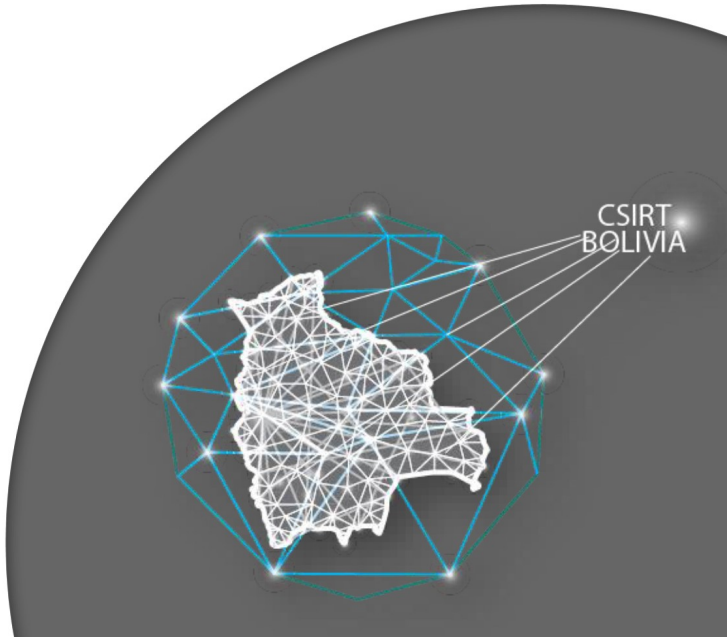
INFORME DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES INFORMÁTICAS



SEGUNDO TRIMESTRE 2025

Índice

1. Resumen Ejecutivo....3
2. Alcances....4
3. Actividades....4
4. Estadísticas....5
4.1. Casos Abiertos....5
4.2. Casos Abiertos por Categoría....7
4.2.1 Incidentes....7
4.2.2 Vulnerabilidades....8
4.3. Casos Resueltos....10
4.4. Casos Resueltos por Vulnerabilidad e Incidente....11
5. Términos y Definiciones....12
6. Historial de Cambios....15

Índice de tablas

Tabla 1: Detalle de Casos Abiertos....6
Tabla 2: Incidentes por Categoría....7
Tabla 3: Vulnerabilidades por Categoría....9
Tabla 4: Casos Abiertos y Resueltos....10
Tabla 5: Casos Resueltos por Vulnerabilidad e Incidente....11

Índice de gráficos

Gráfico 1: Casos Abiertos....6
Gráfico 2: Incidentes por Categoría....8
Gráfico 3: Vulnerabilidades por Categoría....9
Gráfico 4: Porcentaje de Casos Resueltos....10
Gráfico 5: Tickets Resueltos....11

2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

1. Resumen Ejecutivo

El Centro de Gestión de Incidentes Informáticos (CGII) de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) publica el Informe de Gestión de Incidentes y Vulnerabilidades correspondiente al segundo trimestre del 2025, en el marco del Decreto Supremo 2514 que establece las funciones del CGII:

- Monitorear los sitios web gubernamentales y la aplicación de las políticas y lineamientos definidos por la AGETIC.
- Comunicar y otorgar información a todas las entidades del sector público acerca de incidentes informáticos y vulnerabilidades de los que se haya tomado conocimiento.
- Prestar soporte técnico a las entidades del sector público, en caso de que ocurriera un incidente informático.
- Otorgar soporte técnico para la prevención de incidentes informáticos a las entidades del Nivel Central del Estado a solicitud de las mismas.
- Coordinar la gestión de incidentes informáticos gubernamentales con entidades de similar función a nivel internacional.

Durante los meses: abril, mayo y junio del 2025 se gestionaron 243 casos de incidentes y vulnerabilidades informáticas, que corresponden a reportes nuevos y abiertos de períodos anteriores. Del total de casos, 221 fueron resueltos a través de una correcta comunicación, seguimiento y validación con las entidades afectadas y 22 se encuentran abiertos, los cuales están siendo gestionados para su solución; los resultados serán reflejados en siguientes informes.

2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

El actual informe muestra estadísticas de la atención de casos válidos de incidentes y vulnerabilidades informáticas durante el segundo trimestre del 2025, cuyos datos son clasificados por casos “tipo” en términos de cantidad y porcentaje.

También se hace una relación porcentual entre los casos que fueron resueltos en el transcurso del trimestre y aquellos que están en proceso de solución.

2. Alcances

La información de cantidades y porcentajes mostrados en el presente informe corresponden a casos gestionados por el CGII en los meses: abril, mayo y junio del 2025, a partir de casos válidos de incidentes y vulnerabilidades informáticas originados por las siguientes fuentes:

- Responsables de Seguridad de la Información de las entidades del sector público.
- Herramientas de monitoreo y detección implementadas por el CGII.
- Equipos de Respuesta ante Incidentes Informáticos.
- Participantes del muro de la fama a través del formulario de reporte.

3. Actividades

A continuación las actividades realizadas por el CGII durante el referido período de tiempo:

- Análisis de indicadores de compromiso, obtenidos de fuentes abiertas de información que tuvieron incidencia en entidades del sector público.
- Validación de reportes para descartar falsos positivos que no corresponden.

2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

- Comunicación de incidentes y vulnerabilidades informáticas a las entidades afectadas, brindando la información técnica necesaria para su solución.
- Seguimiento al estado de solución de los casos pendientes a través de llamadas telefónicas y correo electrónico, también soporte técnico, en caso de que así lo requieran.
- Validación de las medidas aplicadas por las entidades para solucionar el incidente o vulnerabilidad informática, y posterior cierre del caso.
- Detección de incidentes y vulnerabilidades informáticas realizadas a través del monitoreo continuo de sitios web gubernamentales.

4. Estadísticas

Las siguientes estadísticas presentadas en tablas y gráficos corresponden a casos abiertos y resueltos de reportes de incidentes y vulnerabilidades informáticas gestionadas durante el segundo trimestre del 2025.

4.1. Casos Abiertos

En este período, se gestionaron 243 casos de incidentes y vulnerabilidades informáticas, de los cuales, 219 fueron abiertos en el segundo trimestre del 2025 y 24 corresponden a períodos anteriores; en la siguiente tabla se podrá apreciar la información desagregada:

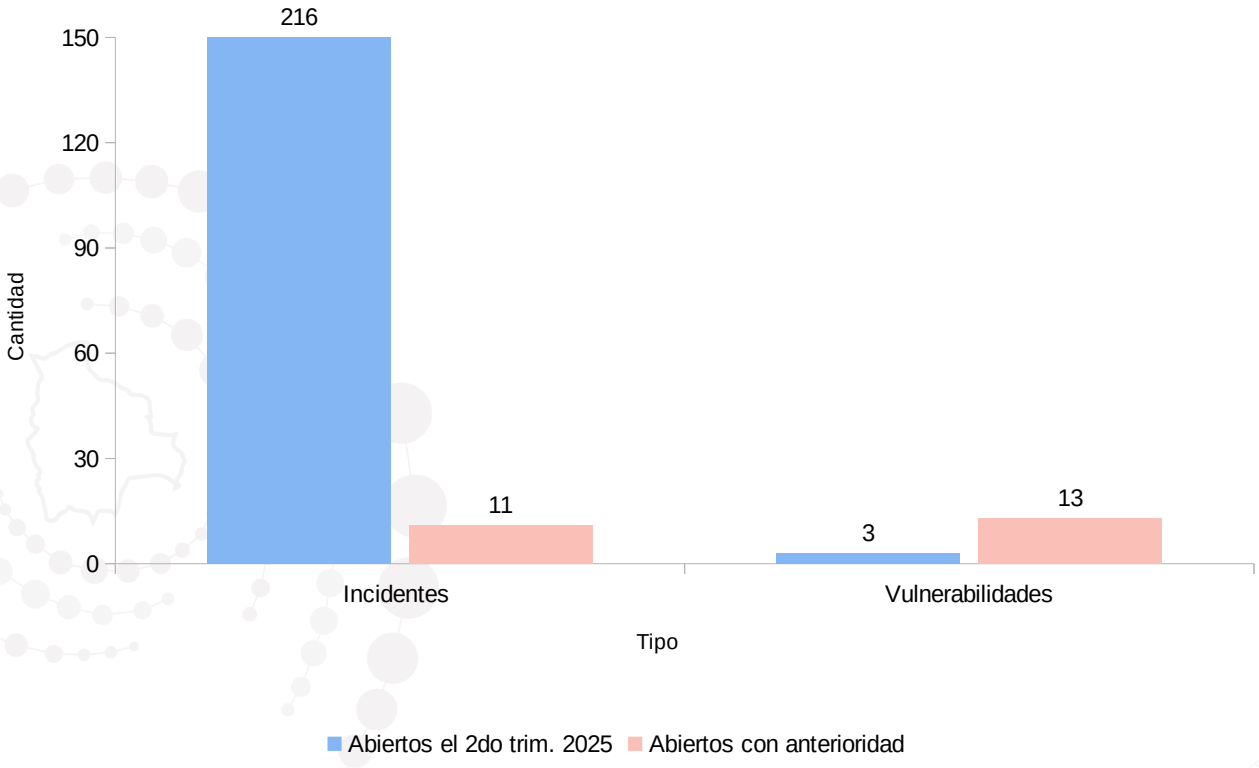
2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

Tabla 1: Detalle de Casos Abiertos

Tipo	Descripción	Cantidad
Incidentes	Abiertos en el segundo Trim. 2025	216
	Abiertos con anterioridad	11
Vulnerabilidades	Abiertas en el segundo Trim. 2025	3
	Abiertas con anterioridad	13
	Totales	**243**

En el siguiente gráfico se puede observar la distribución de incidentes y vulnerabilidades informáticas abiertas en el segundo trimestre y con anterioridad:

Gráfico 1: Casos Abiertos



2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

4.2. Casos Abiertos por Categoría

4.2.1 Incidentes

En el segundo trimestre del 2025 se registraron 216 nuevos incidentes informáticos, que fueron categorizados de acuerdo al detalle, representado por la siguiente tabla y su respectivo gráfico:

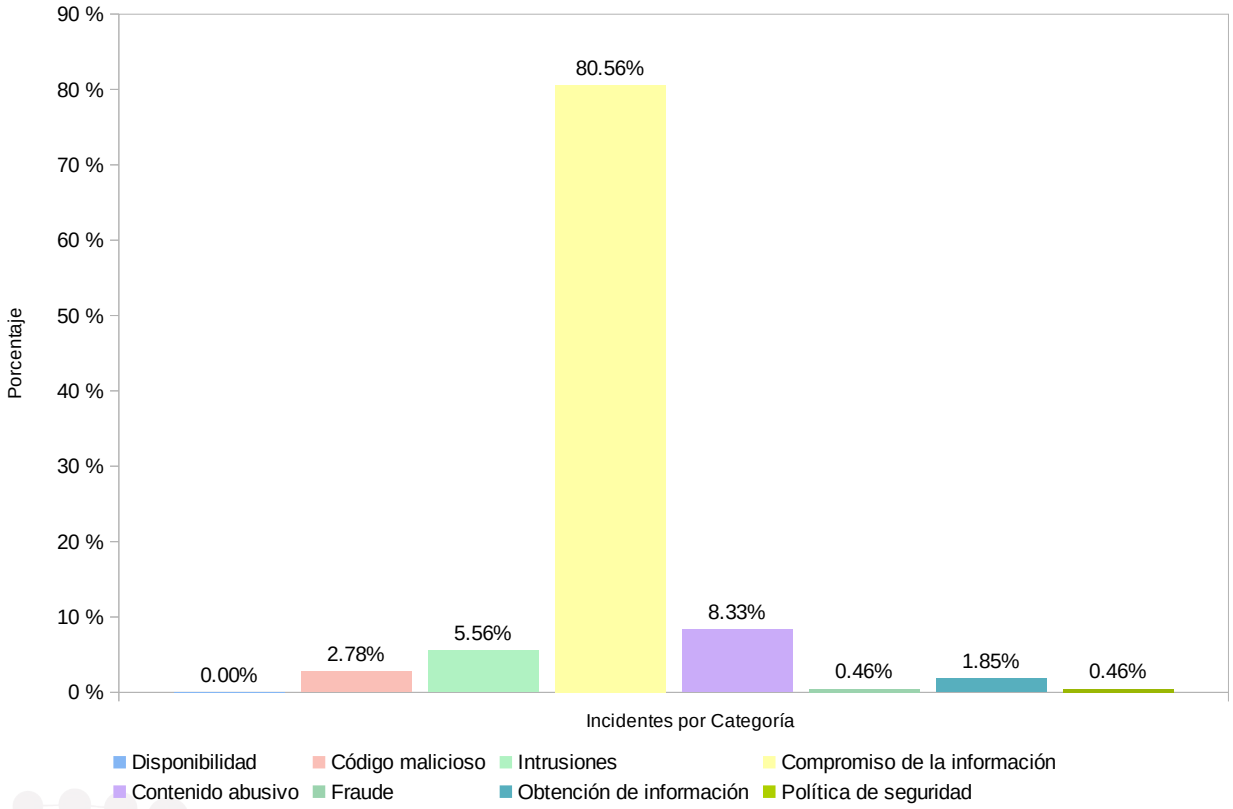
Tabla 2: Incidentes por Categoría

Categoría	Cantidad	Porcentaje
Disponibilidad	0	0.00%
Código malicioso	6	2.78%
Intrusiones	12	5.56%
Compromiso de la información	174	80.56%
Contenido abusivo	18	8.33%
Fraude	1	0.46%
Obtención de información	4	1.85%
Política de seguridad	1	0.46%
Totales	**216**	**100.00%**

Dentro de las categorías mencionadas, se tuvo mayor incidencia en ***compromiso de la información*** debido a que se identificaron usuarios y contraseñas de sistemas de entidades públicas que estaban siendo vendidos por actores maliciosos en la DarkWeb. Se notificó a las entidades afectadas para la actualización inmediata de contraseñas.

2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

Gráfico 2: Incidentes por Categoría



4.2.2 Vulnerabilidades

En el segundo trimestre de la gestión 2025 se registraron 3 nuevos casos de vulnerabilidades de severidad alta o crítica, que han sido categorizados de acuerdo al detalle de la siguiente tabla y su gráfico:

