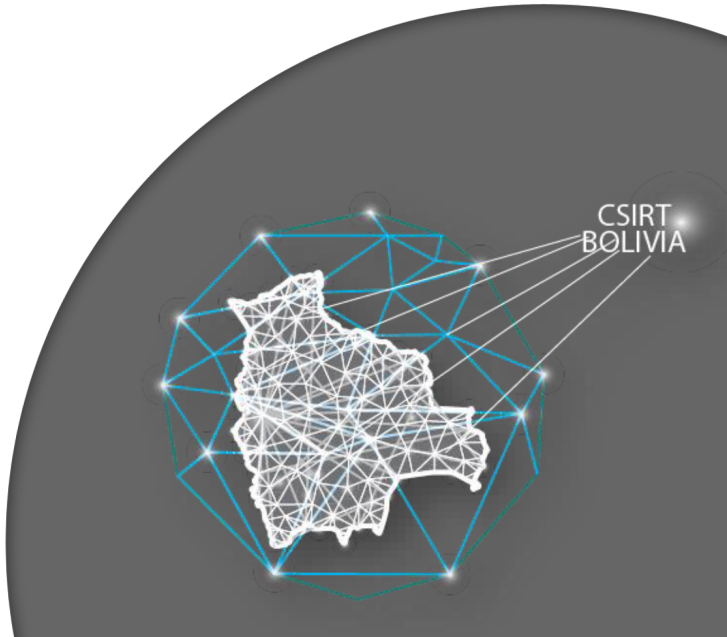
ESTADO PLURINACIONAL DE BOLIVIA
MINISTERIO DE LA PRESIDENCIA

AGETIC
Digitalizando Bolivia
Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación

INFORME DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES INFORMÁTICAS



JULIO 2021

Índice

Índice de tablas

Índice de gráficos

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 a julio 2021, 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 el mes de julio, se gestionaron 55 casos de incidentes y vulnerabilidades informáticas, que corresponden a reportes nuevos y abiertos de meses anteriores. Del total de casos, 25 fueron resueltos a través de una correcta comunicación, seguimiento y validación con las entidades afectadas y 30 se encuentran abiertos, los cuales están siendo gestionados para su solución; los resultados serán reflejados en posteriores informes.

El actual informe muestra estadísticas de la atención de casos válidos de incidentes y vulnerabilidades informáticas durante el mes de julio, 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 mes y aquellos que están en proceso de solución.

2. Alcances

La información de cantidades y porcentajes mostrados en el presente informe corresponde a casos gestionados por el CGII en el mes de julio 2021, 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.

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.

- 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.
- Monitoreo de disponibilidad de 548 sitios web pertenecientes a entidades del sector público.
- 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 mes de julio.

4.1. Casos abiertos

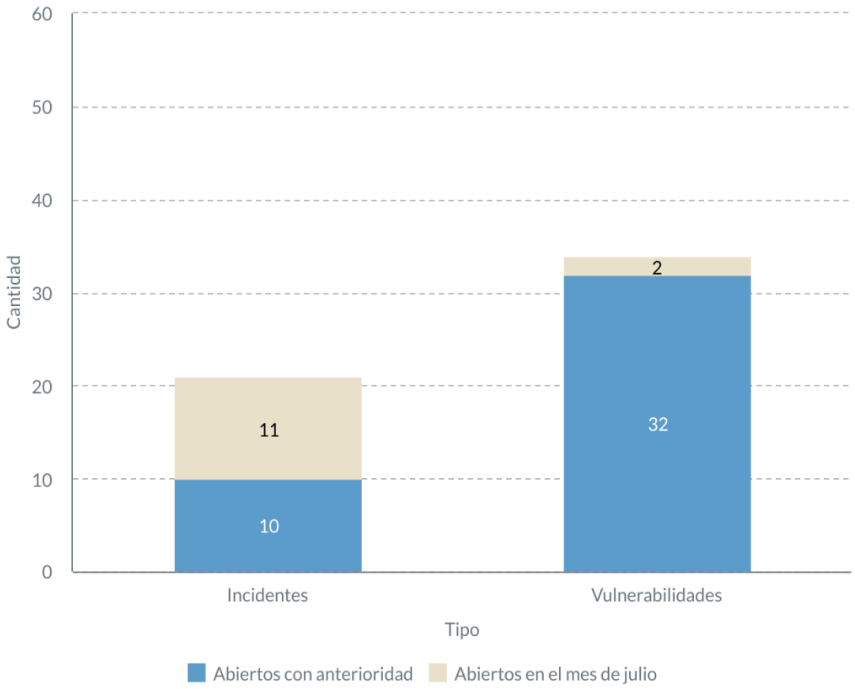
En este periodo, se gestionaron 55 casos de incidentes y vulnerabilidades informáticas, de los cuales, 13 fueron abiertos en julio y 42 corresponden a meses anteriores; en la siguiente tabla se podrá apreciar la información desagregada:

