CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

INFORME MENSUAL GESTIÓN DE TICKETS CSIRT-GOBIERNO DE CHILE

ABRIL 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 del Gobierno de Chile, **CSIRT de Gobierno, Mayo 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 de Gobierno 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 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 del mes de **abril 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

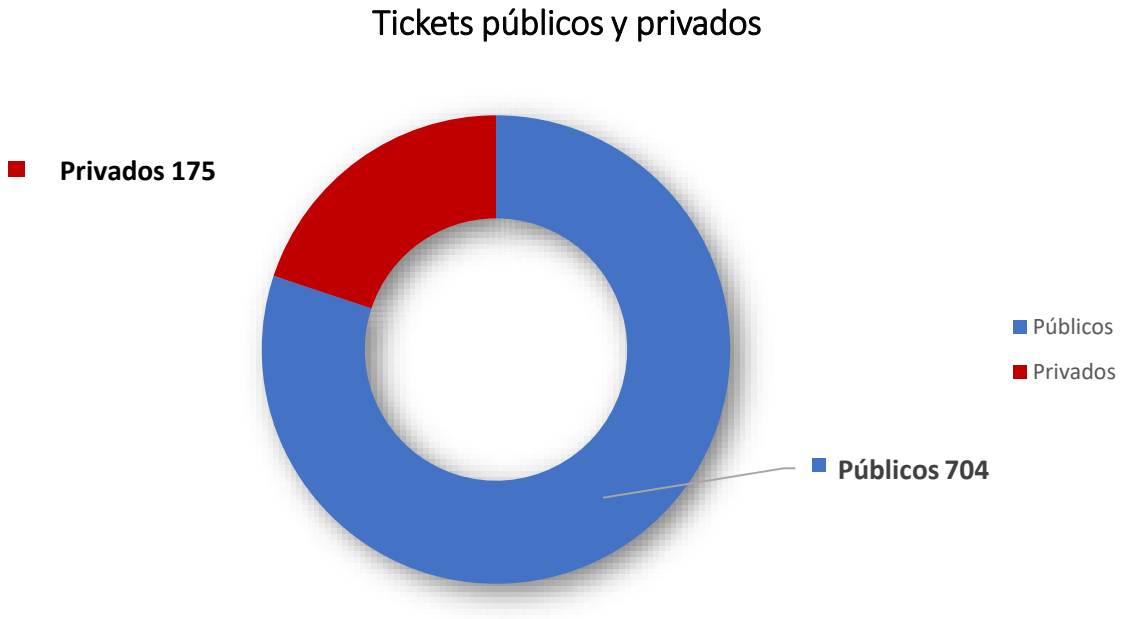
Este apartado recopila la información sobre la apertura del ticket, sus origines, a quien se dirige, el activo afectado y el medio utilizado para reportar.

2.1. Reportes públicos y privados

Por su disposición estratégica, el CSIRT 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.

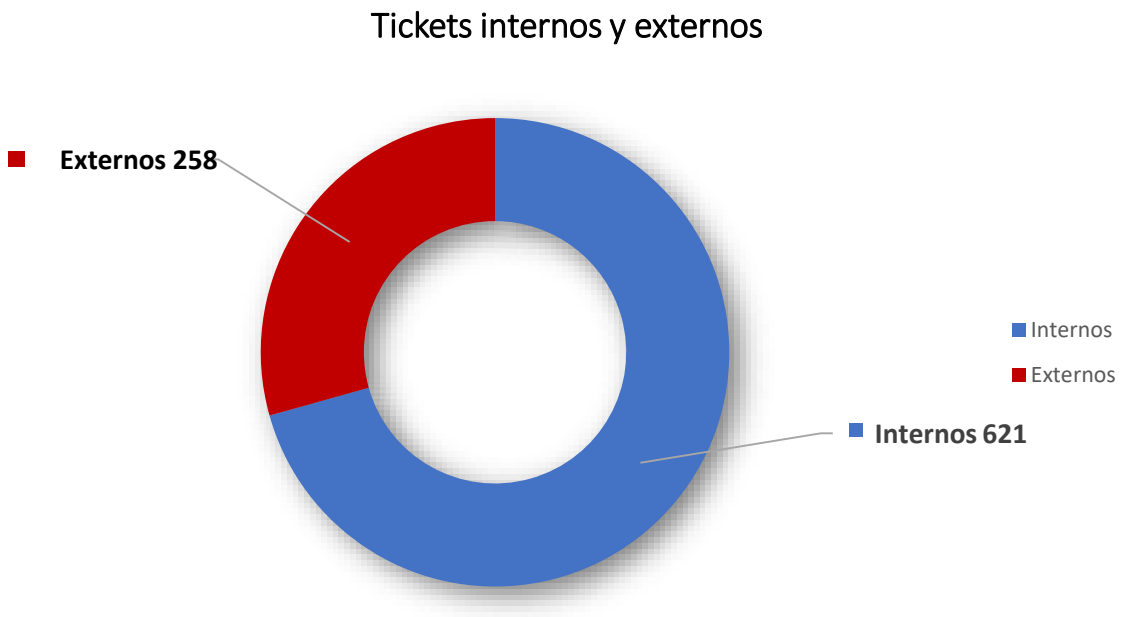
Adicionalmente, y producto de la relación con equipos de respuesta de incidentes de otros países y organizaciones internacionales, el CSIRT entrega y recibe ocasionalmente información sobre incidentes, los que se categorizan como “otros” en este reporte.



