CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

INFORME MENSUAL GESTIÓN DE TICKETS CSIRT-GOBIERNO DE CHILE

14GMT23-00022-01

DICIEMBRE 2023

ÍNDICE

Contenido

Equipo de Respuesta ante Incidentes de Seguridad Informática
Coordinación Nacional de Ciberseguridad, Gobierno de Chile
Contacto: csirt-comunicaciones@interior.gob.cl
Teléfono: 1510 | (56 2) 24863850
Sitio: https://www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

14GMT23-00022-01

INFORME MENSUAL
GESTIÓN DE TICKETS
CSIRT–GOBIERNO DE CHILE
DICIEMBRE 2023

OBJETIVO DEL INFORME

Este informe está dirigido al público en general, para dar a conocer mejor la gestión técnica del CSIRT de Gobierno. El documento reúne así las estadísticas de diciembre 2023, en relación con la gestión de los eventos e incidentes que están resumidos en los tickets procesados durante ese período.

ACERCA DE LA GESTIÓN

Cada uno de los eventos, consultas, notificación e incidentes de ciberseguridad que gestiona el CSIRT de Gobierno está vinculado a un ticket. Este instrumento permite tener trazabilidad desde su reporte y respuesta hasta su cierre.

Cada ticket está asociado a indicadores de compromiso, 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 de los casos observados por el CSIRT se resume en estos tickets, ayudando a la respuesta técnica, la generación de estadísticas, el acompañamiento y la asesoría a las instituciones en la gestión en la respuesta, junto con el ofrecimiento de beneficios complementarios de apoyo comunicacional, además de alertar al resto del ecosistema de los incidentes en curso.

PROCESAMIENTO

Para procesar sus 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 y 37 subcategorías. La gestión se divide a su vez en cuatro tipos; Incidente, notificación, consulta y evento.

1. REPORTES DE TICKETS

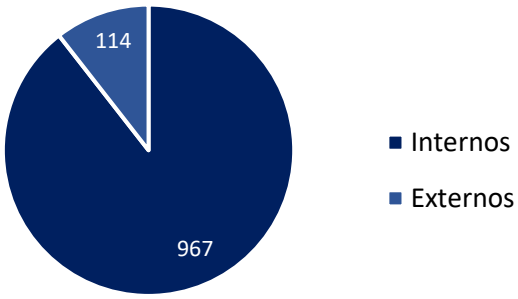
Este apartado recopila la información sobre la apertura del ticket, sus orígenes, a quien se dirige, el activo afectado y el medio utilizado para reportar. Este mes se procesaron 1.081 tickets.

1.1. Reportes públicos y privados

Por su disposición estratégica, el CSIRT atiende en su mayor parte incidentes ocurridos dentro de organizaciones del Estado, con un énfasis en aquellas que son parte de la red de Conectividad del Estado (RCE). De todas formas, reporta incidentes de entidades privadas dada su importancia por los servicios estratégicos o sensibles que entregan a la ciudadanía.

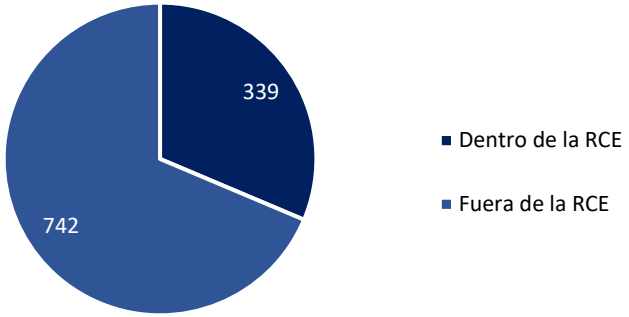
1.2. Reportes internos y externos

La fuente del reporte del incidente que origina el ticket, ya sea interna o externa, es relevante porque refleja 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, firmas privadas con convenio y la ciudadana, entre otros.



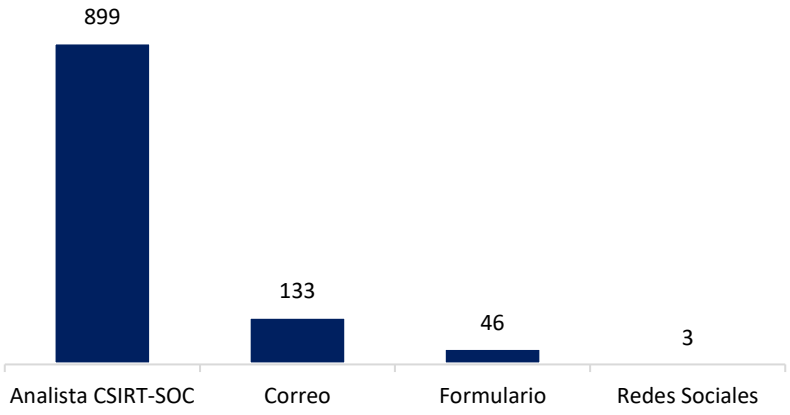
1.3. Ubicación de activo afectado

Los activos involucrados 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 de un incidente.



1.4. Medio de Ingreso

La fuente del reporte permite identificar el medio utilizado para reportar o notificar un incidente. Los más comunes son los generados por análisis de los propios funcionarios del CSIRT, seguidos por aquellos advertidos por fuentes externas como el formulario web, el correo electrónico, el teléfono y las redes sociales.



83,16% **de los reportes surge de un análisis del CSIRT**

1.5. Notificación por 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.

1 tickets haciendo mención el Decreto 273

2. PROCESAMIENTO DE TICKETS

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 con la taxonomía asignada y sus niveles de afectación.

2.1. Categoría

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

Para los propósitos de la gestión de tickets, se entiende como consulta, toda pregunta general o específica que no tiene relación con la existencia de un incidente. 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 generan afectación.

2.2. Categoría Eventos procesados

Para los propósitos de la gestión de tickets, 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.

Los tickets corresponden a situaciones que pueden derivar en un incidente en caso de ser explotadas. En la mayoría de los casos, estos fueron generados por el CSIRT como resultado de un análisis controlado, además del reporte de vulnerabilidades por parte de terceras partes, e informes de amenazas que no resultaron en una afectación a personas u organizaciones.

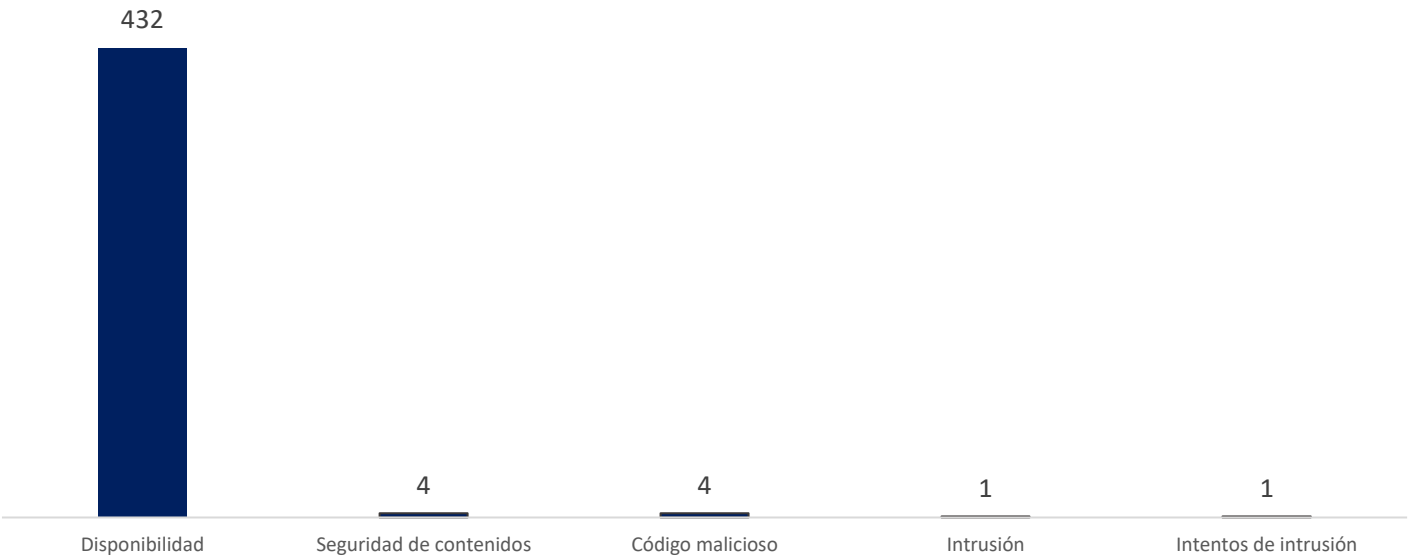
71,8% **de eventos procesados corresponde a análisis controlados.**

2.2.1. Tipo de eventos

Cada categoría de evento tiene una subcategoría, denominadas tipos. Los siguientes son once los tipos de eventos específicos informados durante el mes.

2.3. Categoría de incidentes procesados

Para los propósitos de la gestión de tickets, se entiende como incidentes toda aquella situación en la que existe afectación o compromiso de los activos informáticos de una organización pública, organizaciones privadas o ciudadano.



2.3.1. Tipo de incidentes

Cada clase de incidente tiene una subcategoría. Los siguientes son los doce tipos de incidentes específicos que fueron informados durante el mes

2.3.2. Nivel de afectación

El nivel de afectación corresponde al impacto real o potencial causado por un incidente de ciberseguridad.

Los siguientes niveles de afectación: bajo, medio, alto, muy alto y crítico, son asignados por el CSIRT en una primera instancia y están sujetos a revisión, por lo cual pueden existir variaciones que no estén representadas en el gráfico.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.26 10:58:53 -03'00'

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática