción del total de los tickets gestionados en un año normal (4,7%), su importancia yace en la consolidación del vínculo entre la organización y la ciudadanía.



Cómo costumbre, CSIRT reconoce el rol de la ciudadanía que reporta incidentes utilizando el formulario web y lo hace a través del boletín semanal de ciberseguridad, específicamente en la sección "muro de la fama". Durante el año pasado, CSIRT reconoció públicamente el aporte de 449 personas (un promedio de 37 personas por mes) por su ayuda en la detección de incidentes.

3.2.3. Correo y teléfono

Además del formulario, el CSIRT cuenta con el correo de contacto soc-csirt@interior.gob.cl y el teléfono 1510. Aunque estas herramientas tienen un mayor uso en la gestión administrativa, de todas formas, prestan un importante apoyo para el reporte de incidentes.



Las estadísticas de gestión respaldan lo antes señalado si comparamos el menor uso de estas herramientas para el reporte ciudadano. Entre ambas herramientas, durante 2022, se notificaron

539 incidentes de ciberseguridad. 88,9% se realizó a través de un email y un 11,1% vía llamada telefónica.

3.2.4. Redes sociales

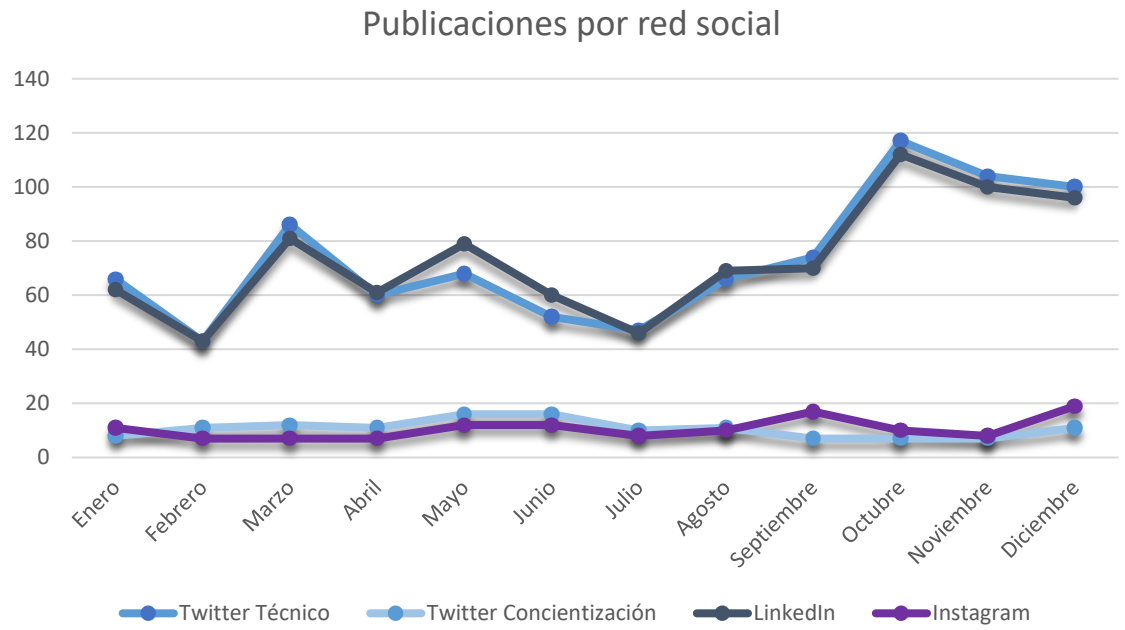
Para difundir información y promover la conciencia sobre ciberseguridad, el CSIRT utiliza diferentes redes sociales, siendo las preferentes Twitter, LinkedIn e Instagram. Cada una de ellas pone énfasis en públicos específicos.

En el caso de Twitter, CSIRT cuenta con dos cuentas. La primera (https://twitter.com/CSIRTGOB), pone énfasis en un público técnico y especializado de ciberseguridad, así como en las organizaciones. En este canal se transmite información sobre vulnerabilidades, amenazas e incidentes, así como comunicados y alertas especiales. Por otra parte, la segunda cuenta de Twitter pone énfasis en la ciudadanía (https://twitter.com/CSIRTConciencia). Este medio permite difundir información de concientización, noticias y reportes generales.

En el año recién pasado la cuenta especializada registró un crecimiento de 29,95% de seguidores, mientras que la cuenta de concientización experimentó un alza de 21,8%. En términos de distribución de información, existe una mayor oferta de información especializada, en consecuencia, el Twitter técnico cuenta con una mayor proporción de insumos que el de concientización (87,4% vs 12,6%).

En el caso de LinkedIn, la evolución de la cuenta en el mismo período muestra un importante crecimiento de 53,1% en seguidores. En parte, la explicación yace en que esta cuenta reúne el aspecto técnico y el de concientización, por lo que la oferta informativa que ofrece es mucho más amplia.

En el caso de Instagram, el 2022 experimentó el más alto crecimiento entre las redes sociales del CSIRT, consiguiendo un 65,7% de nuevos seguidores, esto, pese a que la cuenta de Instagram está dedicada casi exclusivamente a información de concientización.



Como se puede advertir en el gráfico, las cuentas que involucran información técnica concentran una mayor cantidad de publicaciones que aquellas que solo informan de concientización. El objetivo a mediano plazo es mantener la oferta especializada y aumentar paulatinamente el contenido de concientización.

3.3. Gestión de los canales de cooperación

La gestión de los canales de cooperación se realiza cotidianamente a través de la difusión de información, pero también se manifiesta en acciones de promoción de la ciberseguridad, como eventos, capacitaciones e instancias de intercambio de experiencias e ideas.

El CSIRT tiene diferentes canales de cooperación técnica y de concientización, las que suceden en la Red de Conectividad del Estado, con entidades asociadas en convenios de colaboración y con agencias y organizaciones internacionales a través de MoU (Manifiestos de Entendimiento).

En el caso de la cooperación internacional, esta se mantiene activa con 7 países (Argentina, España, Colombia, Ecuador, Israel, Reino Unido y Estonia) y con un bloque internacional (La Organización de Estados Americanos).

En el caso de los convenios de colaboración nacional, el pasado año 2022 se sumaron 8 organizaciones con acuerdos firmados o en trámite de firma (Cámara de Comercio de Santiago, Coopeuch, Fundación de las Familias, Casa Moneda, USACH, Microsoft, Kaspersky y Vías Chile), las que junto con la actuales organizaciones en convenio (Forum, Asociacion Chilena de empresas de Tecnologías de Información Ag, Sercor S.A, Alianza Chilena de Ciberseguridad, Orion Seguros Generales, Deloitte, Compañía Cervecerías Unidas, Centurylink, Pit Chile, Mercadolibre, Asociación Cloud Security Alliance Capitulo Chileno, 8.8 Computer Security Conference, Redbanc S.A, Enel Chile,

IBM de Chile Sac, Asociación Chilena de Seguridad, (Isc)2, Appit, Asociación Aseguradores De Chile, Banco Falabella, Bupa Chile, Reuna, Universidad Adolfo Ibañez, Universidad de Chile, Universidad Mayor, Universidad Andres Bello, Banco del Estado, Banco Central Chile, Sernac, Essbio, Universidad Autónoma De Chile, Instituto Nacional de Normalización, Aguas Antofagasta, Corporación de Universidades Privadas, Corporación Alta Ley, Bolsa de Comercio de Santiago, Trend Micro Latinoamericana S.A, Matic Kard S.A, AFC, Aguas Andinas, BHP Chile Inc, Saam S.A, Cámara Chilena de Infraestructura Digital A.G, Cencosud Scotiabank, Cisco, Entel, Fortinet, Fundación Whilolab Chile, Empresas SEP, Tribunal Constitucional, Mutual de Seguridad, CCHC, Maissa S.A, Asociación de Empresas Eléctricas, Inversiones Renacer Spa (Andes Salud), Instituto Regional de Administración de Empresas (Irade), Universidad de Concepción, Esval S.A y Aguas del Valle S.A) totalizan 67 entidades.

3.3.1. Intercambio de información

CSIRT mantiene un intenso intercambio de información de ciberseguridad y coordinación con organizaciones del Estado, empresas públicas, organizaciones privadas, agencias de ciberseguridad y organizaciones internacionales.

Tanto a nivel nacional como internacional, una de las herramientas más activas de intercambio de información es la plataforma para compartir de información de malware (MISP), la que se utiliza para aportar con información tanto técnica como de concientización a nivel de América Latina a través del CSIRT de las Américas de la organización de Estados Americanos, y con los convenios de colaboración en un MISP nacional.

Una parte de las alertas sobre incidentes de ciberseguridad que se publican y comparten a nivel nacional también es compartida en el MISP del CSIRT de las Américas, además de campañas de concientización y buenas prácticas.

El CSIRT también registra una serie de intercambios de información con agencias (CERT's y CSIRT's) y organizaciones internacionales de ciberseguridad (FIRST, Meridian, Alianza del Pacífico, CSIRT de las Américas), en algunos casos, sin tener un acuerdo explícito de colaboración. Es cotidiano que al conocer un incidente que pueda amenazar a otro país, las agencias compartan la información en forma clasificada bajo el protocolo TLP, para que puedan gestionar su respuesta.

Por otro lado, el CSIRT habilitó un MISP nacional, en el que se comparten principalmente información sobre indicadores de compromiso entre las organizaciones que se encuentran en convenio de colaboración, pero siempre está abierta la posibilidad de que otras entidades que cumplan los estándares técnicos y logísticos mínimos, puedan vincularse a la plataforma.

3.3.2. Capacitaciones y ejercicios

Durante el año 2022 se realizaron 13 grandes actividades de capacitación dirigidos a diferentes públicos, entre ellos, funcionarios de gobierno, encargados de ciberseguridad, encargados de seguridad TI, Organizaciones en convenio de colaboración y público en general.

Una de las actividades más destacadas fue el diplomado en seguridad de la información y ciberseguridad de la USACH, Especialmente dirigido encargado de ciberseguridad del gobierno. Para este público también se organizaron simulacros y ejercicios decir seguridad en coordinación con empresas como Microsoft y Kaspersky, además de la conferencia 8.8 Gobierno en el contexto del mes de la ciberseguridad.

Para las entidades en convenios de colaboración se gestionaron dos simulacros especialmente dirigidos a las áreas del retail y del retail financiero.

Entidad	Actividad	Público
USACH	Diplomado en Seguridad de la Información y Ciberseguridad	Encargados
Microsoft	Seguridad, Cumplimiento e Identidad	Encargados
Kaspersky	Ejercicio Simulación Gestión de Ciberseguridad	Encargados
CSIRT GOB	8.8 Gobierno	Encargados
Microsoft	Cybersecurity Simulacro de Ataque	Interno
Kaspersky	Ejercicio Simulación Gestión de Ciberseguridad para el Retail	Convenio
OEA	OEA CyberWomen	General
OEA	OEA Cybersecurity Invovarion Councils	Gobierno
Know For One	CGE Modelo CIS Protección del Correo Electrónico y Navegación WEB	Interno
Correos de Chile	Factor Humano eslabón clave en la Ciberseguridad	Interno
SEGEGOB	Riesgos y desafíos de ciberseguridad en instituciones públicas	Funcionarios
Caja de Los Héroes	Digitalización y Seguridad en Personas Mayores	General
Kaspersky	Primer Ejercicio de Simulación de Seguridad Retail Financiero	Convenio

Finalmente, como todos los años, se realizaron eventos en el marco de convenios de cooperación internacional, de los cuales se destacan el Cybersecurity Innovation Council de la OEA, que este año 2022 tuvo como sede nuestro país y la quinta versión del OEA Cyberwomen Challenge, el ejercicio de simulación en ciberseguridad dirigido a mujeres y realizado de forma on-line.

Las actividades gestionadas por el CSIRT buscan concientizar, por un lado, a los líderes de las organizaciones y jefes de servicio, para que puedan sopesar la importancia de las ciberseguridad y riesgos que existen en el ecosistema nacional y global; y por otro a los encargados de ciberseguridad, especialistas de seguridad TI y funcionarios en general, con el objetivo de prepararlos para que puedan gestionar exitosamente un ciberincidentes, pero también para que implementen buenas prácticas, políticas y concientización en sus organizaciones, de manera de crear una cultura de trabajo basada en la ciberseguridad.

GESTIÓN DE MARCOS NORMATIVOS

4. Gestión de marcos normativos

Todas las organizaciones del Estado tienen la obligación cumplir lo establecido en las leyes, decretos e instructivos. Para facilitar que las organizaciones puedan saber cuáles son las normas de ciberseguridad que se deben seguir, el CSIRT cuenta con un repositorio de información en su sitio web, al cual todos los jefes de servicios, encargados de ciberseguridad, encargados de seguridad TI, funcionarios públicos, medios de comunicación y la ciudadanía pueden acceder.

Adicionalmente, el CSIRT ha comenzado a trabajar en una nueva serie de guías para apoyar la comprensión y orientación sobre las normas que las organizaciones deben cumplir y también sobre los estándares de ciberseguridad que se deben implementar.

Durante 2022 se promulgó la ley de delitos informáticos y se firmó el Decreto 273 sobre notificación de incidentes de ciberseguridad. Ambas normas se incorporaron en el catálogo de instrumentos que las instituciones tienen para gestionar la ciberseguridad en sus organizaciones.

4.1. Ley de Delitos Informáticos

La ley 21.459 se promulgó el 9 de junio de 2022 y se publicó el día 20 del mismo mes, establece las normas sobre delitos informáticos y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. Esta Ley actualiza la legislación chilena en materia de delitos informáticos, adecuándola a las exigencias del Convenio de Budapest, del cual Chile es parte.

Entre sus principales novedades, la ley tipifica como delitos informáticos las conductas de ataque a la integridad de un sistema informático, el acceso ilícito, interceptación ilícita, el ataque a la integridad de los datos informáticos, la falsificación informática, la receptación de datos informáticos, el fraude informático y el abuso de dispositivos.

Para estos delitos se contemplan penas, según su gravedad, que van desde presidio menor en su grado mínimo a presidio mayor en su grado mínimo, así como aplicación de multas. Adicionalmente, se incorporan circunstancias modificatorias de responsabilidad penal, en particular, como atenuante, la cooperación eficaz, y como agravantes, a modo ejemplar, cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función, o de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.

Asimismo, se agregan reglas especiales en materia de procedimiento, concediéndose legitimación activa al Ministerio del Interior y Seguridad Pública, delegados presidenciales regionales y delegados presidenciales provinciales cuando las conductas señaladas en la ley afecten servicios de utilidad pública. Se permite ordenar técnicas de investigación de aquellas reguladas en los artículos 222 a 226 del Código Procesal Penal, cumpliendo los requisitos previstos en la ley, y se hace referencia expresa al comiso y evidencia digital.

4.1. Decreto 273

El pasado 13 de septiembre de 2022, se estableció por decreto la obligación de reportar incidentes de ciberseguridad al Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior y Seguridad Pública, CSIRT.

El decreto, que fue publicado en el diario oficial el pasado viernes 2 de diciembre de 2022, se compone de cuatro artículos. Los artículos 1° y 2° abordan la notificación de incidentes de ciberseguridad y el plazo en que debe ser realizada la notificación. En el primer artículo se pone énfasis en la afectación del incidente. Una vez que el jefe de servicio toma conocimiento de esa afectación, este tiene que cumplir un plazo para informar sobre éste y sus alcances al CSIRT, notificación que se debe realizar a través de un formulario en el sitio web de la organización.

Para facilitar la notificación de incidentes, la comprensión de este decreto, y específicamente para entender cómo se debe proceder en el sitio web para la notificación, el CSIRT elaboró una guía especial que está disponible en el siguiente enlace: https://www.csirt.gob.cl/reportes/guia-y-resumen-decreto-273/. La guía también sirve de ayuda para entender algunos conceptos explicitados en el decreto, así como un anexo con la taxonomía que puede servir de orientación para clasificar un incidente y su afectación, y para distinguir si el incidente puede o no constituir un delito informático.

El artículo 3° del decreto trata sobre la gestión que se debe realizar para obtener información oportuna de parte de los proveedores de servicios de tecnologías de información sobre las amenazas y que ésta fluya hacia los órganos de la administración del Estado

Por último, el artículo 4° se refiere a la importancia de la búsqueda preventiva de vulnerabilidades en estos organismos del Estado. Para apoyar este aspecto en particular, el CSIRT también dispone de un beneficio para las organizaciones del Estado que estén interesadas, para realizar un escaneo de vulnerabilidades completando un formulario y cumpliendo algunos requisitos técnicos con ese objetivo.

ANÁLISIS DE GESTIÓN DE TICKETS

5. Análisis de gestión de tickets

Todos los incidentes de ciberseguridad que gestiona el CSIRT están vinculados a un ticket. Este instrumento permite que el incidente tenga una trazabilidad desde su reporte hasta su posterior respuesta y cierre. La historia del incidente está sintetizada en los tickets. En estos instrumentos de gestión podemos hallar indicadores de compromisos, información de los vectores de ataques, el presunto origen del incidente y la naturaleza de este, además de otros datos de las entidades afectadas y los activos involucrados. Toda esta información tiene una utilidad para la respuesta técnica y comunicacional del incidente, así como para prevenir que se expanda a otras entidades de similares sectores de la economía, del gobierno y de otras organizaciones.

Pero, así como constituye un activo de gestión en el contexto en que se gestiona el incidente, es también un testimonio de lo acaecido en un momento particular y de cómo se reaccionó individual y en conjunto para enfrentar el desafío en ese contexto. El ticket permite evaluar la reacción ante el incidente, la eficiencia y eficacia de los equipos y las herramientas, el cumplimiento de plazos de gestión, la pertinencia de las decisiones sobre la gestión, y en el mediano y largo plazo, pueden ayudar a calcular los costos de los incidentes, ya sean en términos de imagen como en la afectación directa a los servicios de negocio o de los servicios.

Expresado de otra manera, podemos decir que los tickets permiten gestionar la respuesta de un incidente, y a la vez, en su conjunto nos permiten obtener una imagen del ecosistema de la ciberseguridad en un momento determinado. Esa información, que para muchos puede tener un simple valor estadístico, es la que permite a los líderes de los negocios y a las autoridades políticas tomar decisiones sobre cómo implementar la ciberseguridad para garantizar la continuidad operativa, así como la integridad y disponibilidad de los activos informáticos de cada organización.

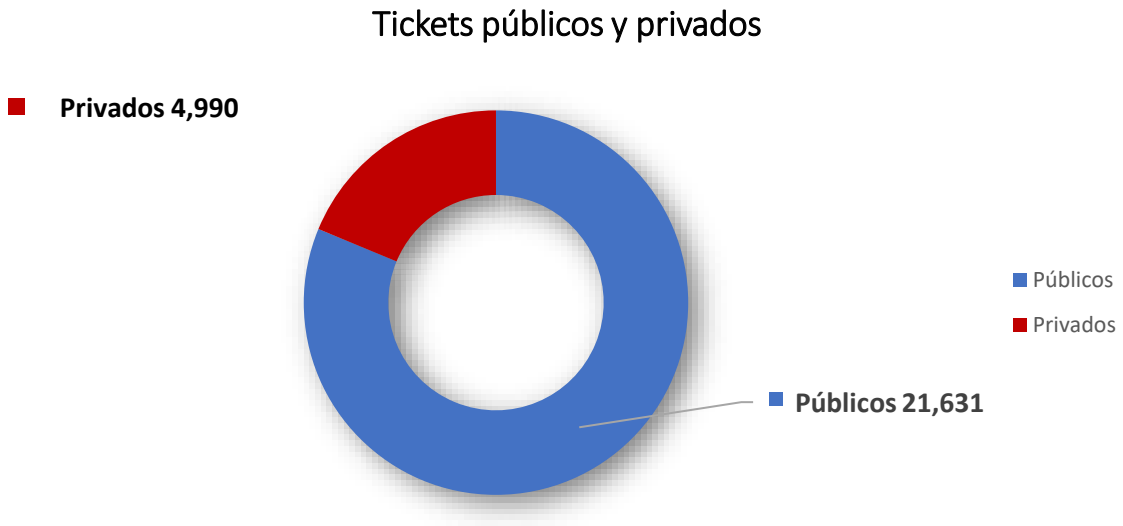
A nivel de gobierno, esta información permite orientar las políticas públicas sobre ciberseguridad, definir metas, prioridades y estrategias, quienes son los responsables de ejecutar las tareas y definir presupuestos con ese objetivo.