Durante el mes de abril se procesaron 879 tickets, de estos, 704 fueron públicos (80,1%) y 175 fueron privados (19,9%).

2.2. Reportes internos y externos

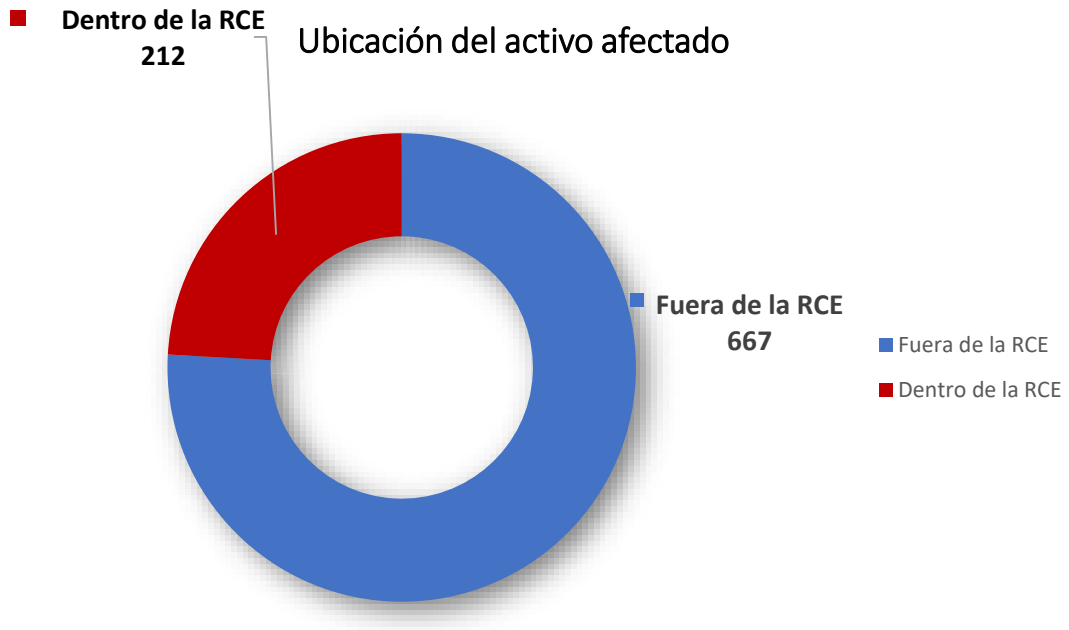
La fuente del reporte del incidente que origina el ticket es relevante en varios aspectos: el resultado del trabajo de monitoreo y escaneo de detección de vulnerabilidades del CSIRT, el aporte de los canales de comunicación pública y la gestión de las plataformas de intercambio de información con agencias,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



De acuerdo con la recopilación estadística de abril, los tickets de origen externo representaron un 29,4% (258 tickets), mientras que los tickets internos alcanzaron un 70,6% (621 tickets).

2.3. Ubicación del activo afectado

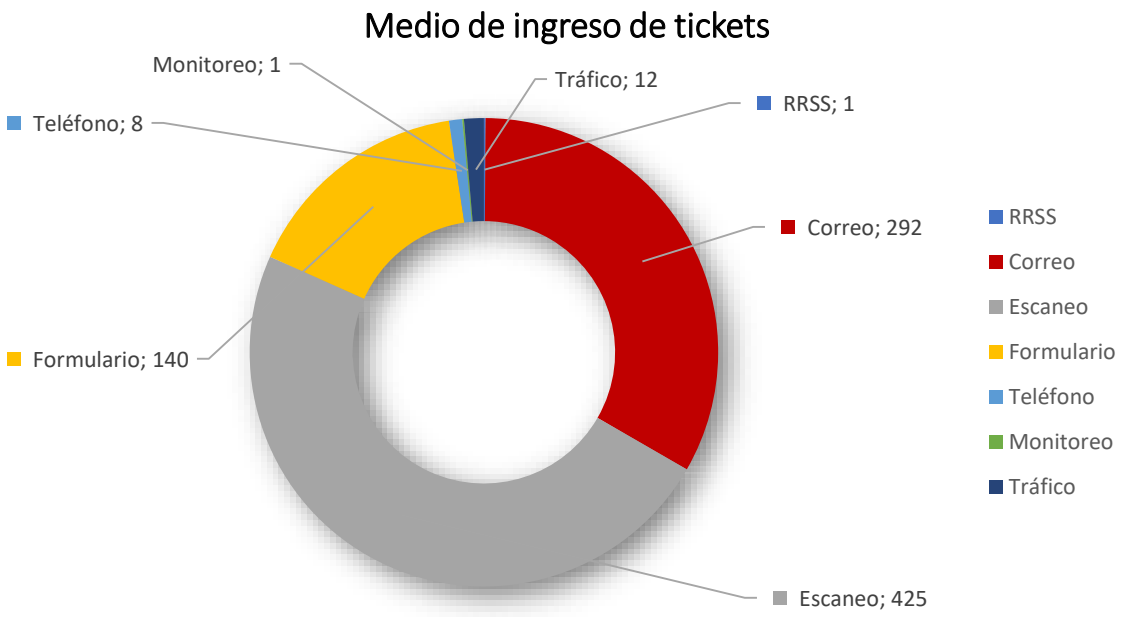
Los activos involucrados en un incidente pueden encontrarse dentro o fuera de la Red de Conectividad del Estado (RCE). Identificar el espacio en el que se encuentra ayuda a facilitar la aplicación de medidas preventivas, correctivas y de mitigación ante un evento o incidente.



Durante el mes de abril, 667 tickets (75,9%) fueron identificados fuera de la Red de Conectividad del Estado, mientras que 212 (24,1%) 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 abril el 48,8% de los tickets procesados (425 tickets) se originaron producto del escaneo de vulnerabilidades; un 33,2% (292 tickets) ingresaron por correo electrónico; un 15,9% (140 tickets) llegaron por formulario web; un 1,4% (12 tickets) se crearon a partir del análisis de tráfico; un 0,9% (8 tickets) llegaron por teléfono, y por redes sociales y monitoreo de disponibilidad se registraron un ticket respectivamente, lo que equivale a un 0,1%.

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 abril se notificaron cuatro incidentes (0,5%) por parte de organizaciones de la Administración Pública del Estado argumentando el Decreto 273.[1]

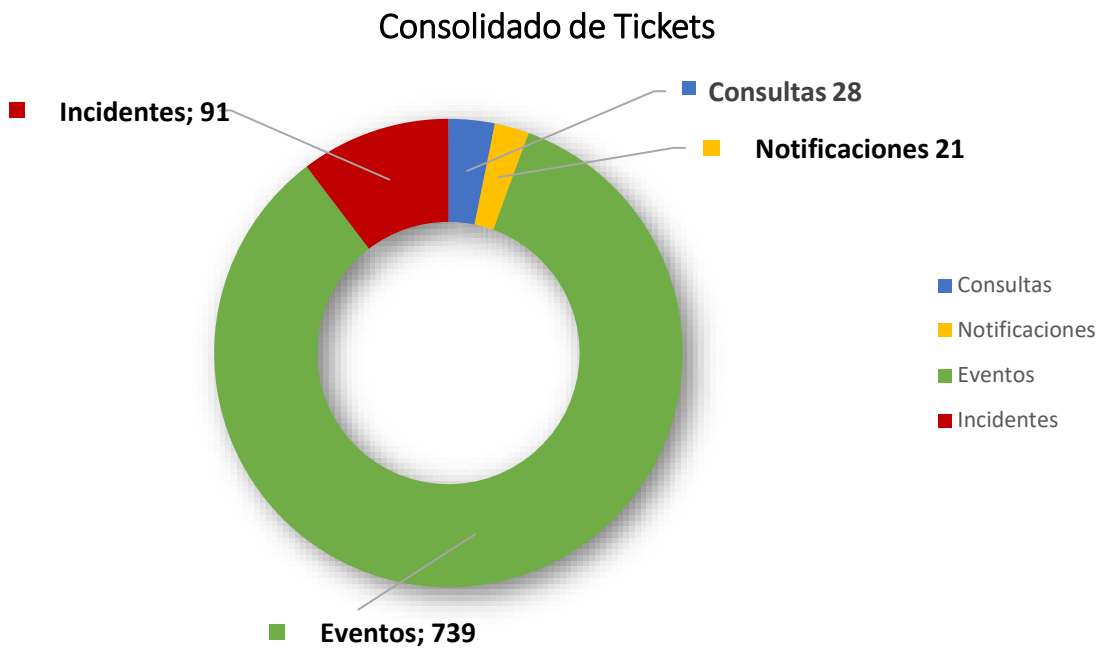
[1] Es importante considerar que la vigencia de la norma es reciente. Existe la expectativa de que el número aumente conforme se haga más conocido el alcance del D.S. 273.

3. Procesamiento del ticket

Este apartado recopila la información sobre el procesamiento de los tickets, identificando la categoría de su procesamiento, así como la clase y el tipo al que se adscriben de acuerdo a la taxonomía asignada, su nivel de afectación y el nivel de peligrosidad.

3.1. Categorías de tickets procesados en el mes de abril

Los tickets gestionados a través de la plataforma de CSIRT se procesan según cuatro categorías: notificaciones, consultas, eventos o incidentes.



Durante el mes de abril se procesaron 879 tickets, de los cuales el 84,1% (739 tickets) correspondieron a eventos, e 10,4% (91 tickets) a incidentes, el 3,2% (28 tickets) a consultas y un 2,4% (21 tickets) a notificaciones.

3.2. Tickets procesados como consultas y notificaciones

Para los propósitos de la gestión de tickets, se entiende como **consulta**, toda pregunta general o específica que no tiene relación directa con la existencia de un incidente o evento informático que afecta a alguna organización o persona, o toda pregunta que debe ser redirigida a otra entidad para la gestión de su respuesta.

Por otra parte, se entiende como **notificación**, toda situación en la que una tercera parte (persona u organización) reporta que otra organización está siendo afectada por un incidente.

