C.R. & F. ROJAS
ABOGADOS

Fundado en 1900

NEWSLETTER

Diciembre 2022 No. 2

Informe de Gestión de Incidentes preparado por el Centro de Gestión de Incidentes Informáticos de la AGETIC - Bolivia

La Paz Centro
Calle Federico Zuazo 1598,
Edificio Park Inn
Piso 11

(+591 - 2) 211 3165
(+591 - 2) 231 3737

La Paz Zona Sur
Avenida Ballivián 1063
Edificio Green Tower
Piso 13

(+591 – 2) 211 3165

Cochabamba
Avenida América 1228
Edificio Ferrara
Piso 1, Oficina 11 (Bloque A)

(+591) 783 62100

Santa Cruz
Avenida San Martín 155,
Edificio Ambassador Business Center
Piso 19

(+591 - 3) 337 7474

www.rojas-lawfirm.com

Informe de Gestión de Incidentes preparado por el Centro de Gestión de Incidentes Informáticos de la AGETIC - Bolivia

El Centro de Gestión de Incidentes Informáticos (CGII) tiene como misión establecer los lineamientos para la protección de los activos de información críticos para y del Estado, promoviendo de esta forma, la conciencia sobre la seguridad, prevención y respuesta oportuna a incidentes de seguridad informáticos.

La comunidad objetivo del CGII es, principalmente, todo el Estado Plurinacional de Bolivia. En este entendido, el Centro brinda apoyo directo a los usuarios finales, de quienes se espera se pongan en contacto con su proveedor de servicios de Internet (ISP), administrador del sistema, administrador de red o jefe de departamento para obtener asistencia.

El CGII brinda sus servicios a partir de avisos, alertas y Coordinación de Respuesta de Incidentes. Los avisos proporcionan la información necesaria para proteger los sistemas y redes. El servicio de alertas y advertencias tiene como objetivo difundir información sobre ciberataques o interrupciones, vulneraciones de seguridad, alertas de intrusión, virus informáticos y brindar recomendaciones para abordar el problema de la comunidad a la que brinda estos servicios, los mismos que son coordinados con instituciones y órganos del Estado, propietarios y proveedores de las partes afectadas, y operadores de telecomunicaciones.

La normativa sobre la que basa sus actuaciones se enmarca dentro de la Ley No. 164 de Telecomunicaciones, así como el Decreto Supremo No. 2514 de Creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), en cuanto a las Obligaciones y Funciones del Responsable de Seguridad de la Información (RSI).

En el ámbito de sus funciones y misión, el Centro dependiente de la AGETIC ha publicado el informe de gestión de incidentes y vulnerabilidades correspondiente al tercer trimestre del año 2022. Dicho informe arroja los siguientes datos sobre reportes nuevos y abiertos de meses anteriores, específicamente del mes de abril a mayo:

- 323 casos de incidentes y vulnerabilidades informáticas.
- 154 casos resueltos a través de una correcta comunicación, seguimiento y validación con entidades afectadas
- 228 casos abiertos en el tercer trimestre del año 2022
- 95 casos abiertos, los que se encuentran siendo gestionados para su solución.

Tabla 1: Detalle de casos abiertos

Tipo	Descripción	Cantidad
Incidentes	Abiertos en el tercer trimestre	27
	Abiertos con anterioridad	12
Vulnerabilidades	Abiertas en el tercer trimestre	201
	Abiertas con anterioridad	83
Totales		**323**

Cuadro preparado por el CGII

Los incidentes y vulnerabilidades informáticas reportados fueron originados por agentes Responsables de Seguridad de la Información de entidades del sector público, herramientas de monitoreo y detección implementadas por el CGII y participantes del muro de la fama a través de un formulario de reporte.

En el tercer trimestre del año 2022 se reportaron 27 nuevos incidentes informáticos, categorizados de la siguiente manera:

Tabla 2: Incidentes por categoría

Categoría	Cantidad	Porcentaje
Disponibilidad	0	0 %
Código malicioso	5	19 %
Intrusiones	6	22 %
Compromiso de la información	0	0 %
Contenido abusivo	13	48 %
Fraude	0	0 %
Obtención de información	3	11 %
Política de seguridad	0	0 %
Totales	**27**	**100 %**

Cuadro preparado por el CGII

Dentro de la categoría de "vulnerabilidades", se presentaron 201 nuevos casos relativos específicamente a configuraciones de seguridad incorrectos y exposición de datos sensibles.

Tabla 3: Vulnerabilidades por categoría

Categoría	Cantidad	Porcentaje
Exposición de datos sensibles	27	13 %
Pérdida de autenticación	7	3 %
Configuración de seguridad incorrecta	65	32 %
Inyecciones (HTML, SQL, ficheros)	18	9 %

Categoría	Cantidad	Porcentaje
Secuencia de Comandos en Sitios Cruzados (XSS)	16	8 %
Entidades externas XML (XXE)	0	0 %
Pérdida de control de acceso	56	28 %
Deserialización insegura	0	0 %
Componentes con vulnerabilidades conocidas	12	6 %
Registro y monitoreo insuficientes	0	0 %
Totales	**201**	**100%**

Cuadro preparado por el CGII

Los incidentes reportados en el último tiempo, se tratan de casos en los que, por ejemplo, se ha revelado una vulnerabilidad de alta gravedad en la biblioteca de la base de datos SQLite que se introdujo como parte de un cambio de código que data de octubre de 2000 y podría permitir a los atacantes bloquear o controlar programas.

https://www.cgii.gob.bo/es/alertas-de-seguridad/vulnerabilidad-en-la-biblioteca-de-base-de-datos-de-sqlite

En otro caso, se está explotando activamente una vulnerabilidad de ejecución remota de código en el software de colaboración empresarial y la plataforma de correo electrónico de Zimbra, que no cuenta con ningún parche disponible para remediar el problema. Un atacante puede cargar archivos arbitrarios a través de Amavis por un error de cpio.

https://www.cgii.gob.bo/es/alertas-de-seguridad/explotacion-activa-de-vulnerabilidad-critica-en-zimbra

Forninet publicó un parche de seguridad de una vulnerabilidad crítica de omisión de autenticación en sus productos FortiOS. FortiProxy y FortiSwitchManager que podría conducir al acceso del administrador.

https://www.cgii.gob.bo/es/alertas-de-seguridad/omision-de-autenticacion-en-fortios-fortiproxy-y-fortiswitchmanager

Como se puede apreciar del contenido y análisis de cada caso reportado, el CGII cumple funciones de naturaleza técnica y no así investigativa del origen de los ataques y sus responsables. Los responsables de cada entidad o institución deberán efectuar las denuncias para iniciar el proceso investigativo que corresponda.

Paula Bauer
C.R. & F. Rojas Abogados
El presente articulo no se trata de un análisis, es un breve comentario sobre la norma legal vigente en Bolivia

Anteriores Boletines

- Bolivia y los Derechos de Autor en la Comunidad Andina de Naciones
- Latin Lawyer 250 has ranked C. R. & F. Rojas – Abogados as Highly Recommended Firm in its 2023 edition
- Comentarios sobre la Décima Segunda Versión de la Clasificación Internacional de Niza que incluye a los NFT
- The Legal 500 menciona a C.R. & F. Rojas – Abogados en su ranking 2022