Tabla 1: Detalle de casos abiertos

Tipo	Descripción	Cantidad
Incidentes	Abiertos en julio	11
	Abiertos con anterioridad	10
Vulnerabilidades	Abiertos en julio	2
	Abiertos con anterioridad	32
Totales		**55**

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

Gráfico 1: Casos abiertos



4.2. Casos abiertos por categoría

4.2.1 Incidentes

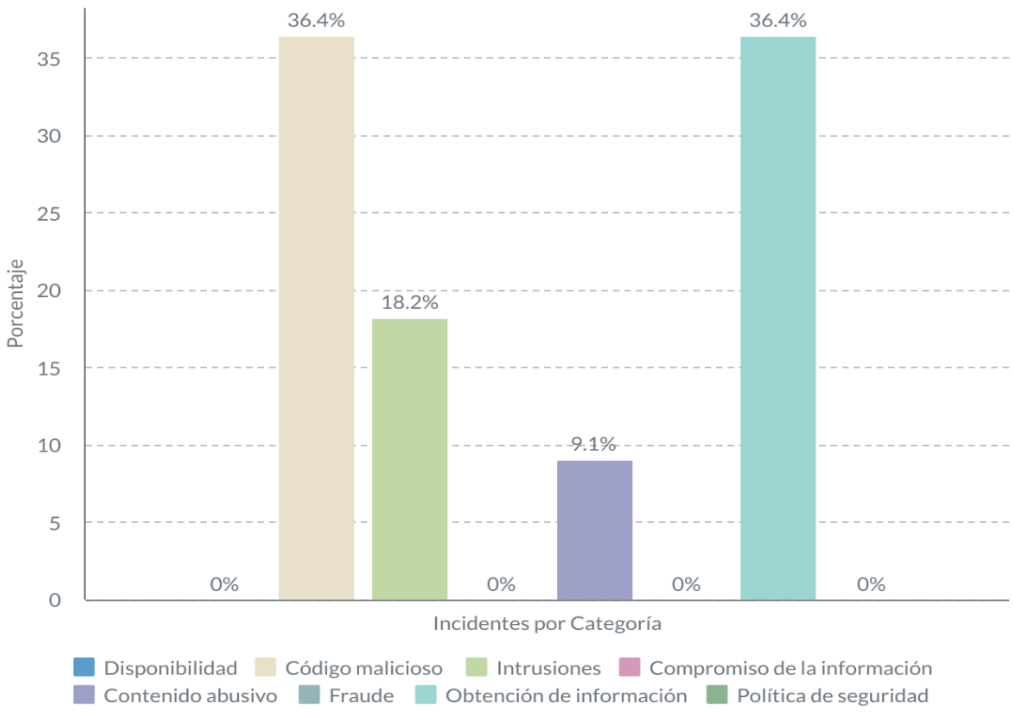
En julio se registraron 11 nuevos incidentes informáticos, que fueron categorizados de acuerdo al detalle, representado por la siguiente tabla y su respectivo gráfico:

Tabla 2: Incidentes por categoría

Categoría	Cantidad	Porcentaje
Disponibilidad	0	0 %
Código malicioso	4	36,4 %
Intrusiones	2	18,2 %
Compromiso de la información	0	0 %
Contenido abusivo	1	9,1 %
Fraude	0	0 %
Obtención de información	4	36,4 %
Política de seguridad	0	0 %
Totales	**11**	**100 %**

Dentro de las categorías: ***Código malicioso*** *y* ***obtención de información,*** que cuentan con la mayor cantidad de incidencias, se gestionaron casos de malware presentes en la red interna de entidades públicas y correos electrónicos no solicitados con técnicas para obtener contraseñas de cuentas de correo.

Gráfico 2: Incidentes por categoría



4.2.2 Vulnerabilidades

En julio se registraron 2 nuevos casos de vulnerabilidades, que han sido categorizados de acuerdo al detalle de la siguiente tabla y su gráfico:

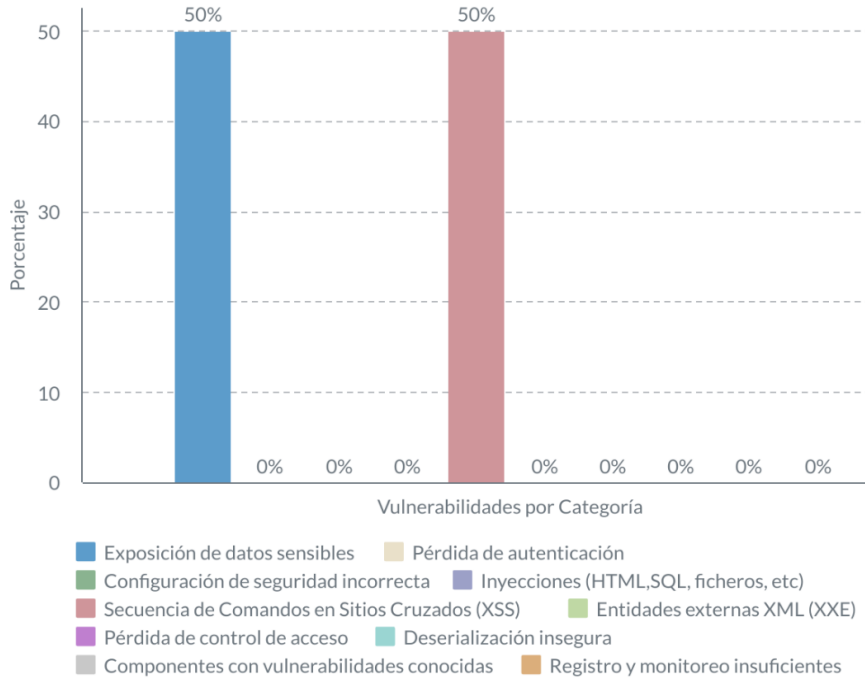
Tabla 3: Vulnerabilidades por categoría

Categoría	Cantidad	Porcentaje
Exposición de datos sensibles	1	50 %
Pérdida de autenticación	0	0 %
Configuración de seguridad incorrecta	0	0 %
Inyecciones (HTML, SQL, ficheros)	0	0 %

Categoría	Cantidad	Porcentaje
Secuencia de Comandos en Sitios Cruzados (XSS)	1	50 %
Entidades externas XML (XXE)	0	0 %
Pérdida de control de acceso	0	0 %
Deserialización insegura	0	0 %
Componentes con vulnerabilidades conocidas	0	0 %
Registro y monitoreo insuficientes	0	0 %
Totales	**2**	**100%**

Como se aprecia en el gráfico, el mes de julio se detectaron casos de ***Secuencia de Comandos en Sitios Cruzados (XSS)*** y ***Exposición de Datos Sensibles*** presentes en sistemas de información de las entidades del sector público.

Gráfico 3: Vulnerabilidades por categoría



4.3. Casos resueltos

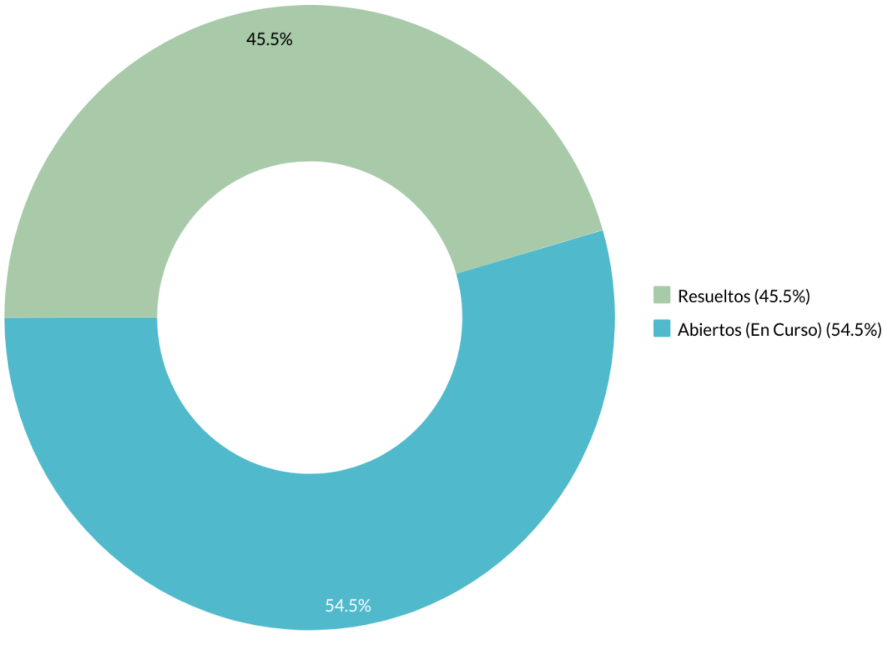
Como resultado de las actividades de gestión de incidentes y vulnerabilidades informáticas en julio, el CGII resolvió 25 casos, quedando pendientes de solución para siguientes periodos 30 casos, a los cuales se está dando el seguimiento respectivo.

Estos datos se aprecian en la siguiente tabla y su correspondiente gráfico:

Tabla 4: Casos abiertos y resueltos

Estado	Cantidad	Porcentaje
Resueltos	25	45,5 %
Abiertos (En curso)	30	54,5 %
Totales	**55**	**100%**

Gráfico 4: Porcentaje de casos resueltos



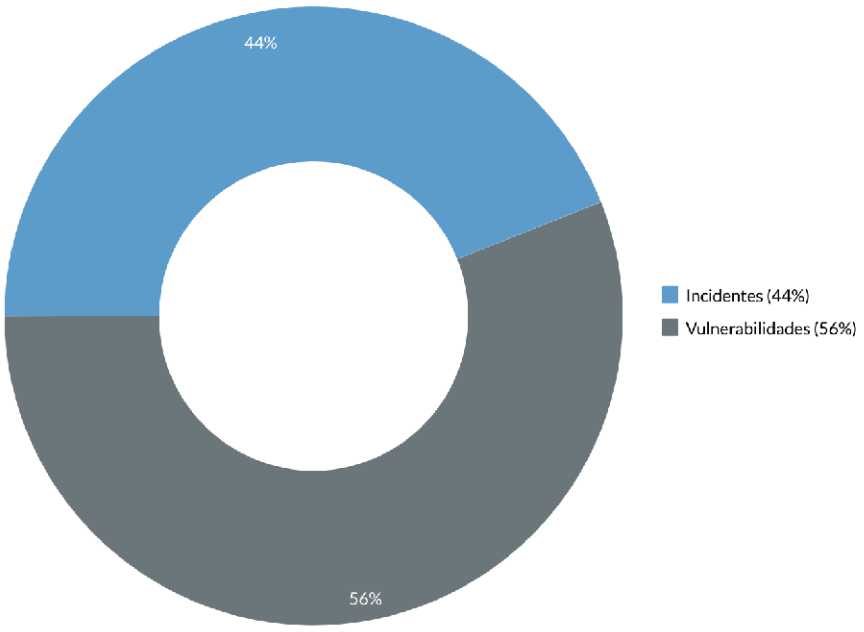
4.4. Casos resueltos por vulnerabilidad e incidente

Del total de casos resueltos en el mes de julio, 11 corresponden a incidentes y 14 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	11	44 %
Vulnerabilidades	14	56 %
Totales	**25**	**100%**

Gráfico 5: Tickets resueltos



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.

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.

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.

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	13/08/2021	Rodrigo Uruchi	Elaboración	Datos iniciales, estructura y datos
1.0	13/08/2021	Jazmin Valdivieso	Revisión	Redacción
1.0	13/08/2021	Franz Rojas	Aprobación	Aprobación