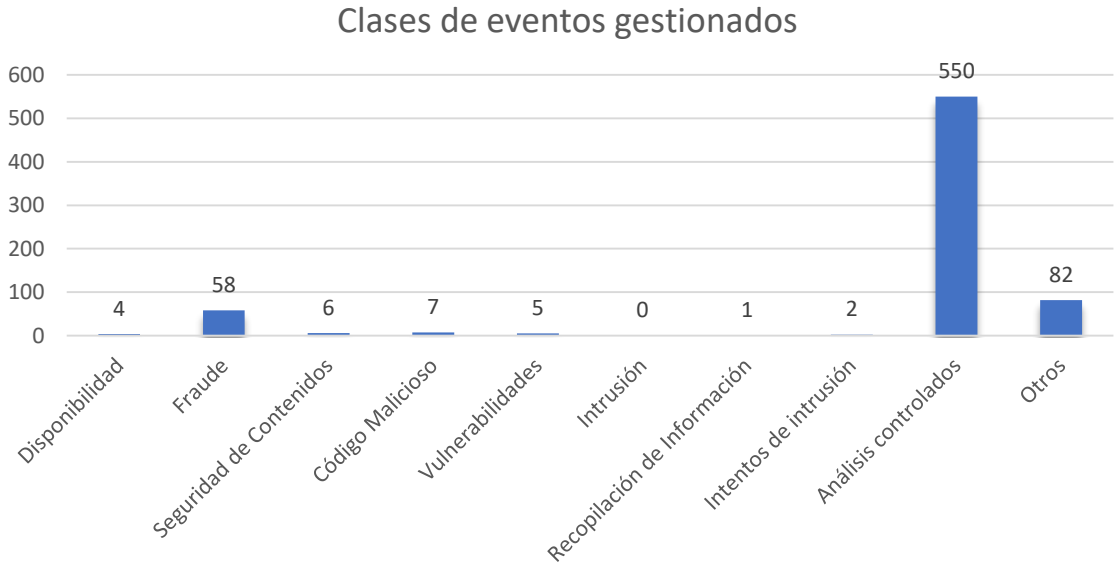
Este informe no profundiza en los detalles de ambas categorías por tratarse de situaciones que no tienen afectación o peligrosidad directa.

3.3. Tickets procesados como eventos de ciberseguridad

Para los propósitos de la gestión de tickets en el sistema OTRS del CSIRT, así como para este informe, se entiende como evento de ciberseguridad, toda situación en la que se produce el hallazgo de un riesgo o amenaza que, de ser explotada, podría poner en riesgo los activos informáticos de personas u organizaciones, por ejemplo, el hallazgo de vulnerabilidades, el reporte de phishing o fraude que no ha sido explotad o indicadores de compromiso.

3.4. Clase de eventos

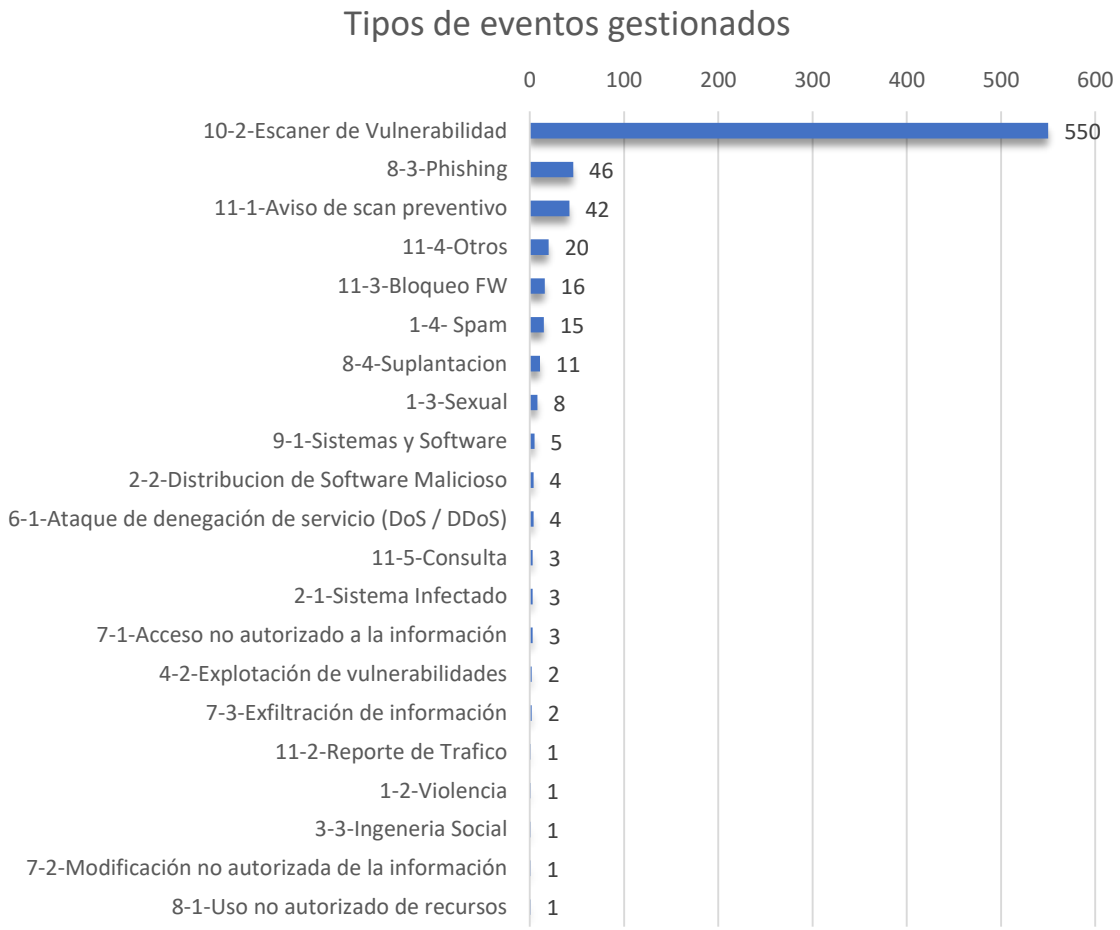
Los tickets de este apartado corresponden a situaciones que pueden derivar en un incidente en caso de ser explotadas. En la mayoría de los casos fueron tickets abiertos por el CSIRT como resultado de un análisis controlado (monitoreo preventivo o escaneo solicitado), además de vulnerabilidades halladas por el CSIRT o terceras partes y reportes sobre amenazas que no resultaron en una afectación a personas u organizaciones.



El mes de abril se registraron 739 eventos, de ese universo, un 74,4% (550 tickets) correspondieron a análisis controlados. Los eventos relacionados con amenazas a los fraudes alcanzaron un 7,8% (58 tickets), mientras que los contenidos maliciosos acumularon un 3,2% (24 tickets), los de código maliciosos un 0,9% (7 tickets), los relacionados a seguridad de contenidos a 0,8% (6 tickets), los de disponibilidad a 0,5% (4 tickets), los intentos de intrusión a 0,3% (2 tickets) y la recopilación de información a 0,1% (1 ticket). Los tickets clasificados como “otros” representaron el 11,1% (82 tickets), mientras que bajo la categoría de intrusión no se registraron eventos.

3.5. Tipos de eventos

Cada clase de evento tiene una subcategoría. Los siguientes son los tipos de eventos específicos que fueron informados durante el mes pasado.



21 tipos específicos de eventos fueron descritos en los tickets reportados durante el mes de abril de 2023. El74,4% de ellos corresponden a escaneos de vulnerabilidades (550 tickets), que son parte de los análisis controlados que realiza el CSIRT.

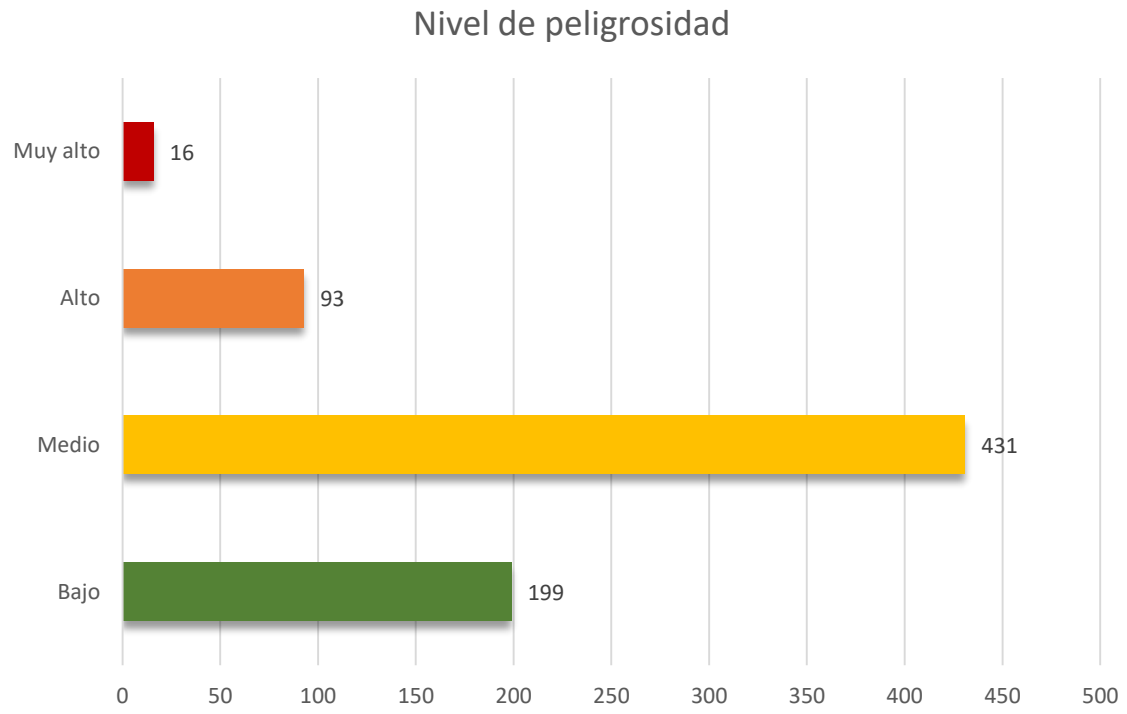
Entre los tipos de eventos, los más recurrentes son el phishing con 6,2% (46 tickets), los avisos de escaneos preventivos con 5,7% (42 tickets), el bloqueo de firewall con 2,2% (16 tickets), el spam con 2,0% (15 tickets), la suplantación con 1,5% (11 tickets), y la extorsión sexual o de otro tipo con 1,1% (8 tickets).[2]

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

3.6. Nivel de peligrosidad

El nivel de peligrosidad determina la potencial amenaza que supondría la explotación de un evento de ciberseguridad 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.



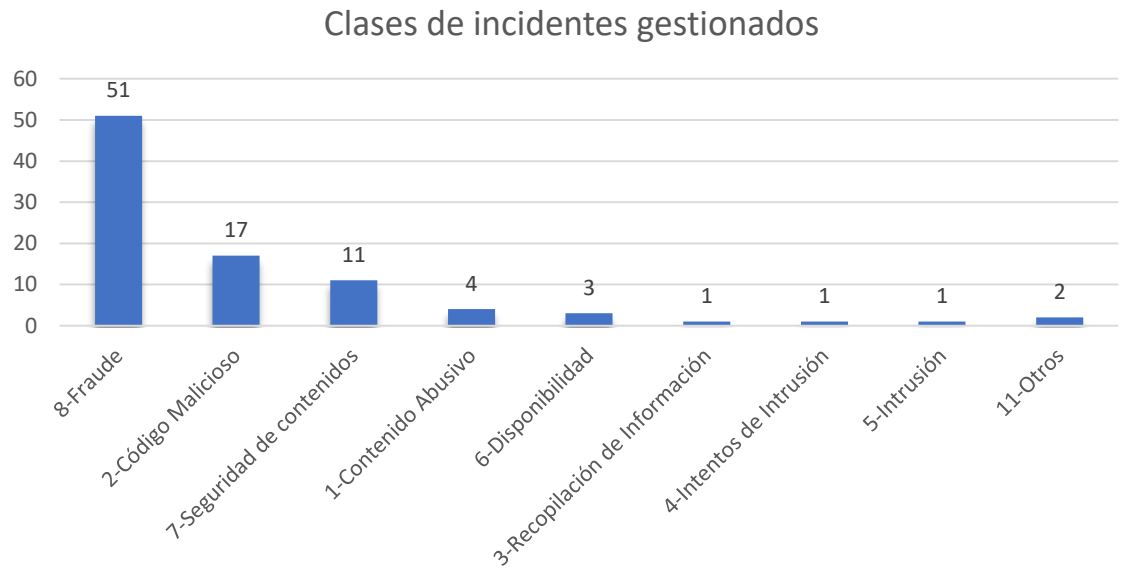
En el mes de abril un 58,3% de los eventos de ciberseguridad (431 tickets) fueron de peligrosidad media. El 26,9% de los eventos (199 tickets) fueron de peligrosidad baja; el 12,6% (93 tickets) fueron de peligrosidad alta, mientras que el 2,2% (16 tickets) fueron de peligrosidad muy alta.

3.7. Tickets procesados como incidentes

Para los propósitos de la gestión de tickets en el sistema OTRS del CSIRT, así como para este informe, se entiende como incidentes, toda aquella situación en la que existe afectación o compromiso de los activos informáticos de una organización pública o de organizaciones privadas de carácter público.

3.8. Clase de incidentes

Las categorías contenidas en este apartado están asociadas a incidentes como contenido abusivo, código malicioso, recopilación de información, intentos de intrusión, intrusión, disponibilidad, información de seguridad de contenidos y fraude.