5.1. Reportes públicos y privados

Por su disposición estratégica, el CSIRT atiende mayoritariamente a incidentes dentro de organizaciones del Estado. En consecuencia, la mayoría de los tickets abiertos son de organizaciones de la administración pública, con un énfasis en aquellas que son parte de la Red de Conectividad del Estado (RCE).

Sin embargo, el CSIRT también monitorea sitios web de entidades que no pertenecen al Estado por estar en convenio de colaboración. El análisis de estos activos permite reconocer sobre todo vulnerabilidades, lo que explica también el aumento de este tipo de tickets dentro de la estadística anual.

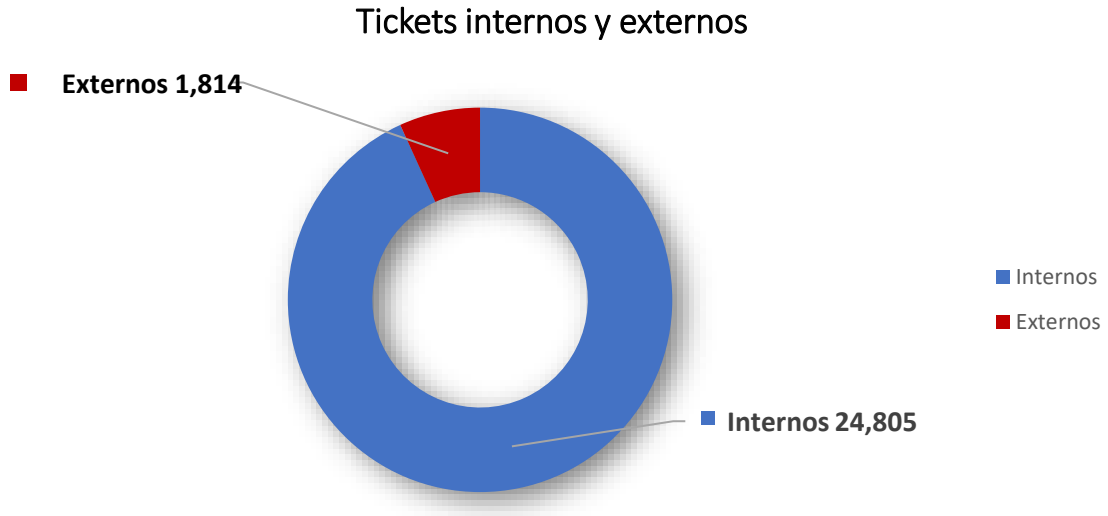
Tal como lo ilustra el gráfico, durante el año 2022 se abrieron 21.631 tickets de organizaciones públicas (83,3%) y 4.990 de organizaciones privadas (18,7%).



También se debe considerar que una parte de los tickets dirigidos a instituciones privadas son recibidos por reportes externos o en el tráfico de la RCE. Un ejemplo de incidentes pueden ser los correos de phishing bancario. Estos se reportan a las instituciones a las que suplantan para su consideración, constituyendo un reporte interno pero dirigido a una entidad externa.

5.2. Reportes internos y externos

La fuente del reporte del incidente que origina el ticket es relevante en varios aspectos: el resultado del trabajo de monitoreo y escaneo del CSIRT, el aporte de los canales de comunicación pública y la gestión de las plataformas de intercambio de información con agencias, proveedores, entidades en convenio, entre otros.



De acuerdo a la recopilación estadística de 2022, los tickets de origen externo (tickets reportados al el CSIRT) representaron un 6,8% (1.814 tickets) del total, mientras que los tickets internos (tickets reportados por el CSIRT) se encumbraron hasta alcanzar un 93,2% de los tickets (24.805 incidentes).

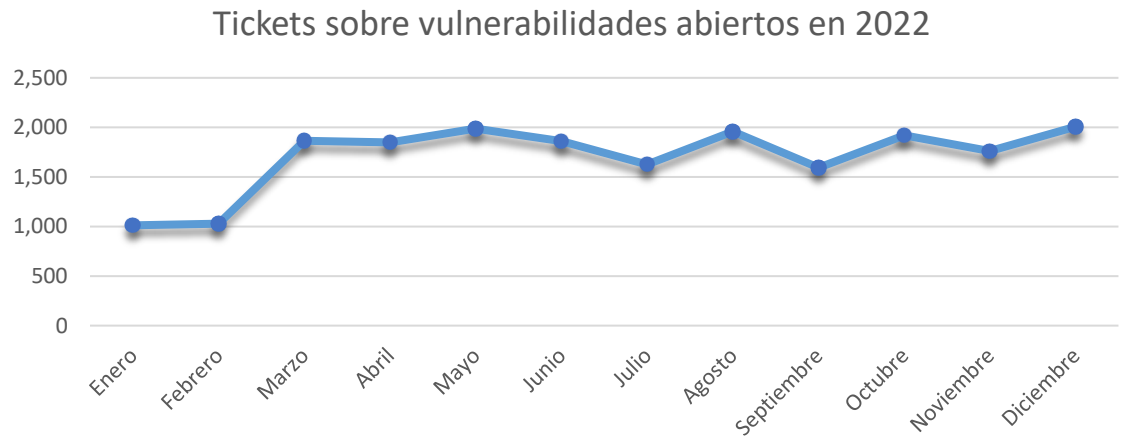
Pese a que disminuyó la creación de tickets externos en comparación años anteriores, el factor más determinante para la mayor cantidad de tickets internos está en el escaneo de vulnerabilidades, tanto a nivel del monitoreo de sitios web como en la gestión de beneficios que entrega el CSIRT a solicitud de las organizaciones.

En lo que respecta al origen del ticket externo, el formulario web fue el instrumento más utilizado (68,7% del total). Le siguieron el uso del correo electrónico (26,4%) y el call center (3,3%). El resto de las fuentes acumularon, entre todas, un 1,5%.

5.3. Vulnerabilidades

Las vulnerabilidades no constituyen un incidente por sí mismos. Muchas de ellas son detectadas por trabajos de escaneos periódicos que realiza el CSIRT en el proceso de monitoreo 24x7o por la gestión del área de escaneo de vulnerabilidades que analiza en detalle los activos informáticos que las organizaciones estiman convenientes evaluar.

Por sexto año consecutivo las vulnerabilidades a nivel global superaron las contabilizadas el año anterior alcanzando un total de 25.226, un incremento de un 25,1% respecto a lo registrado el 2021.



En este escenario, las organizaciones no sólo tienen el desafío de mitigar las nuevas vulnerabilidades, sino que conocer cuáles son aquellas que yacen en sus sistemas que por diferentes razones no han mitigado aún (desconocimiento de las vulnerabilidades y los parches publicados por los fabricantes, falta de capacidades para implementar correctamente las mitigaciones de seguridad sugeridas, la falta de gestión propia o de un proveedore de servicios, etc.).

Durante 2022, algunos de los incidentes más connotados que afectaron a nuestro ecosistema nacional fueron originados en vulnerabilidades que no fueron atendidas oportunamente.

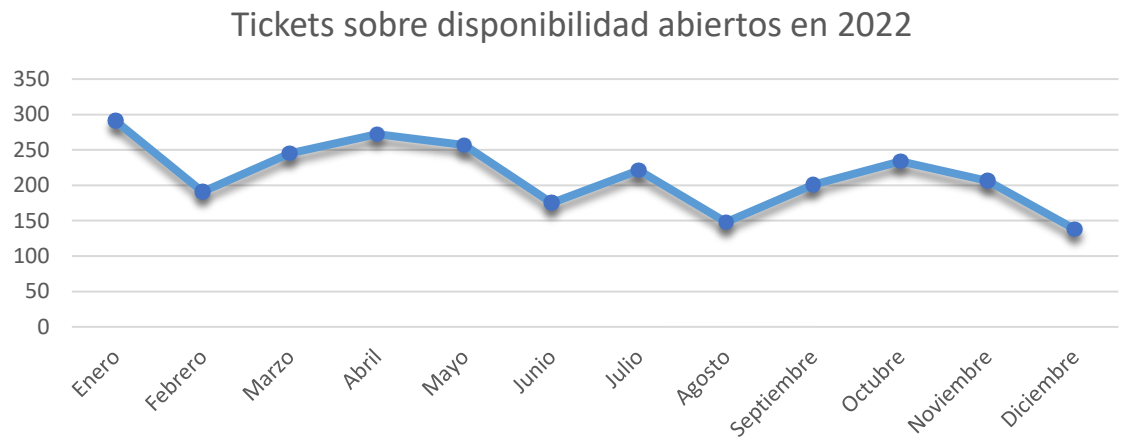
Como resultado del monitoreo permanente que se realizan sobre los sitios expuestos a la internet y que pertenecen a la Red de Conectividad del Estado, el CSIRT informa a las organizaciones que administran esos sitios sobre las vulnerabilidades detectadas en estos.

Durante el año 2022 fueron informadas 20.470 vulnerabilidades en sitios de gobierno (1.706 por mes), lo que equivale a un incremento de 53,1% respecto a 2021. En el total de tickets informados por el CSIRT, las vulnerabilidades acapararon el 76,9% el último año vs el 59,5% de 2021.

5.4. Disponibilidad

La disponibilidad es una de las tres dimensiones de la seguridad de la información. Dentro de la taxonomía que utiliza el CSIRT como guía para clasificar incidentes, la amenaza a la disponibilidad corresponde a la degradación de los accesos a los sistemas informáticos.

Una de las gestiones que realiza cotidianamente el CSIRT para mejorar este aspecto de la ciberseguridad de las organizaciones que pertenecen a de la red de conectividad del Estado (RCE) y las que están convenio de colaboración, es el monitoreo de sitios web. Las organizaciones que solicitan este beneficio completan un formulario en el que indican los sitios que deben ser monitoreados.



Durante el año 2022 se abrieron 2.579 tickets reportando este tipo de incidentes. Luego de las vulnerabilidades, los reportes de disponibilidad fueron la segunda mayor proporción de incidentes, un 9,7% del total. En enero de 2022 se registró la mayor cantidad de incidentes de este tipo (291 tickets). El resto del año se mantuvo siempre dentro de un promedio (215 incidentes mensuales), aunque el pasado mes de diciembre experimentó una disminución importante, registrando la cifra más baja de 2022, con tan solo 138 incidentes.

5.5. Fraude

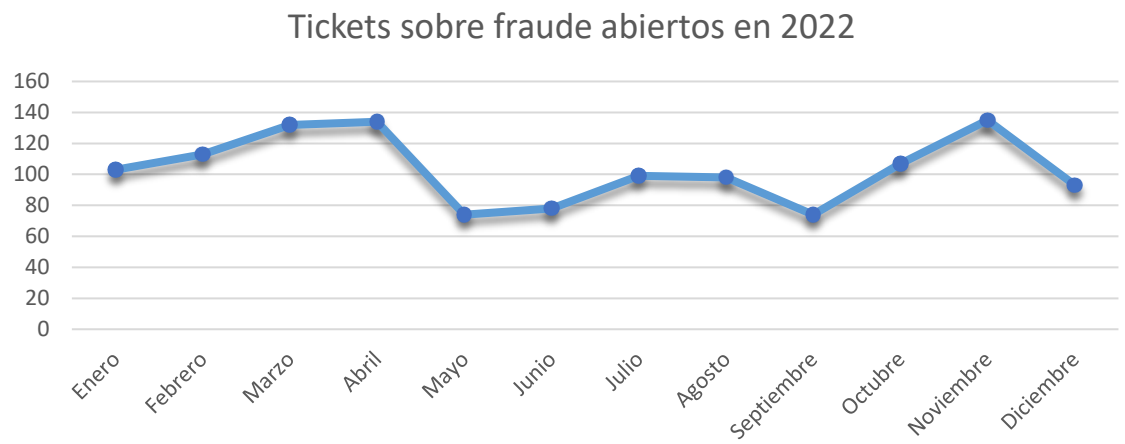
En esta sección se entiende como fraude informático todo aquel perjuicio patrimonial mediante la manipulación, alteración de datos o sistemas informáticos.

Entre los diferentes incidentes de este tipo que se gestionan en el CSIRT, se cuentan el uso no autorizado de recursos , la vulneración de los derechos de autor (Copia, distribución o instalación ilícita de activos digitales, por ejemplo, software comercial u otro tipo de material protegido), el phishing (envío de correos electrónicos que tienen apariencia legítima, pero que en realidad pretenden manipular al receptor para robar información) y la suplantación (el robo de identidad en internet para hacerse pasar por otra persona u organización con el fin de cometer actividades delictivas).

La mayoría de los reportes de incidentes corresponden a los tipos de phishing (por correo, mensaje de texto o smishing, redes sociales y mensajes dirigidos o spearphishing) y a la suplantación de sitios.

Muchos de estos tickets son reportados por fuentes externas y otra porción por análisis interno, pero en la mayoría de los casos la afectación es una organización ajena al Estado.

Este tipo de incidentes representa un 4,7% del total de lo reportado el año 2022, acumulando 1.240 tickets abiertos.



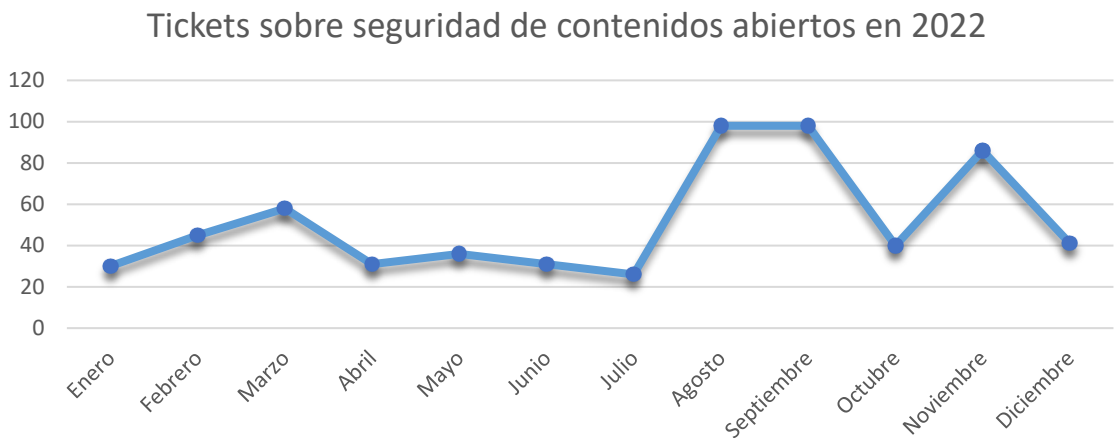
En la evolución de la curva se aprecia un crecimiento entre enero y abril (siempre arriba de los 100 casos mensuales), con un acentuado descenso en mayo. Desde entonces la cifra se mantiene estable hasta octubre en que se eleva a los 107 reportes y el noviembre en el que alcanza el récord anual (135 tickets), pero vuelve a bajar abruptamente en diciembre.

5.6. Información de seguridad de contenidos

Los incidentes de este tipo tienen que ver con eventos relacionados con la confidencialidad e integridad de la información, por lo tanto, comprende a dos de las tres dimensiones de la seguridad de la información.

Entre los tipos de incidentes que se pueden encontrar en esta tipificación están, el acceso no autorizado a la información (uso de permisos o credenciales obtenidas ilícitamente para acceder a servicios, recursos o activos informáticos), la exfiltración de información (extracción de datos que afecta la confidencialidad), la pérdida de información y la modificación no autorizada de información

(cualquier alteración ilícita sobre los datos de un sistema o aplicación que afectan su integridad, como un ataque de defacement).



La mayoría de los tickets reportados daban cuenta de ataques de defacement en infraestructuras externas, con bajos niveles de severidad e impacto en los respectivos negocios.

También se consideran en esta categoría algunos incidentes en el que los atacantes utilizan bases de datos exfiltradas en incidentes anteriores (algunas de larga data de obsolescencia), para crear la sensación pública de inseguridad. Esos tickets son investigados hasta que se descarta la vigencia de la información.

Durante el año 2022 se abrieron 620 tickets de este tipo, lo que representa un 2,3% del total. Solo los meses de agosto, septiembre y noviembre estuvieron muy por encima del promedio anual (52 incidentes mensuales).

5.7. Código malicioso

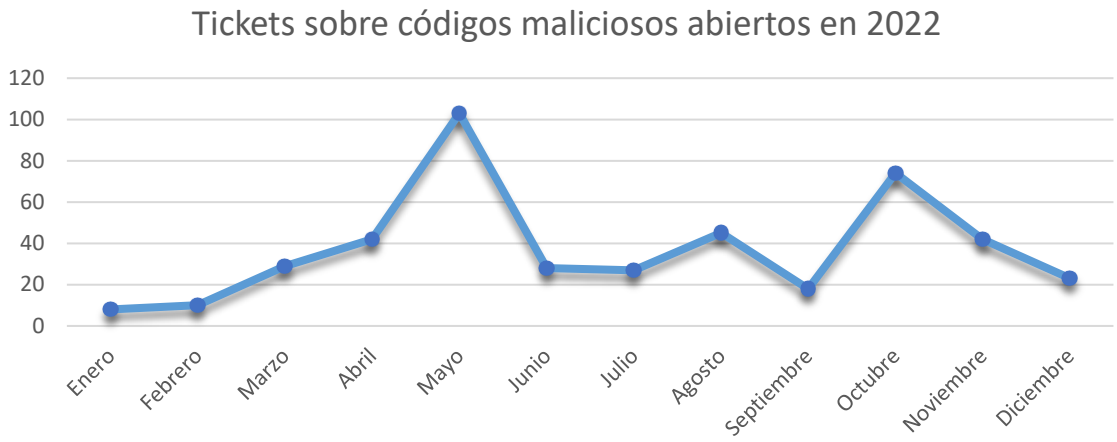
El código malicioso es un programa o código dañino, cuyo objetivo es afectar la confidencialidad, integridad o disponibilidad de la información. El principal vector de entrada del código malicioso es el correo electrónico, por medio del cual se distribuye un malware.

Los tickets sobre código malicioso son producto, por un lado, del reporte externo, y por otro, del trabajo de análisis sobre el tráfico de la red.

El CSIRT y la Red de Conectividad del Estado sistemáticamente introducen mejoras sobre el tráfico de red local. Las reglas aplicadas al Firewall de la RCE ayudan a discriminar con mayor precisión el tráfico normal, del tráfico malicioso. De este último se obtienen las muestras analizadas para advertir sobre potenciales amenazas, gestionar el incidente y, cuando corresponde, publicar una alerta de ciberseguridad.

En total, esta categoría acumuló 449 tickets, lo que equivale a un 1,7% del total de los incidentes gestionados el año 2022.

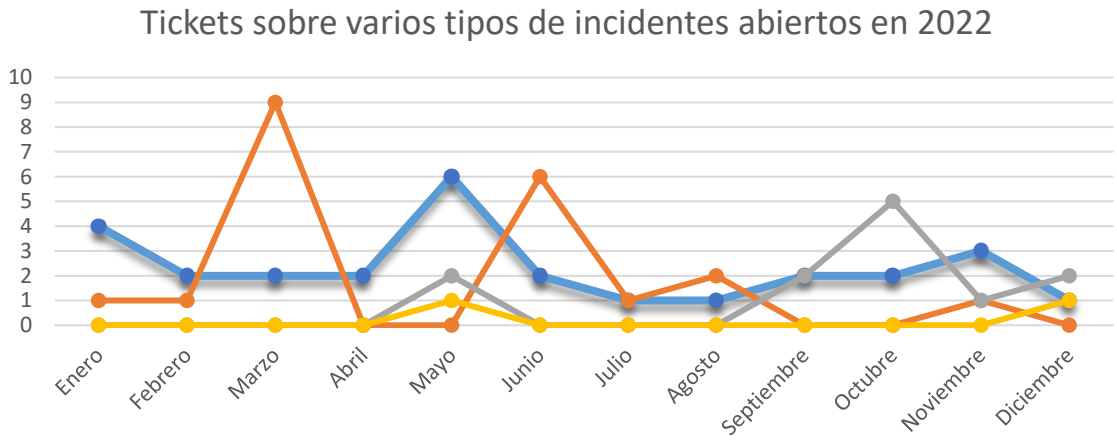
Con respecto al año 2021, los tickets sobre softwares maliciosos o malware disminuyeron en el total. Sin embargo, el comportamiento de la curva experimentó dos importantes alzas en los meses de mayo y octubre, para ajustarse a la baja en los meses finales del 2022.



La primera alza puede estar dentro de un contexto global de aumento de malware -la desactivación de grupos de ataque a finales del 2021 realizado por las policías en Europa y la división de otros en el contexto de la guerra entre Ucrania y Rusia-, el de la segunda mitad se explica tanto en el contexto de mejoras aplicadas al tráfico de red como en la reactivación temporal de Emotet.

5.8. Otros incidentes y tickets abiertos

CSIRT utiliza la clasificación de la taxonomía de ENISA (Agencia de la Unión Europea para la Ciberseguridad) para organizar la información de los tickets relacionados con incidentes y vulnerabilidades. Sin embargo, no todos los incidentes de esa taxonomía son gestionados por el CSIRT. Algunos, como los contenidos abusivos, que se refieren a incidentes que comprometen la imagen de una entidad, o en la mayor cantidad de veces a personas, mediante el uso de sistemas para realizar acciones que contienen aspectos prohibidos, ilícitos u ofensivos, por su connotación son derivados a las policías o fiscalía.



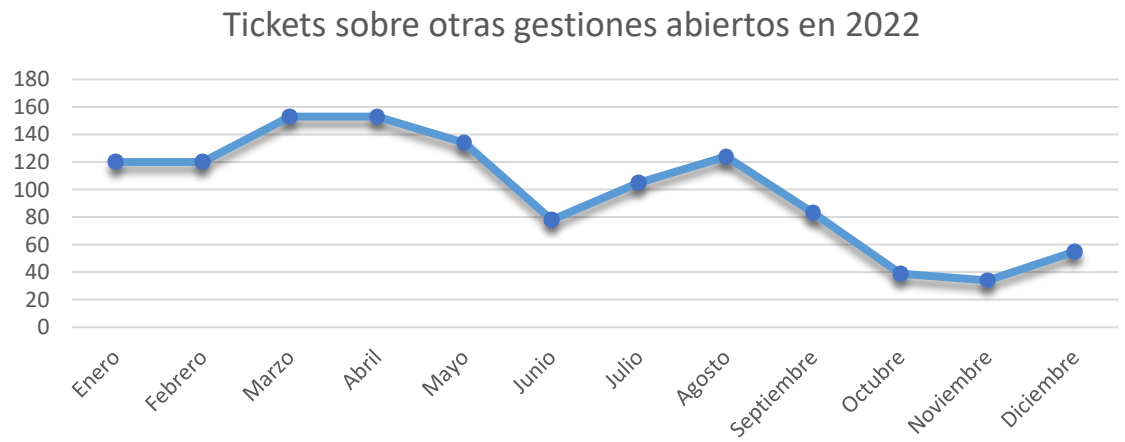
Otros incidentes, como los intentos de intrusión, la intrusión y la recopilación de información, se notifican con poca frecuencia por parte de las organizaciones afectadas. En estos dos casos, la vigencia del Decreto 273 podría cambiar esa estadística en el futuro.

En lo concreto, los tickets abiertos y relacionados con este tipo de incidentes son bajos en comparación con los restantes incidentes y vulnerabilidades. En 2022 se reportaron solo 63 tickets reunidos estas cuatro categorías, lo que no supera el 0,24% del total.

Los intentos de intrusión alcanzaron los 28 tickets (0,11%) y se reportó al menos 1 caso de este tipo en cada mes del año. Hubo otros 21 tickets (0,08%) con incidentes de contenidos abusivos, 12 (0,05%) con intrusiones y solo 2 (0,01%) con recopilación de información.

5.9. Otras gestiones

La taxonomía de ENISA no considera algunas de las gestiones que realiza como incidentes. Para atender esos tickets, se incorporó una categoría general en la que se reúnen los análisis controlados, consultas y otras gestiones propias de la organización.



La mayor parte de los tickets de esta categoría se relacionan con interacciones externas y su criticidad e impacto suele ser mediano o bajo. Pero también es importante comprender que algunos de estos tickets no tenían suficiente información como para ser catalogados correctamente en otras categorías.

La disminución de estos tickets, que se aprecia con mayor acento en la segunda mitad del año, da cuenta del trabajo en la mejora de gestión en la clasificación de información. Desde septiembre de 2022, la categoría “otros” está por debajo de los 100 tickets mensuales. En total se registraron 1.198 tickets de este tipo, lo que representa un 4,5% del total.

TRÁFICO MALICIOSO

6. Tráfico malicioso

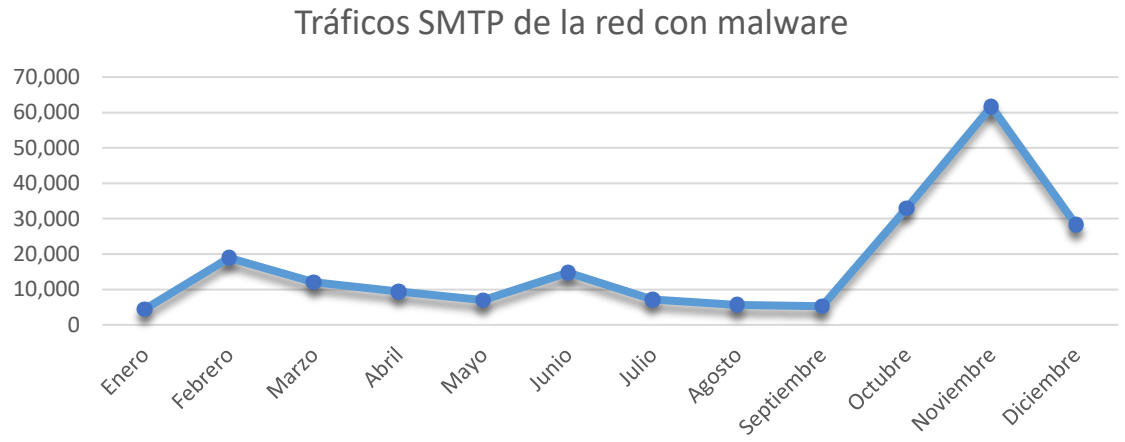
Una de las estrategias proactivas del CSIRT para proteger la red, se concentra en la configuración de sus herramientas para el bloqueo de contenido malicioso. Durante los últimos meses la RCE inició un proceso para actualizar sus motores de detección, lo que mejoró sustancialmente su eficiencia sobre el análisis de las bases de datos y patrones de ataques.

En este informe se incluye la estadística de esa gestión cuyo principal objetivo es bloquear y prevenir ataques de SQL, fuerza bruta, ataques conocidos (CVE) y escaneos de vulnerabilidades.

6.1. Correos con malware

Los correos maliciosos con malware representan una de las brechas de seguridad con las más altas tasas de infección, ya sea por medio de ataques phishing o phishing con malware. En lo que respecta al tráfico de correo analizado durante 2022, la mayoría de los archivos maliciosos portaban campañas de malware de Agent Tesla, Formbook, Mekotio, Emotet, Mispadu, entre otros.

La metodología más común utilizada por los atacantes intenta hacer creer a las víctimas que están frente a un correo legítimo, ya sea de algún pago de deuda, cotizaciones y facturas.

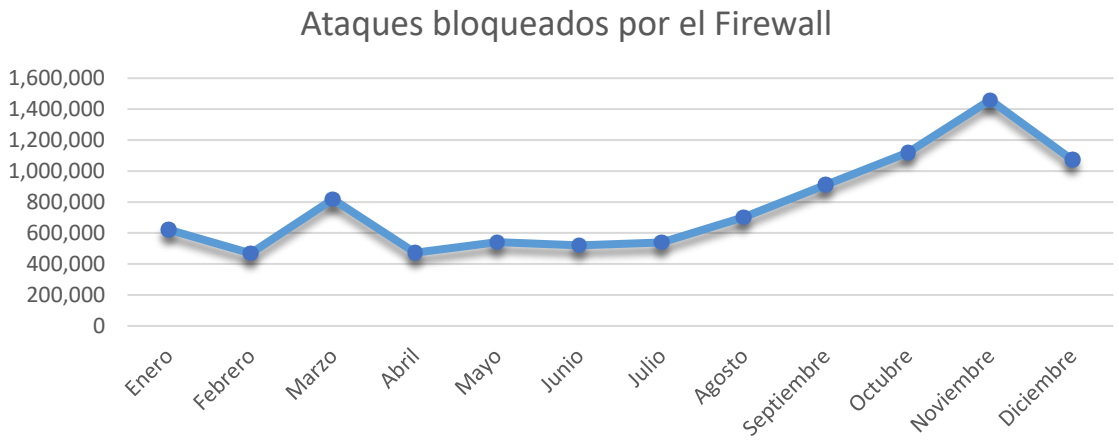


Durante 2022 fueron bloqueados 207.355 correos maliciosos en el tráfico de la red del Estado. Las mayores alzas se registraron a finales del año, entre octubre y diciembre, con su punta más alta en noviembre. La principal explicación del fenómeno yace en las mejorar introducidas en los motores de detección de correos maliciosos, lo que inició a finales del mes de septiembre.

6.2. Prevención de ataques

La prevención de ataques es una de las formas de contrarrestar los intentos de explotación de algunas vulnerabilidades. Las detectadas con mayor frecuencia en 2022 pertenecen a Wordpress, Vmware, Apache, Atlassian, Cisco, Citrix, F5, Joomla, Microsoft Exchange, Palo Alto, Oracle, Sophos, Solar Winds, Zimbra, entre otras.

Otra de las ventajas de la prevención de ataques es disminuir el escaneo de puerto que podría comprometer los activos una organización. El atacante utiliza esta estrategia para mapear los sistemas operativos, aplicaciones, servicios, puertos, entre otros.



Durante el año 2022 se realizaron 9.245.124 de bloqueos. La mayor parte del año el promedio estuvo por debajo los 600 mil bloqueos con puntas en marzo y agosto, para luego experimentar un alza sostenida entre septiembre y noviembre, llegando en este último mes a más de 1,4 millones de bloqueos. Pese a que en diciembre la cifra baja con respecto a noviembre, de todas maneras, está por encima del millón de bloqueos. Tal como se manifestó en un principio, el alza de finales de año se debe a las adecuaciones introducidas en el Firewall a partir de septiembre de 2022.

HERRAMIENTAS DE GESTIÓN

7. Herramientas de gestión (beneficios)

Durante el año 2022, el CSIRT trabajó en el desarrollo de una serie de herramientas de gestión de ciberseguridad con el objetivo de que estén disponibles para las organizaciones que pertenecen a la Red de Conectividad del Estado (RCE) y entidades que están en convenio de colaboración.

Entre las herramientas disponibles se encuentra el escaneo de vulnerabilidades. Este beneficio en particular está disponible para todas las organizaciones del Estado, con el objetivo de cumplir lo indicado en el Artículo 4° del Decreto 273, sobre la búsqueda preventiva de vulnerabilidades. La siguiente tabla muestra cuales son los beneficios y qué entidades pueden acceder a ellos.

HERRAMIENTA DE GESTIÓN	NORMATIVA QUE CUMPLE	BENEFICIARIO
Monitoreo web	Reglamento Ley n°21.180 Decreto Supremo n°1/2015 Instructivo Presidencial n°8	Organismos del Estado, Convenios
Escaneos de sitios	Decreto Supremo n°273/2022 Decreto Supremo n°1/2015 ISO27002:2022 Instructivo Presidencial n°8	Organismos del Estado
Alertas de incidentes y vulnerabilidades	Decreto Supremo n°273/2022 Instructivo Presidencial n°8 Decreto Supremo n°83	Organismos del Estado, Convenios
Campañas de concientización y buenas prácticas	Decreto Supremo n°83 ISO27002:2022	Organismos del Estado, Convenios
Capacitación para funcionarios	Decreto Supremo n°83 ISO27002:2022	Organismos del Estado
Intercambio de indicadores de compromiso	Decreto Supremo n°1/2015 ISO27002:2022	Organismos del Estado, Convenios
Detección y prevención de intrusiones	Decreto Supremo n°1/2015 ISO27002:2022 Decreto Supremo n°83	Red Conectividad del Estado
Auditorías de ciberseguridad	ISO27002:2022 Instructivo Presidencial n°8	Organismos del Estado, Convenios
Protección Anti DDoS	Reglamento Ley n°21.180 Instructivo Presidencial n°8	Red Conectividad del Estado
Protección Web Aplication Firewall (WAF)	Reglamento Ley n°21.180 Instructivo Presidencial n°8	Red Conectividad del Estado
Bloqueo preventivo de amenazas	ISO27002:2022 Decreto Supremo n°83	Red Conectividad del Estado
DNS Resolver	Decreto Supremo n°1/2015 Decreto Supremo n°14/2014	Red Conectividad del Estado
Creación de dominios ".gob.cl"	Decreto Supremo n°1/2015 Decreto Supremo n°14/2014	Entidades de Gobierno

Para optar a estos beneficios, las entidades deben contar con ciertos requisitos técnicos y lógicos mínimos y completar los formularios correspondientes.

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA
MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA
SUBSECRETARÍA DEL INTERIOR
https://www.csirt.gob.cl/
Teatinos 92 piso 6 Santiago, Chile
Teléfono 1510
soc-csirt@interior.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes
de Seguridad Informática