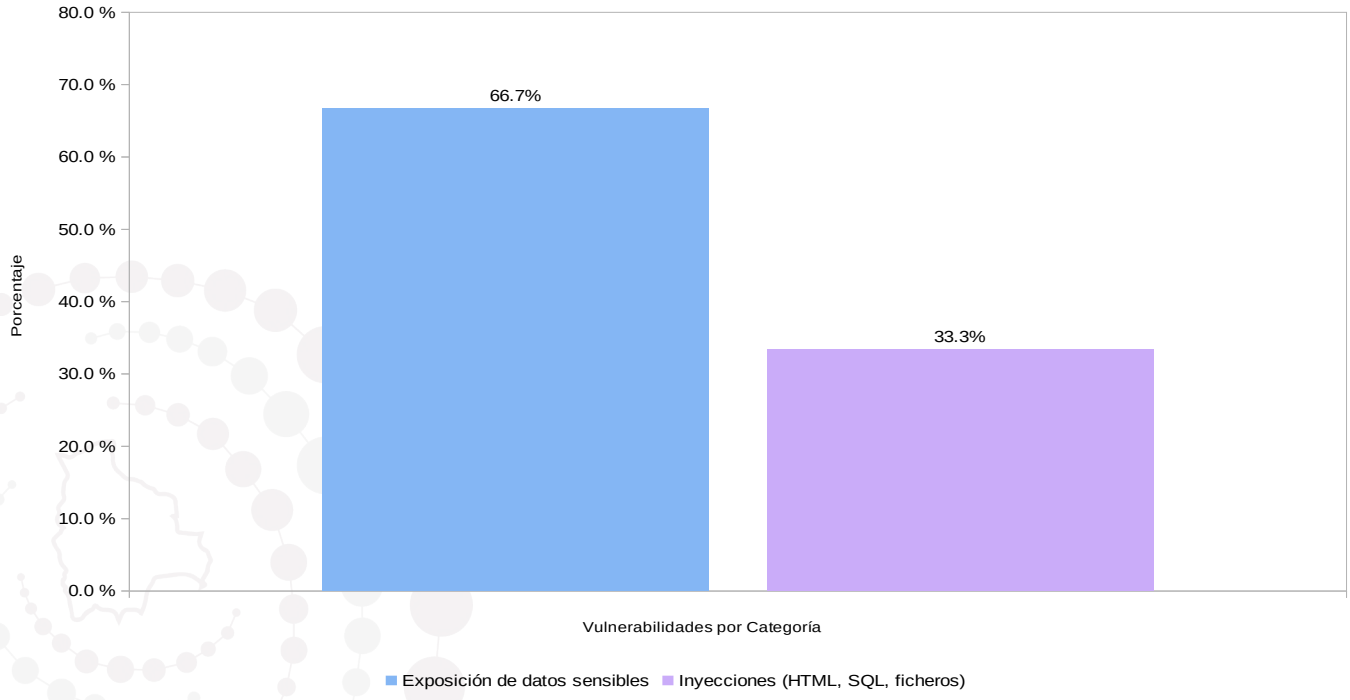
2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

Tabla 3: Vulnerabilidades por Categoría

Categoría	Cantidad	Porcentaje
Exposición de datos sensibles	2	66.7%
Inyecciones (HTML, SQL, ficheros)	1	33.3%
Totales	**3**	**100%**

Se identificaron fallas de ***exposición de datos sensibles*** que permitirían el acceso a recursos que expondrían información sensible perteneciente a sistemas de la entidad.

Gráfico 3: Vulnerabilidades por Categoría



2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

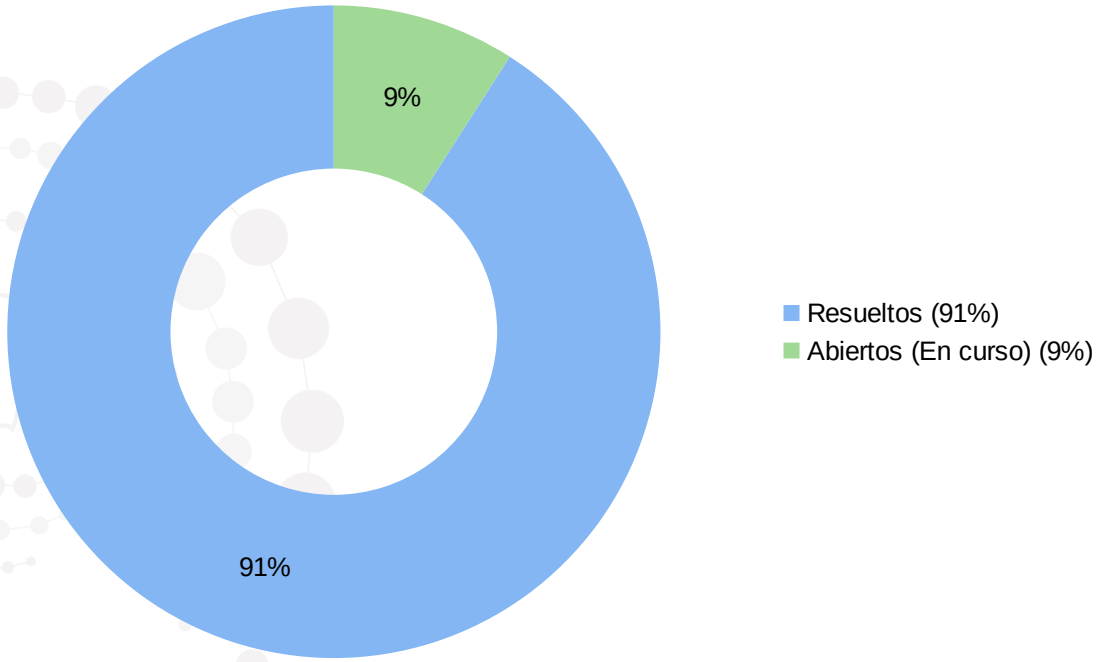
4.3. Casos Resueltos

Como resultado de las actividades de gestión de incidentes y vulnerabilidades informáticas en el segundo trimestre del 2025, el CGII resolvió 221 casos, quedando pendientes de solución para siguientes períodos 22 casos, a los cuales se está dando el seguimiento respectivo. Estos datos se aprecian en la siguiente tabla y su correspondiente gráfico:

Tabla 4: Casos Abiertos y Resueltos

Estado	Cantidad	Porcentaje
Resueltos	221	91%
Abiertos (En curso)	22	9%
Totales	**243**	**100.00%**

Gráfico 4: Porcentaje de Casos Resueltos



2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

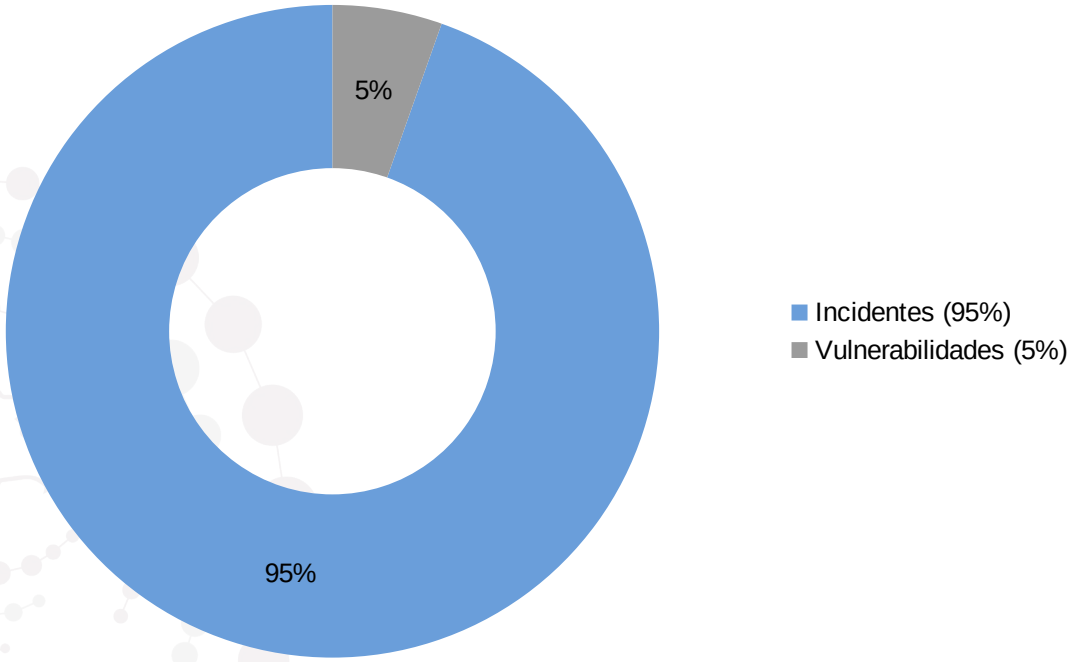
4.4. Casos Resueltos por Vulnerabilidad e Incidente

Del total de casos resueltos en el segundo trimestre del 2025, 209 corresponden a incidentes y 12 a vulnerabilidades informáticas, datos que se pueden observar en la siguiente tabla y su correspondiente gráfico:

Tabla 5: Casos Resueltos por Vulnerabilidad e Incidente

Tipo	Cantidad	Porcentaje
Incidentes	209	95%
Vulnerabilidades	12	5%
Totales	**221**	**100%**

Gráfico 5: Tickets Resueltos



2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

5. Términos y Definiciones

Código Malicioso.- Programas informáticos que tienen como objetivo acceder al sistema sin ser detectados y realizar acciones como el secuestro de información o recopilación de datos privados.

Componentes con Vulnerabilidades Conocidas.- Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación; si se explota un componente vulnerable, el ataque puede provocar pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas que pueden debilitar las defensas y permitir diversos ataques e impactos.

Compromiso de la Información.- Acceso, modificación, borrado o publicación de información sin autorización del propietario.

Configuración de Seguridad Incorrecta.- Una configuración errónea de seguridad surge cuando dichas configuraciones se definen, implementan y se mantienen con valores predeterminados.

Contenido Abusivo.- Incidentes que muestren signos evidentes de correos electrónicos no solicitados (spam).

Deserialización Insegura.- Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos que pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.

2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

Disponibilidad.- Falta de disponibilidad del sistema o servicio producto de ataques de denegación de servicio, mala configuración, interrupciones de servicio por factores no previstos.

Entidades Externas XML (XXE).- Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Un ataque de entidad externa XML exitoso puede revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).

Exposición de Datos Sensibles.- Acceso a datos sensibles como contraseñas, claves privadas de API, errores o debug, rutas completas, datos personales o uso de algoritmos de cifrado débil.

Fraude.- Incidentes que tengan nexo con el uso no autorizado, derechos de autor, suplantación de identidad, exfiltración de información o uso ilegítimo de credenciales.

Incidente.- Evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Intrusiones.- Acceso al sistema o a uno de sus componentes aprovechando sus vulnerabilidades.

Inyecciones.- Son fallas de inyección, como SQL, NoSQL, OS o LDAP que ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta.

Obtención de Información.- Obtención de datos personales, información de las redes de datos, credenciales de acceso del usuario a través de técnicas de engaño.

2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

Pérdida de Autenticación.- Este tipo de debilidad puede permitir a un atacante capturar u omitir los métodos de autenticación que usa una aplicación web.

Pérdida de Control de Acceso.- Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos.

Política de Seguridad.- Incidentes de abuso de privilegios de los usuarios, acceso a servicios no autorizados, o relacionados al uso de sistemas desactualizados.

Registro y Monitoreo Insuficientes.- El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permite a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Historial de cambios

Secuencia de Comandos en Sitios Cruzados (XSS).- Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador.

Phishing .- Conjunto de técnicas que consiste en engañar al usuario para robarle información confidencial.

Caso Abierto.- Reporte de un incidente o vulnerabilidad informática que fue validado y se encuentra en proceso de solución.

Caso Resuelto.- Reporte de un incidente o vulnerabilidad informática que fue resuelta satisfactoriamente.

2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4

Vulnerabilidad.- Debilidad o falla en un sistema de información que pone en riesgo la seguridad del mismo, permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad.

6. Historial de Cambios

Versión	Fecha	Autor	Descripción	Motivo de cambios
1.0	01/07/2025	Rodrigo Uruchi	Elaboración	Datos iniciales, estructura y datos
1.0	01/07/2025	Pamela García Meza de Ugarte	Revisión	Redacción
1.0	01/07/2025	Franz Rojas	Aprobación	Aprobación

2-2184026 +591 72016254 Agetic Bolivia agetic_bolivia @AgeticBolivia ageticbolivia
Sopocachi Calle Pedro Salazar N° 631 Edif. Fondo Nacional de Desarrollo Regional (FNDR) Piso. 4