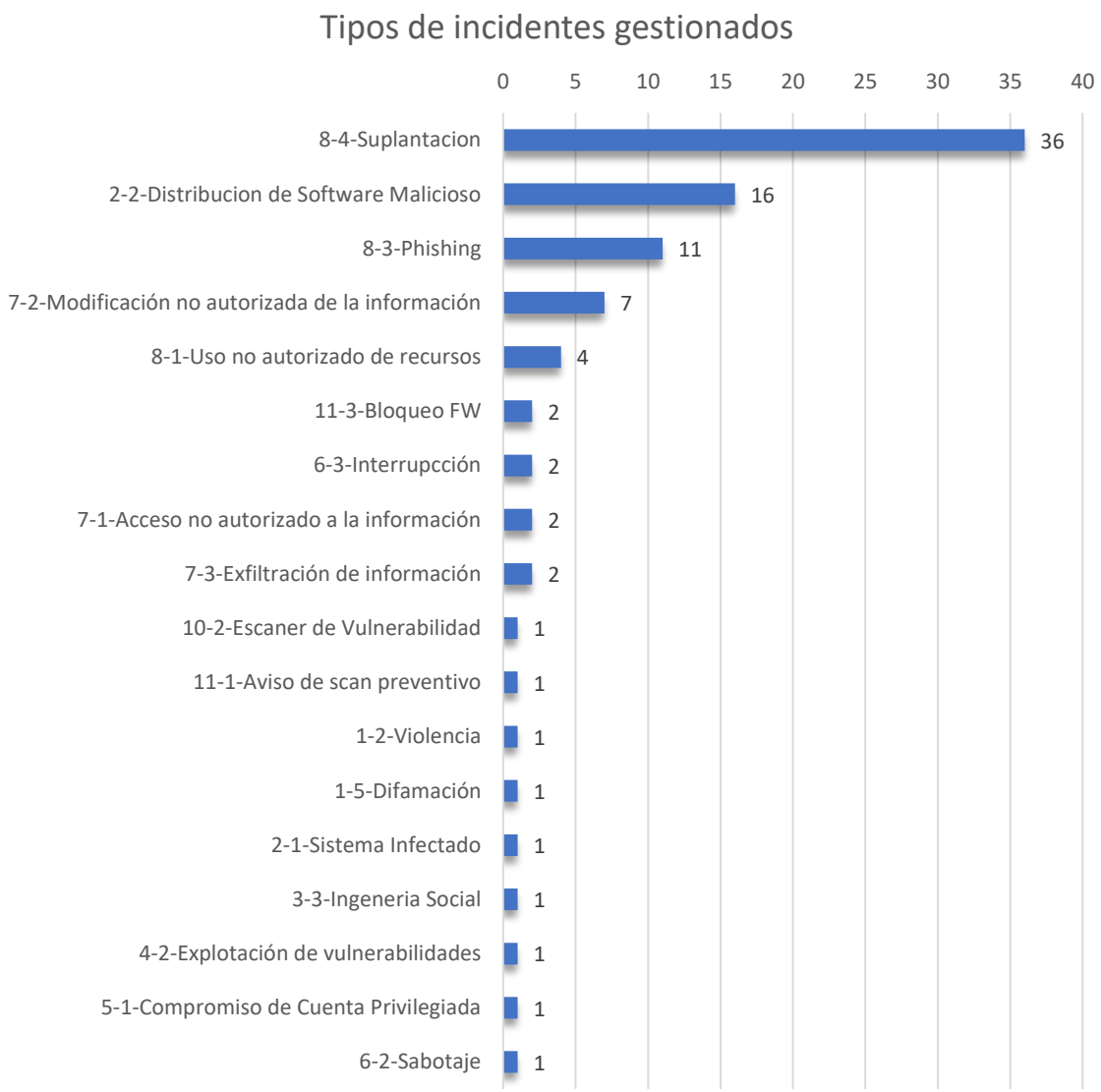
De los 91 tickets de incidentes registrados en abril, el 56,0% (51 tickets) correspondieron fraudes. Los incidentes relacionados a la presencia de códigos maliciosos representaron el 18,7% del total (17 tickets), seguido por incidentes de seguridad de contenidos con el 12,1% (11 tickets), contenido abusivo con el 4,4% (4 tickets), disponibilidad con el 3,3% (3 tickets), mientras que la recopilación de información y los intentos de intrusión, alcanzaron cada uno el 1,1% (1 ticket cada uno). Otros dos tickets fueron registrados como otros, lo que corresponde a 2,2%.

3.9. Tipos de incidentes

Cada clase de incidente tiene una subcategoría, la que a su vez describe un tipo específico de incidente. Este mes se registraron 18 tipos específicos de incidentes.

El 39,6% de los tickets gestionados corresponden a incidentes de suplantación de identidad o de marcas en sitios web fraudulentos (36 tickets). También se destacan este mes la distribución de software malicioso con el 17,6% (16 tickets), el phishing con el 12,1% (11 tickets), la modificación no autorizada de la información con el 7,7% (7 tickets), el uso no autorizado de recursos con el 4,4% (4 tickets), el bloqueo de firewall, la interrupción los accesos no autorizados a la información y la exfiltración de informes, cada uno registró 2 tickets, equivalente al 2,2%, mientras que los incidentes de violencia, difamación, sistemas infectados, ingeniería social, explotación de vulnerabilidades, compromiso de cuenta privilegiada y sabotaje, registraron un incidentes a cada uno, lo que

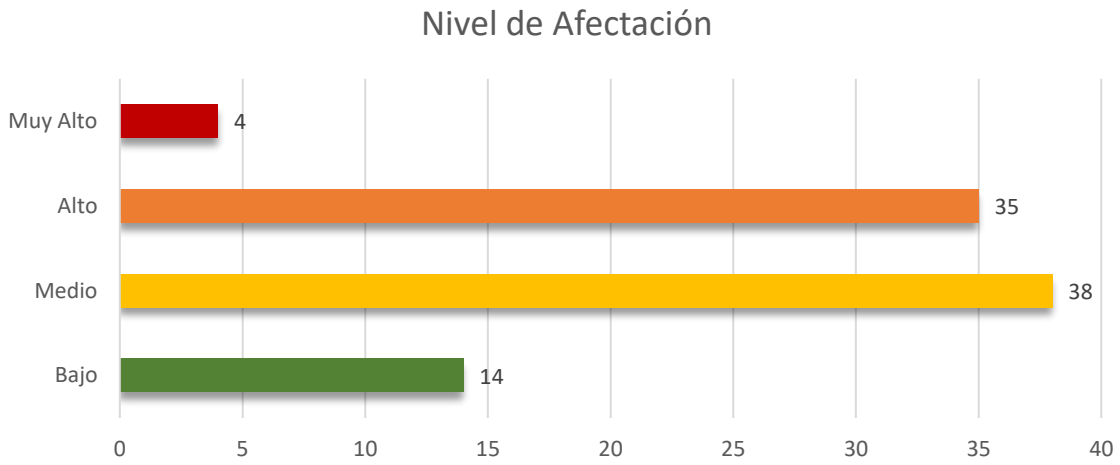
representa el 1,1% en cada caso. Hay dos incidentes que corresponden a la categoría otros, lo que equivale al 2,2%.[3]



3.10. 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.

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

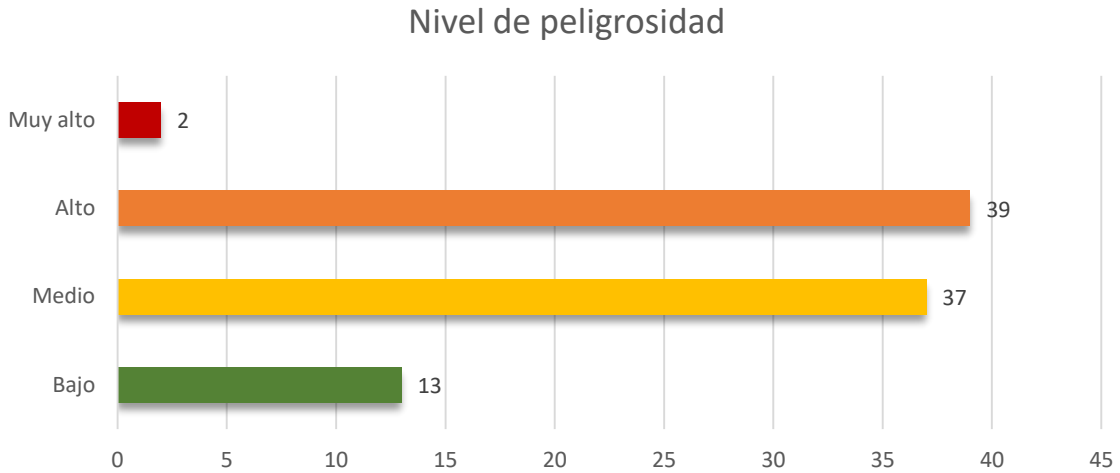


En el mes de abril un 41,8% de los incidentes de ciberseguridad (38 tickets) tuvieron afectación media. El 38,5% de los incidentes (35 tickets) tuvo una afectación alta, el 15,4% (14 tickets) tuvo una afectación baja, y el 4,4% (4 tickets) tuvo una afectación muy alta.

3.11. 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.



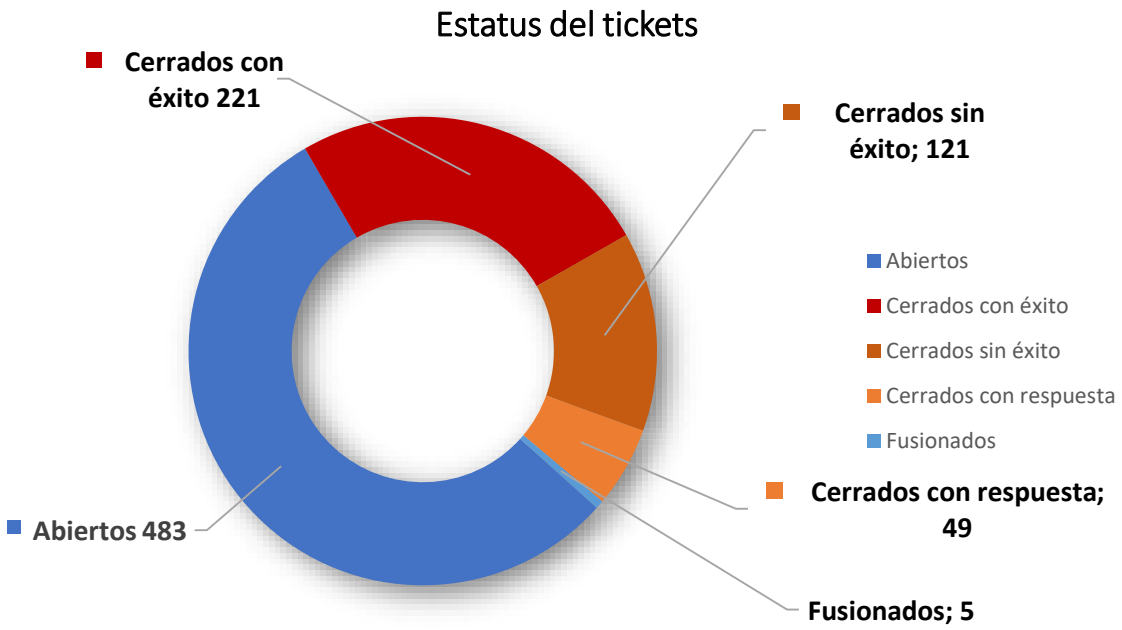
En el mes de abril un 42,9% de los incidentes (39 tickets) fueron de peligrosidad alta, el 40,7% (37 tickets) fueron de peligrosidad alta, el 14,3% (13 tickets) fueron de peligrosidad baja, y el 2,2% (2 tickets) fueron de peligrosidad muy alta.

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, cerrados con éxito y fusionados.



El 54,9% de los incidentes (483 tickets) de abril se mantienen abiertos, mientras que el 45,1% (396 tickets) fueron cerrados. De los tickets cerrados, un 55,8% (221 tickets) fueron cerrados con éxito, mientras que un 30,6% (121 tickets) fueron cerrados sin éxito y un 12,4% (49 tickets) fueron cerrados con respuestas. Hubo 5 tickets cerrados que fueron fusionados, lo que equivale a un 1,3%.

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: 2023.05.08 14:21:48 -04'00'

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática