CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

INFORME MENSUAL GESTIÓN DE TICKETS CSIRT-GOBIERNO DE CHILE

MARZO 2023

ÍNDICE

Dirección Ingrid Inda Camino | **Edición general** Carlos Silva Caffi | |**Contenido y Diseño** Patricio Quezada Andaur | **Corrección de estilo** Carolina Covarrubias Escudero y Ramón Rivera Notario | **Contacto** comunicaciones@csirt.gob.cl | Equipo de Respuesta ante Incidentes de Seguridad Informática de Chile, **CSIRT de Gobierno, abril de 2023. Elaborado a partir de los datos de la OTRS del CSIRT de Gobierno.**

1. Acerca de la gestión de tickets

Todos los eventos e incidentes de ciberseguridad que gestiona el CSIRT de Gobierno están vinculados a un ticket. Este instrumento permite que el incidente tenga una trazabilidad desde su reporte, hasta su posterior respuesta y cierre.

En estos instrumentos de gestión podemos hallar indicadores de compromisos, información de los vectores de ataques, el presunto origen del incidente y su naturaleza (clase y tipo de incidente), además de información sobre las entidades y activos involucrados.

La historia del incidente está sintetizada en los tickets, y su utilidad no es solo es para la respuesta técnica y su acumulación estadística para la elaboración de políticas públicas en ciberseguridad. El ticket y la información que se reúne en este instrumento también permite que el CSIRT pueda asesorar en la respuesta práctica, acompañar la gestión de logros en la respuesta, ofrecer beneficios complementarios y guiar comunicacionalmente a la organización involucrada, además de prevenir al resto del ecosistema de los incidentes en curso.

1.1. Procesamiento de los tickets

Para procesar los tickets, el CSIRT de Gobiero utiliza como marco de referencia la taxonomía elaborada por la Agencia Europea de Ciberseguridad (ENISA). Dicha taxonomía fue adaptada para la gestión cotidiana del CSIRT e incluye 11 categorías, 37 subcategorías y 127 tipos de eventos e incidentes.

La gestión de incidentes tiene relación con la afectación en la confidencialidad, integridad o disponibilidad de los activos informáticos y se refiere a las categorías de contenido abusivo, código malicioso, recopilación de información, intentos de intrusión, intrusión, disponibilidad, información de seguridad de contenidos y fraude. El riesgo de incidentes se concentra en las categorías de vulnerabilidad y las de análisis controlado. Esta última es consecuencia de la gestión de permanente monitoreo y escaneo de vulnerabilidades que se realiza en el CSIRT.

1.2. Objetivo y características del informe

Este informe está dirigido a especialistas de ciberseguridad y al público en general, para transparentar la gestión técnica del CSIRT de Gobierno.

El informe reúne la estadística de ***marzo de 2023*** en relación con la gestión de los eventos e incidentes que están sintetizados en los tickets procesados durante ese período.

2. Reporte de tickets

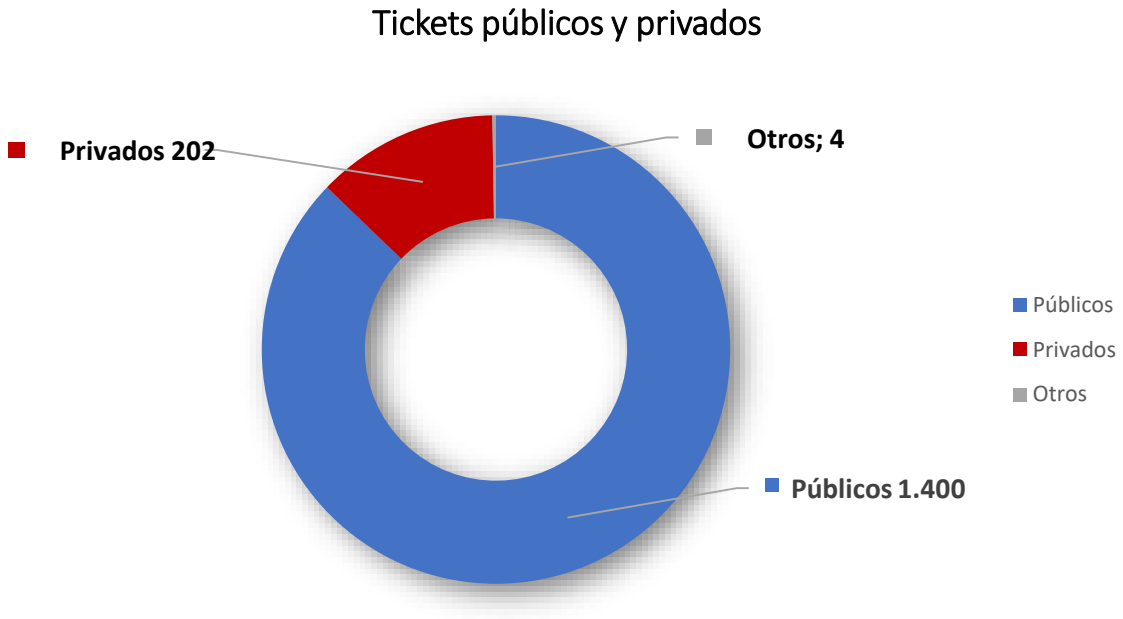
Este apartado recopila la información sobre la apertura del ticket, sus origines, a quien se dirige, el activo afectado y el medio utilizado para reportar.

2.1. Reportes públicos y privados

Por su disposición estratégica, el CSIRT de Gobierno 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).

De todas formas, el CSIRT también reporta incidentes de entidades privadas en su gestión de monitoreo, ya sea porque son parte de un convenio de colaboración o dada su importancia por los servicios estratégicos, sensibles o simbólicos que entrega a la ciudadanía. El análisis de estos activos permite reconocer principalmente incidentes de disponibilidad y vulnerabilidades con diferentes grados de riesgo, lo que se informa oportunamente a las organizaciones administradoras de esos activos.

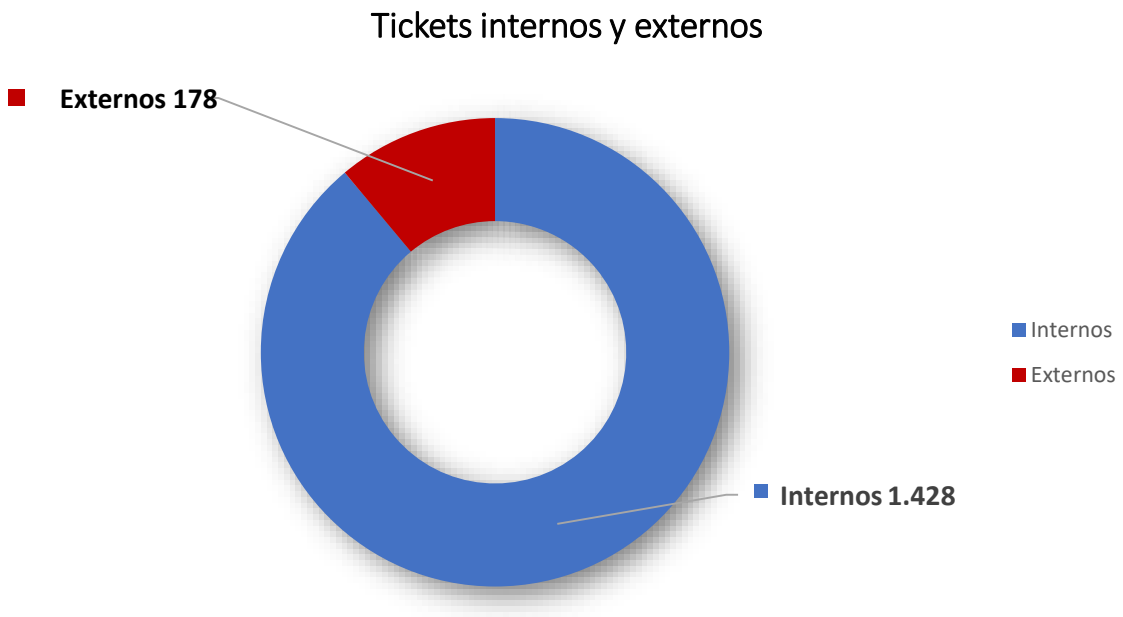
Adicionalmente, y producto de la relación con equipos de respuesta de incidentes de otros países y organizaciones internacionales, el CSIRT entrega y recibe ocasionalmente información sobre incidentes, los que se categorizan como “otros” en este reporte.



Durante el mes de marzo se procesaron 1.606 tickets, 1.400 fueron públicos (87,2%), 202 fueron privados (12,6%) y 4 (0,2%) están en la categoría de otros (internacionales).

2.2. Reportes internos y externos

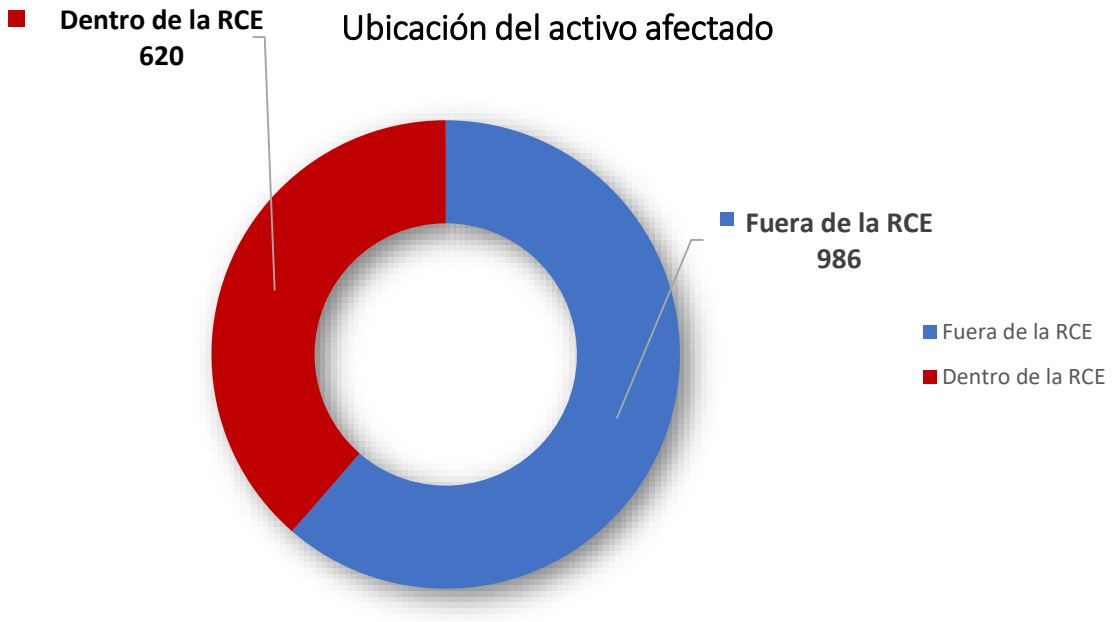
La fuente del reporte del incidente que origina el ticket es relevante en varios aspectos: el resultado del trabajo de monitoreo y escaneo de detección de vulnerabilidades del CSIRT, el aporte de los canales de comunicación pública y la gestión de las plataformas de intercambio de información con agencias,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



De acuerdo con la recopilación estadística de marzo, los tickets de origen externo representaron un 11,1% (178 tickets), mientras que los tickets internos alcanzaron un 88,9,2% (1.428 tickets).

2.3. Ubicación del activo afectado

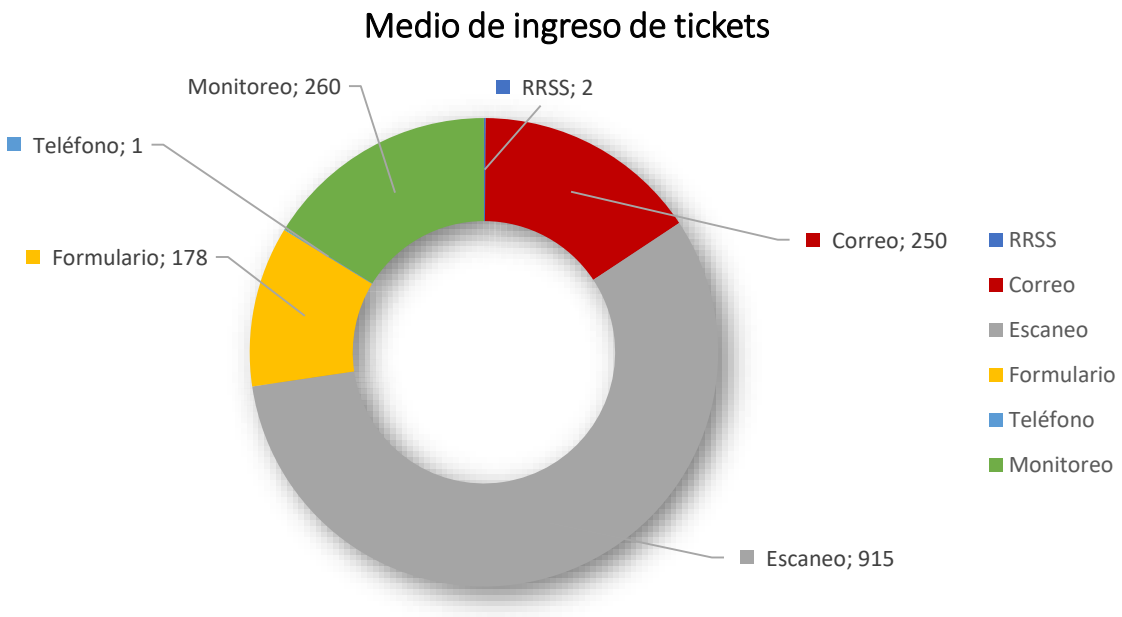
Los activos involucrados en un incidente pueden encontrarse dentro o fuera de la Red de Conectividad del Estado. Identificar el espacio en el que se encuentra ayuda a facilitar la aplicación de medidas preventivas, correctivas y de mitigación ante un evento o incidente.



Durante el mes de marzo, 986 eventos o incidentes (61,4%) fueron identificados fuera de la Red de Conectividad del Estado, mientras que 620 (38,6%) estaban dentro de la RCE.

2.4. Medio de ingreso

La fuente del reporte también permite identificar el medio utilizado para reportar o notificar un incidente. Los más utilizados son el producto del escaneo de vulnerabilidades, el monitoreo de disponibilidad, el formulario web, el correo electrónico, el análisis de tráfico, el teléfono y las redes sociales.



En el mes de marzo el 57,0% de los tickets (915) se originaron producto del escaneo de vulnerabilidades; un 16,2% (260 tickets) por el monitoreo de disponibilidad; un 15,6% (250 tickets) vía correo electrónico; un 11,1% (178 tickets) a través del formulario web; un 0,1% (2 tickets) por redes sociales; y 0,1% (1 ticket) vía teléfono.

2.5. Notificación según el Decreto 273

El Decreto Supremo 273, sobre la notificación de incidentes de ciberseguridad, y que fue publicado en el Diario Oficial en el mes de diciembre de 2022, indica que los Jefes de servicio de las organizaciones de la Administración Pública del Estado deben reportar incidentes al CSIRT de Gobierno. Esta sección acumula la estadística de reportes en torno a la materia.

En el mes de marzo se reportaron 16 incidentes (1,0%) por parte de organizaciones de la Administración Pública del Estado argumentando el Decreto 273.[1]

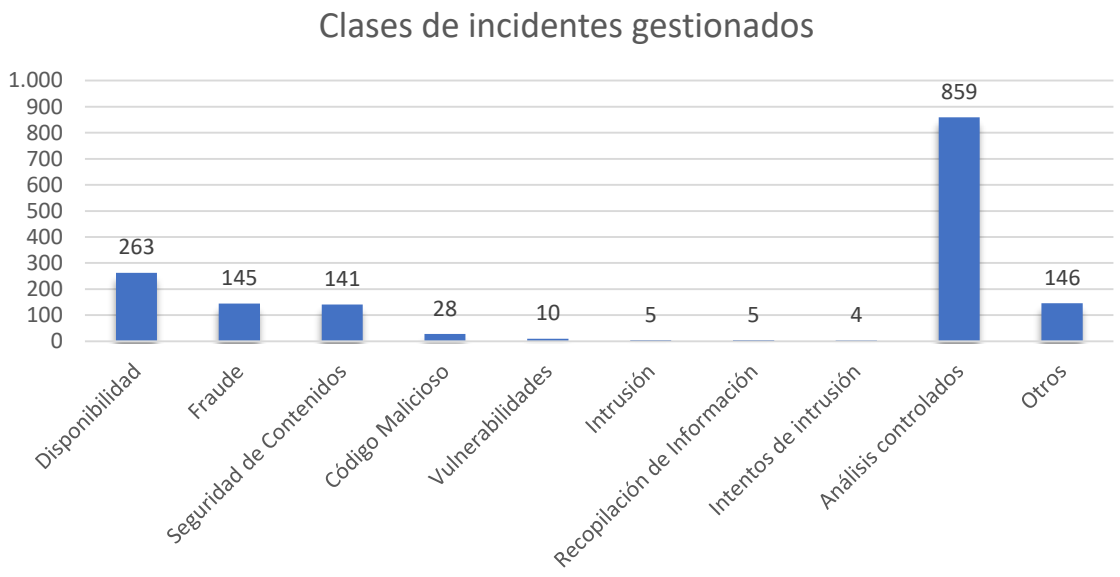
[1] Es importante considerar que la vigencia de la norma es reciente. Existe la expectativa de que el número aumente conforme se haga más conocido el alcance del D.S. 273.

3. Procesamiento del ticket

Este apartado recopila la información sobre el procesamiento del ticket. Incluye información sobre la clase y el tipo de incidente, sobre el nivel de afectación y sobre el nivel de peligrosidad.

3.1. Clase de incidentes

Las categorías contenidas en este apartado se dividen entre aquellas que están directamente asociadas a incidentes (contenido abusivo, código malicioso, recopilación de información, intentos de intrusión, intrusión, disponibilidad, información de seguridad de contenidos y fraude) y aquellas que pueden derivar en un incidente (vulnerabilidades y análisis controlados). También se incluye en este apartado a otros tickets de gestión interna bajo la denominación "otros".



De los 1.606 tickets registrados este mes de marzo, el 53,3% (859 tickets) correspondieron a análisis controlados. Los incidentes de disponibilidad representaron el 16,4% del total (263 tickets), seguido por fraudes con el 9,0% (145 tickets), seguridad de contenidos con el 8,8% (141 tickets), código malicioso con el 1,7% (28 tickets), las vulnerabilidades con el 0,6% (10 tickets), la recopilación de información con el 0,3% (5 tickets), la intrusión con el 0,3% (6 tickets), y los intentos de intrusión con el 0,2% (4 tickets). Los tickets clasificados como "otros" representaron el 9,1% (146 tickets), mientras que bajo la categoría de contenido abusivo no se registraron tickets.

3.2. Tipos de incidentes

Cada clase de incidente tiene una subcategoría, la que a su vez describe un tipo específico de incidente. Los siguientes son los tipos de incidentes específicos que fueron informados durante el mes que se informa.

26 tipos específicos de eventos e incidentes fueron descritos en los tickets reportados durante el mes de marzo de 2023. El 53,3% de ellos corresponden a escaneos de vulnerabilidades (856 tickets), que son parte de los análisis controlados que realiza el CSIRT.

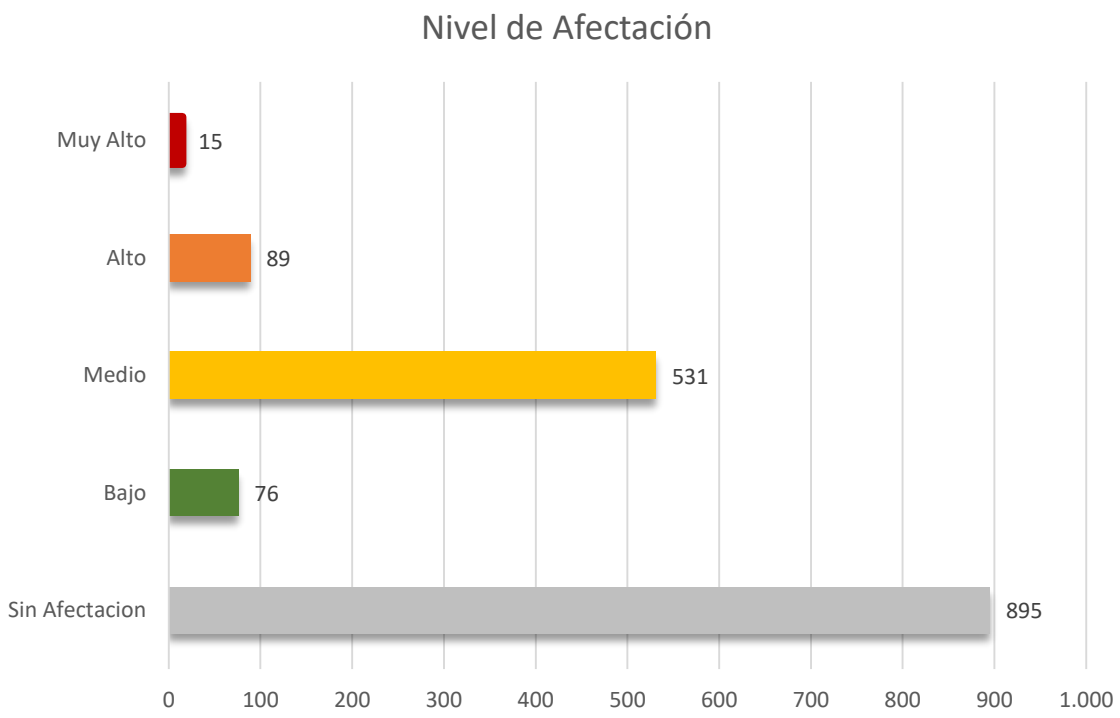
Entre los tipos de incidentes, los más recurrentes son la interrupción con 13,4% (293 tickets), la interrupción con el 13,4% (215 tickets), la exfiltración de información con 5,8% (93 tickets), la suplantación con el 4,5% (73 tickets), el phishing con un 4,5% (72 tickets), la disponibilidad con un 2,9% (47 tickets), la modificación no autorizada de información con el 2,8% (45 tickets), y los sistemas infectados con el 1,6% (26 tickets).[2]

[2] Se destacan los incidentes identificados que superaron el umbral de 1% y que no correspondan a la categoría de otros.

Nivel de afectación

El nivel de afectación corresponde al impacto real o potencial causado por un incidente de ciberseguridad. Todos los incidentes de ciberseguridad tienen algún grado de afectación. En la descripción de los tickets se utilizan las categorías de no afectación, así como afectación baja, media, alta, muy alta y crítica.

La afectación es normalmente identificada por la entidad afectada, pero puede ser evaluado por los analistas del CSIRT de acuerdo con la descripción del incidente entregada por la parte involucrada.

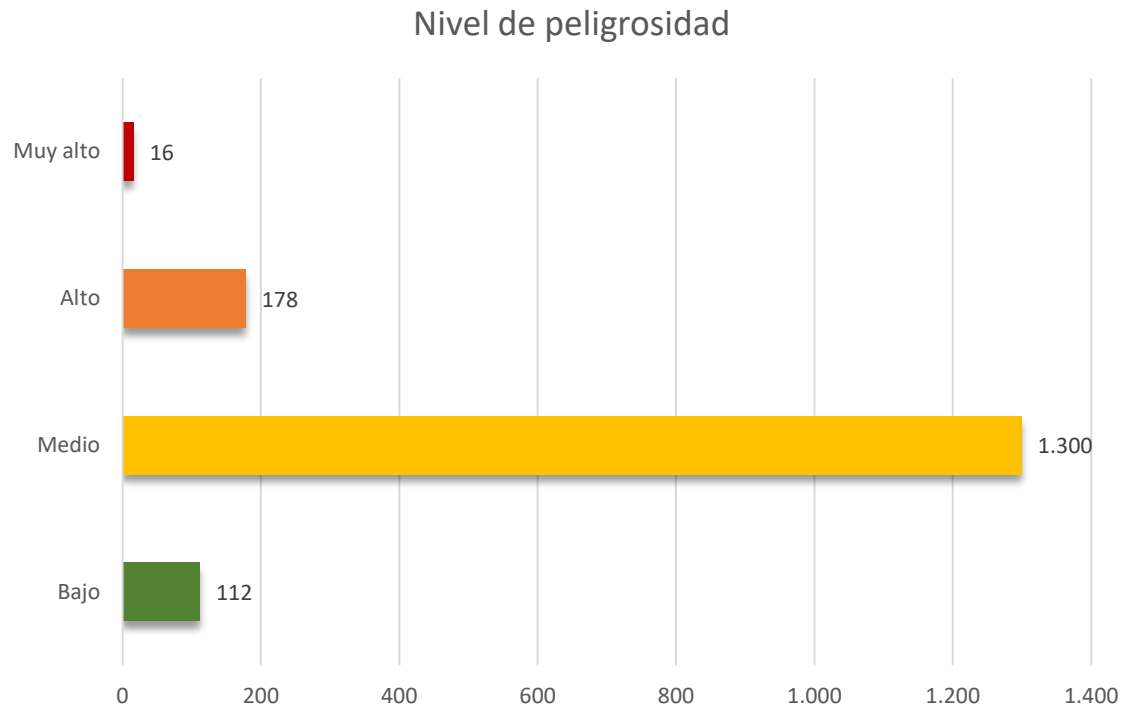


En el mes de marzo un 55,7% de los eventos e incidentes de ciberseguridad (895 tickets) no tuvieron afectación. El 33,1% de los incidentes (531 tickets) tuvo una afectación media, el 5,5% (89 tickets) tuvo una afectación alta, el 4,7% (76 tickets) tuvo una afectación baja y el 0,9% (15 tickets) tuvo una afectación muy alta.

3.3. Nivel de peligrosidad

El nivel de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en las redes, equipos y sistemas de una organización, así como para la calidad o continuidad en el otorgamiento de sus servicios.

Conforme a sus características, las amenazas son clasificadas con los siguientes niveles de peligrosidad: bajo, medio, alto, muy alto y crítico.



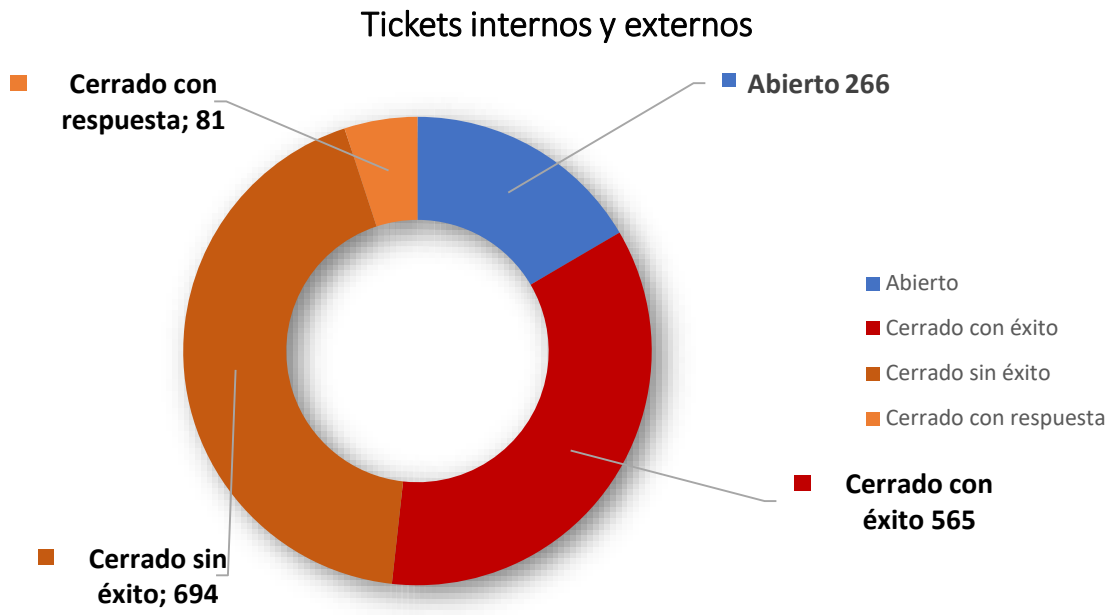
En el mes de marzo un 80,9% de los eventos e incidentes de ciberseguridad (1.300 tickets) fueron de peligrosidad media. El 11,1% de los incidentes (178 tickets) fueron de peligrosidad alta, el 7,0% (112 tickets) fueron de peligrosidad baja, y el 1,0% (16 tickets) fueron de peligrosidad muy alta.

4. Estatus del ticket

Este apartado recopila la información sobre el estado en el que se encuentran los tickets al momento de elaborar este reporte.

4.1. Estado del ticket

Los tickets gestionados a través de la plataforma de CSIRT se clasifican en abiertos, cerrados sin éxito, cerrados con respuesta y cerrados con éxito.



El 16,6% (266) de los tickets de marzo se mantienen abiertos, mientras que el 83,4% (1.340 tickets) fueron cerrados. De los tickets cerrados, un 43,2% (694 tickets) fueron cerrados sin éxito, un 35,2% (565 tickets) fueron cerrados con éxito y un 5,0% (81 tickets) fueron cerrados con respuestas.

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 Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.04.06 21:54:19 -04'00'

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática