MANUAL DE PROCEDIMIENTOS PARA LA GESTIÓN DE INCIDENTES Y VULNERABILIDADES INFORMÁTICAS

Aprobado con Resolución Administrativa AGETIC/RA/0016/2023, de 07 de marzo de 2023

ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS (ACGII)

AGETIC Digitalizando Bolivia	**FICHA DE CONTROL DE CAMBIOS**

Nombre del documento: Manual de procedimientos para la gestión de incidentes y vulnerabilidades informáticas.

Código del Documento: R.A. AGETIC/RA/0047/2022.

CONTROL DE CAMBIOS		
REF.	**VERSIÓN ANTERIOR**	**VERSIÓN ACTUAL**
1	"Manual de procedimientos para la gestión de incidentes y vulnerabilidades informáticas".	ACGII-PR04: Se agrega la asignación de casos en función al puesto y cargo del personal ACGII-PR05: Se agrega toma de decisión para aprobar la elaboración de publicaciones y distribución por lista de correo.

RESPONSABLES DE ELABORACIÓN, REVISIÓN Y DE CONFORMIDAD

Elaborado por:	Revisado por:	Conformidad:
Franz Rojas Cargo: Responsble ACGII Firma Digital	Adriana Orellana Cargo: Técnico de Planificación Firma Digital	Vladimir Terán Cargo: Director General Ejecutivo Firma Digital

CONTENIDO

CAPÍTULO I
DISPOSICIONES GENERALES

1. Objeto

Establecer procedimientos para gestionar incidentes y vulnerabilidades informáticas que afecten a sistemas de información de las entidades del sector público. La gestión involucra comunicar alertas y avisos de seguridad informática, otorgar información acerca de incidentes y vulnerabilidades reportadas o detectadas, además de prestar soporte técnico a solicitud a fin de contener, recuperar y erradicar el incidente o vulnerabilidad.

2. Marco Normativo

- **a.** Constitución Política del Estado, de 7 de febrero de 2009.
- **b.** Ley Nº 164, de 8 de agosto de 2011, Ley General de telecomunicaciones, Tecnologías de Información y Comunicación.
- **c.** Ley Nº 650, de 15 de enero de 2015, pilares de la Agenda Patriótica del Bicentenario 2025.
- **d.** Decreto Supremo Nº 1793, de 13 de noviembre de 2013, Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.
- **e.** Decreto supremo 2514, de 09 de septiembre de 2015, Creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación. Artículo 8, incisos a), d), h), i), j) y m) referente a las funciones del Centro de Gestión de Incidentes Informáticos.

3. Alcance y/o Ámbito de Aplicación

El presente manual de procedimientos es de aplicación para todo el personal del Área Centro de Gestión de Incidentes Informáticos cuyas actividades están relacionadas a la atención de incidentes y vulnerabilidades informáticas.

4. Previsión

En caso de presentarse dudas, omisiones, contradicciones y/o diferencias en la interpretación del presente manual, éstas serán solucionadas en los alcances y previsiones establecidas en las disposiciones legales y normativas pertinentes.

5. Definiciones

- **a. Alerta de seguridad informática,** es un comunicado que contiene datos referentes a una amenaza activa, una vulnerabilidad nueva o un incidente que tiene alta probabilidad de comprometer la seguridad de los sistemas de información de las entidades del sector público. Una alerta debe cumplir con los siguientes criterios:
  - Vulnerabilidad, incidente o amenaza crítica (o con puntaje alto) en productos o servicios de amplio uso o sensible.
  - Con o sin actualización de seguridad disponible.

- Se conoce campañas de explotación activa y agresiva
- Existe exploit público.
- Existe prueba de concepto.

b. Aviso de seguridad informática, es un comunicado que contiene datos referentes a una amenaza activa, una vulnerabilidad nueva o un incidente que tiene alto potencial de comprometer la seguridad de los sistemas de información de las entidades del sector público. Un aviso debe cumplir con los siguientes criterios:

- Vulnerabilidad, incidente o amenaza crítica (o con puntaje alto) en productos o servicios de amplio uso o sensible.
- Actualización de seguridad disponible.
- No se conoce su explotación activa.
- No existe exploit público.
- No existe prueba de concepto.

c. Vulnerabilidad informática, controles técnicos deficientes o inexistentes que pueden ser aprovechadas por actores de amenazas para comprometer la seguridad de la información.

d. Incidente informático, es el aprovechamiento de una o varias vulnerabilidades con impacto en la confidencialidad o integridad de la información, así como en la disponibilidad de servicios.

e. Actividad maliciosa, técnicamente se refiere a la detección e identificación de actores de amenazas que buscan aprovechar una o varias vulnerabilidades en el software y en el usuario final.

f. Sistema de información, conjunto de elementos que permiten administrar, recolectar, recuperar, procesar, almacenar y distribuir información dentro de la infraestructura tecnológica de una entidad.

g. RTIR, abreviatura de Request Tracker for Incident Response (RTIR), herramienta de código abierto para registro y seguimiento de casos de incidentes y vulnerabilidades informáticas.

6. Aprobación, Vigencia, Difusión e Implementación

El presente manual deberá ser aprobado por el Director General Ejecutivo de la AGETIC mediante Resolución Administrativa.

La vigencia del manual será a partir de la fecha establecida en la Resolución Administrativa de aprobación.

La difusión del manual será realizada por el Área de Planificación (AP) en coordinación con el Área Centro de Gestión de Incidentes Informáticos (ACGII), siendo de conocimiento general por el personal de la AGETIC.

La aplicación del manual de procedimientos será efectuada por el Área Centro de Gestión de Incidentes Informáticos.

7. Revisión y Actualización

El presente manual de procedimientos deberá ser ajustado y/o actualizado cuando se produzcan cambios o ajustes en el marco normativo, o cuando por razones internas y/ o del entorno se justifique realizar modificaciones.

El Área Centro de Gestión de Incidentes Informáticos en coordinación con el AP, realizará el ajuste y actualización del manual de procedimientos cuando se produzcan los cambios señalados.

Toda vez que el manual de procedimientos sea actualizado, deberá darse cumplimiento al punto precedente de Aprobación, Vigencia, Difusión e Implementación.

CAPÍTULO II
PROCEDIMIENTOS

8. Procedimiento para la atención de incidentes y vulnerabilidades informáticas

	MANUAL DE PROCEDIMIENTOS AGETIC	**Código:**	ACGII-PR04
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	0
		Páginas:	1 de 4
	Procedimiento para la atención de incidentes y vulnerabilidades informáticas	**Aprobado con:**	R.A. AGETIC/RA/0016/2023 de 07/03/2023
Objetivo: Establecer las actividades necesarias para validar, comunicar, dar seguimiento y otorgar soporte técnico para solucionar incidentes y vulnerabilidades informáticas que afecten a sistemas de información de las entidades del sector público. Funciones del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.			

N°	ACTIVIDAD	RESPONSABLE	SALIDA
1	Reporta incidente o vulnerabilidad informática por correo electrónico, herramienta RTIR o página web, son reportantes los Responsables de seguridad de la información de las entidades públicas, personal del Área Centro de Gestión de Incidentes Informáticos, organismos nacionales e internacionales de similar función al ACGII y personas con conocimientos en seguridad informática.	Reportante	Registro RTIR
2	Valida reporte para evitar falsos positivos, de ser necesario solicita datos adicionales al reportante.	Personal ACGII	Historial RTIR

AGETIC	**MANUAL DE PROCEDIMIENTOS AGETIC**	**Código:**	ACGII-PR04
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	1
		Páginas:	2 de 4
	Procedimiento para la atención de incidentes y vulnerabilidades informáticas	**Aprobado con:**	R.A. AGETIC/RA/0016/2023 de 07/03/2023

Objetivo: Establecer las actividades necesarias para validar, comunicar, dar seguimiento y otorgar soporte técnico para solucionar incidentes y vulnerabilidades informáticas que afecten a sistemas de información de las entidades del sector público. Funciones del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
3	Si el reporte no es válido, rechaza cuando el reporte no corresponde a un incidente o vulnerabilidad o no se tiene respuesta a datos adicionales solicitados al reportante.	Personal ACGII	Historial RTIR
4	Si el reporte es válido, registra el incidente o vulnerabilidad, que se comunica al Responsable ACGII para su priorización y asignación.	Personal ACGII	Historial RTIR
5	Prioriza atención y asigna el incidente o vulnerabilidad al personal del ACGII considerando el puesto y cargo.	Responsable ACGII	Historial RTIR
6	Comunica con correo electrónico al contacto técnico de la entidad pública afectada, otorgando información acerca del incidente o vulnerabilidad, recomendando acciones y plazo de solución de acuerdo a la severidad del caso. También realiza la notificación por llamada telefónica para confirmar la recepción del correo electrónico.	Personal ACGII	Historial RTIR
7	El contacto técnico de la Entidad Pública toma conocimiento del incidente/vulnerabilidad, de requerir solicita soporte técnico o ampliación de plazo caso contrario toma acción para solucionar el incidente o vulnerabilidad, (Pasa al numeral 10).	Entidad Pública	Historial RTIR

AGETIC Digitalizando Bolivia	**MANUAL DE PROCEDIMIENTOS AGETIC**	**Código:**	ACGII-PR04
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	1
		Páginas:	3 de 4
	Procedimiento para la atención de incidentes y vulnerabilidades informáticas	**Aprobado con:**	R.A. AGETIC/RA/0016/2023 de 07/03/2023

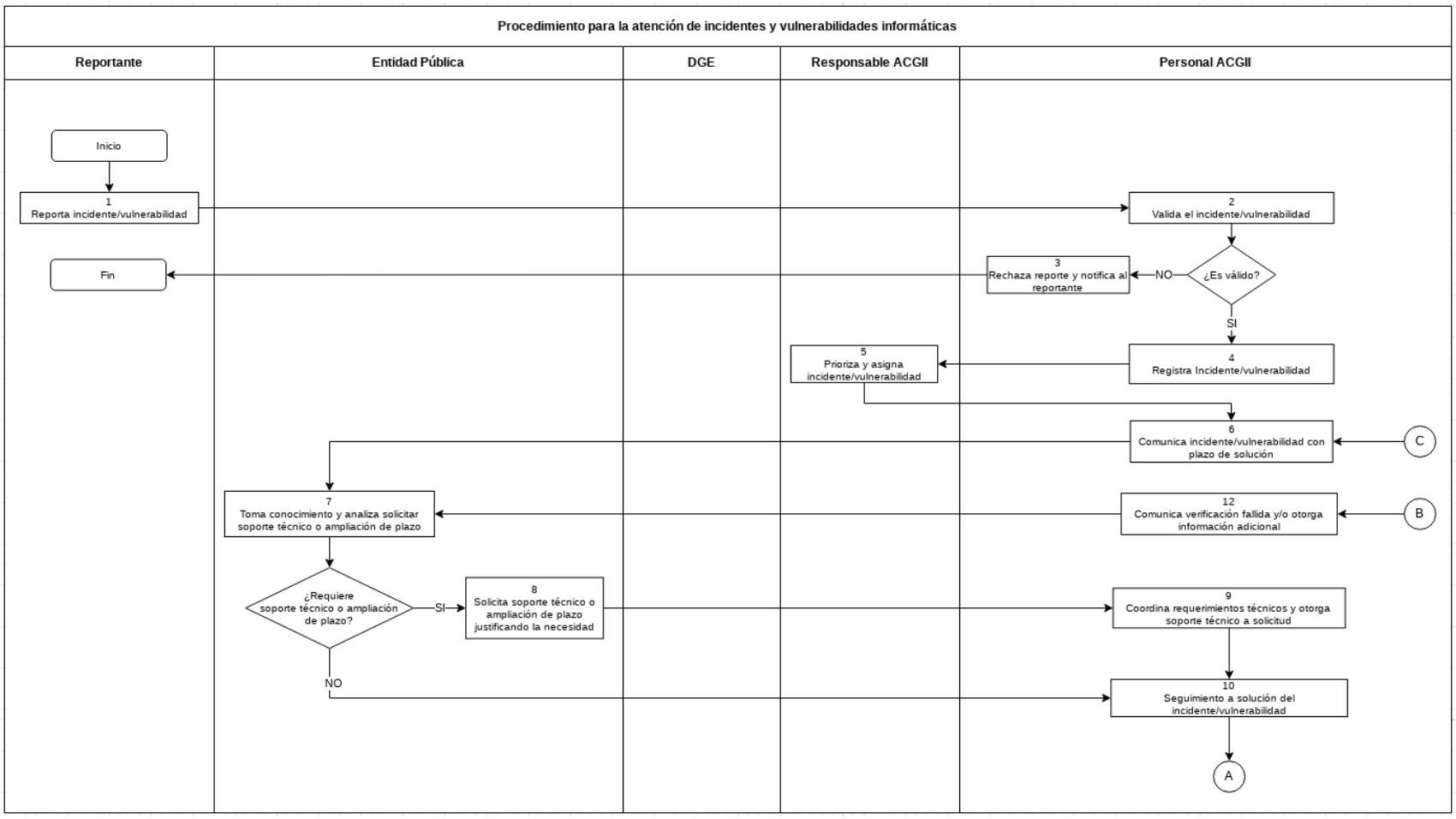
Objetivo: Establecer las actividades necesarias para validar, comunicar, dar seguimiento y otorgar soporte técnico para solucionar incidentes y vulnerabilidades informáticas que afecten a sistemas de información de las entidades del sector público. Funciones del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.

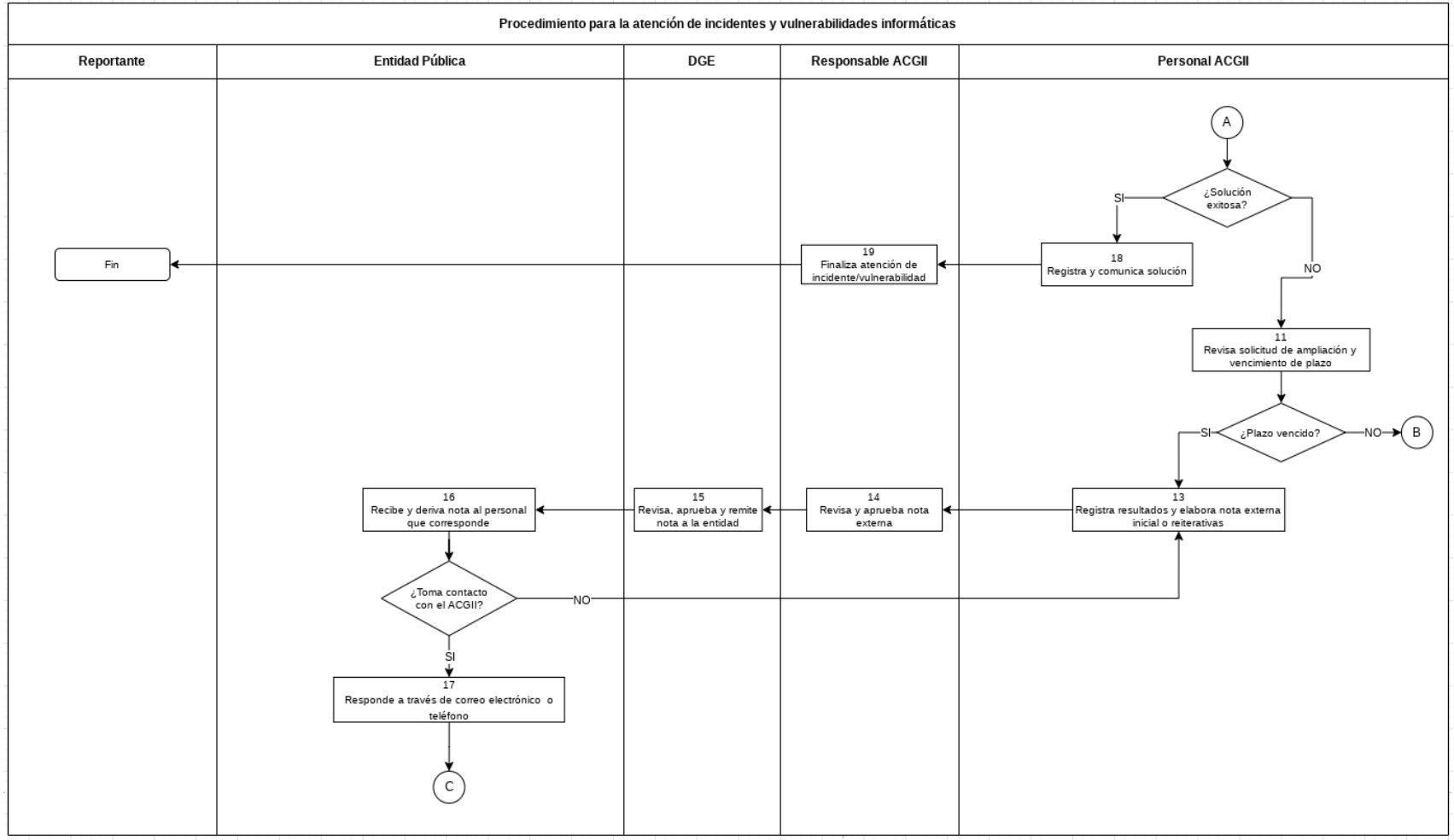
N°	ACTIVIDAD	RESPONSABLE	SALIDA
8	De requerir, el contacto técnico solicita soporte técnico o ampliación del plazo de solución en respuesta a la comunicación, justificando los motivos de la solicitud que se registra en el historial del caso.	Entidad Pública	Historial RTIR
9	Coordina requerimientos técnicos necesarios para otorgar el soporte técnico en estrecha coordinación con el contacto de la Entidad Pública, documentando las acciones realizadas.	Personal ACGII	Historial RTIR
10	Realiza seguimiento del caso, verificando el estado de solución del incidente o vulnerabilidad a solicitud del contacto técnico o al vencimiento del plazo.	Personal ACGII	Historial RTIR
11	Si la solución no fue exitosa, revisa en el historial del caso los plazos de solución y acciones efectuadas por el contacto técnico.	Personal ACGII	Registro RTIR
12	Si, el plazo no concluyo comunica el resultado fallido de la verificación al contacto técnico de la Entidad Pública otorgando información adicional o brindando la asistencia técnica en base a las acciones efectuadas por el contacto técnico, (Pasa al numeral 7).	Personal ACGII	Historial RTIR
13	Si la solución no fue exitosa y el plazo de solución concluyó sin acciones efectuadas por el contacto técnico, el Personal del ACGII elabora la nota externa inicial o reiterativas previo conocimiento del Responsable del ACGII.	Personal ACGII	Historial RTIR Nota Externa

AGETIC Digitalizando Bolivia	**MANUAL DE PROCEDIMIENTOS AGETIC**	**Código:**	ACGII-PR04
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	1
		Páginas:	4 de 4
	Procedimiento para la atención de incidentes y vulnerabilidades informáticas	**Aprobado con:**	R.A. AGETIC/RA/0016/2023 de 07/03/2023

Objetivo: Establecer las actividades necesarias para validar, comunicar, dar seguimiento y otorgar soporte técnico para solucionar incidentes y vulnerabilidades informáticas que afecten a sistemas de información de las entidades del sector público. Funciones del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
14	Revisa y aprueba nota externa de comunicación inicial o reiterativa.	Responsable ACGII	Progreso del documento (Flujo)
15	Revisa, aprueba y remite nota externa a la Entidad Pública.	DGE	Progreso del documento (Flujo
16	Recibe y deriva nota al personal que corresponda. Si el personal de la Entidad Pública no toma contacto con el ACGII, (Pasa al numeral 13).	Entidad Pública	Nota externa recibida
17	Si el personal designado por la Entidad Pública toma contacto con el personal del ACGII a cargo del caso vía correo electrónico institucional o teléfono, el contacto se registra en RTIR, adjuntando el correo si corresponde, (Pasa al numeral 6).	Entidad Pública	Historial RTIR
18	Si la solución fue exitosa, registra el resultado y comunica al contacto técnico de la Entidad Pública y al Responsable del ACGII para finalizar la atención del incidente o vulnerabilidad.	Personal ACGII	Registro RTIR
19	Finaliza la atención del incidente o vulnerabilidad, previa verificación de la solución. La finalización es comunicada al reportante a través del RTIR.	Responsable ACGII	Historial RTIR


Procedimiento para la atención de incidentes y vulnerabilidades informáticas
Reportante
Entidad Pública
DGE
Responsable ACGII
Personal ACGII
Inicio
1
Reporta incidente/vulnerabilidad
Fin
2
Valida el incidente/vulnerabilidad
¿Es válido?
NO
3
Rechaza reporte y notifica al reportante
SI
4
Registra Incidente/vulnerabilidad
5
Prioriza y asigna incidente/vulnerabilidad
6
Comunica incidente/vulnerabilidad con plazo de solución
C
7
Toma conocimiento y analiza solicitar soporte técnico o ampliación de plazo
12
Comunica verificación fallida y/o otorga información adicional
B
¿Requiere soporte técnico o ampliación de plazo?
SI
8
Solicita soporte técnico o ampliación de plazo justificando la necesidad
9
Coordina requerimientos técnicos y otorga soporte técnico a solicitud
NO
10
Seguimiento a solución del incidente/vulnerabilidad
A


Procedimiento para la atención de incidentes y vulnerabilidades informáticas
Reportante
Entidad Pública
DGE
Responsable ACGII
Personal ACGII
A
¿Solución exitosa?
SI
NO
Fin
19
Finaliza atención de incidente/vulnerabilidad
18
Registra y comunica solución
11
Revisa solicitud de ampliación y vencimiento de plazo
¿Plazo vencido?
SI
NO
B
16
Recibe y deriva nota al personal que corresponde
15
Revisa, aprueba y remite nota a la entidad
14
Revisa y aprueba nota externa
13
Registra resultados y elabora nota externa inicial o reiterativas
¿Toma contacto con el ACGII?
NO
SI
17
Responde a través de correo electrónico o teléfono
C

9. Procedimiento para elaborar y comunicar alertas y avisos de seguridad informática

	MANUAL DE PROCEDIMIENTOS AGETIC	**Código:**	ACGII-PR05
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	1
		Páginas:	1 de 3
	Procedimiento para elaborar y comunicar alertas y avisos de seguridad informática	**Aprobado con:**	R.A. AGETIC/RA/0016/2023 de 07/03/2023

Objetivo: Establecer las actividades necesarias para elaborar y comunicar alertas y avisos de seguridad informática a Responsables de Seguridad de la Información y personal de Tecnologías de Información y Comunicación de las Entidades del sector público. En el marco de políticas y acciones para la prevención de incidentes informáticos que realiza el CGII.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
1	Designa por el periodo de un mes al personal del ACGII encargado de realizar la revisión y análisis de información de nuevas vulnerabilidades y actividades maliciosas publicadas en plataformas de noticias de ciberseguridad y organismos de similar función al ACGII. Las alertas y avisos también se podrían originar de la atención de incidentes y vulnerabilidades informáticas que realiza el ACGII.	Responsable ACGII	Instructivo
2	El personal designado revisa publicaciones hechas por plataformas de ciberseguridad sobre nuevas vulnerabilidades y actividades maliciosas que podrían tener un impacto negativo en sistemas de información de las entidades publicas. Envía por correo los enlaces fuente para consideración y autorización del Responsable.	Personal del ACGII	Correo electrónico

AGETIC	**MANUAL DE PROCEDIMIENTOS AGETIC**	**Código:**	ACGII-PR05
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	1
		Páginas:	2 de 3
	Procedimiento para elaborar y comunicar alertas y avisos de seguridad informática	**Aprobado con:**	R.A. AGETIC/RA/0016/2023 de 07/03/2023

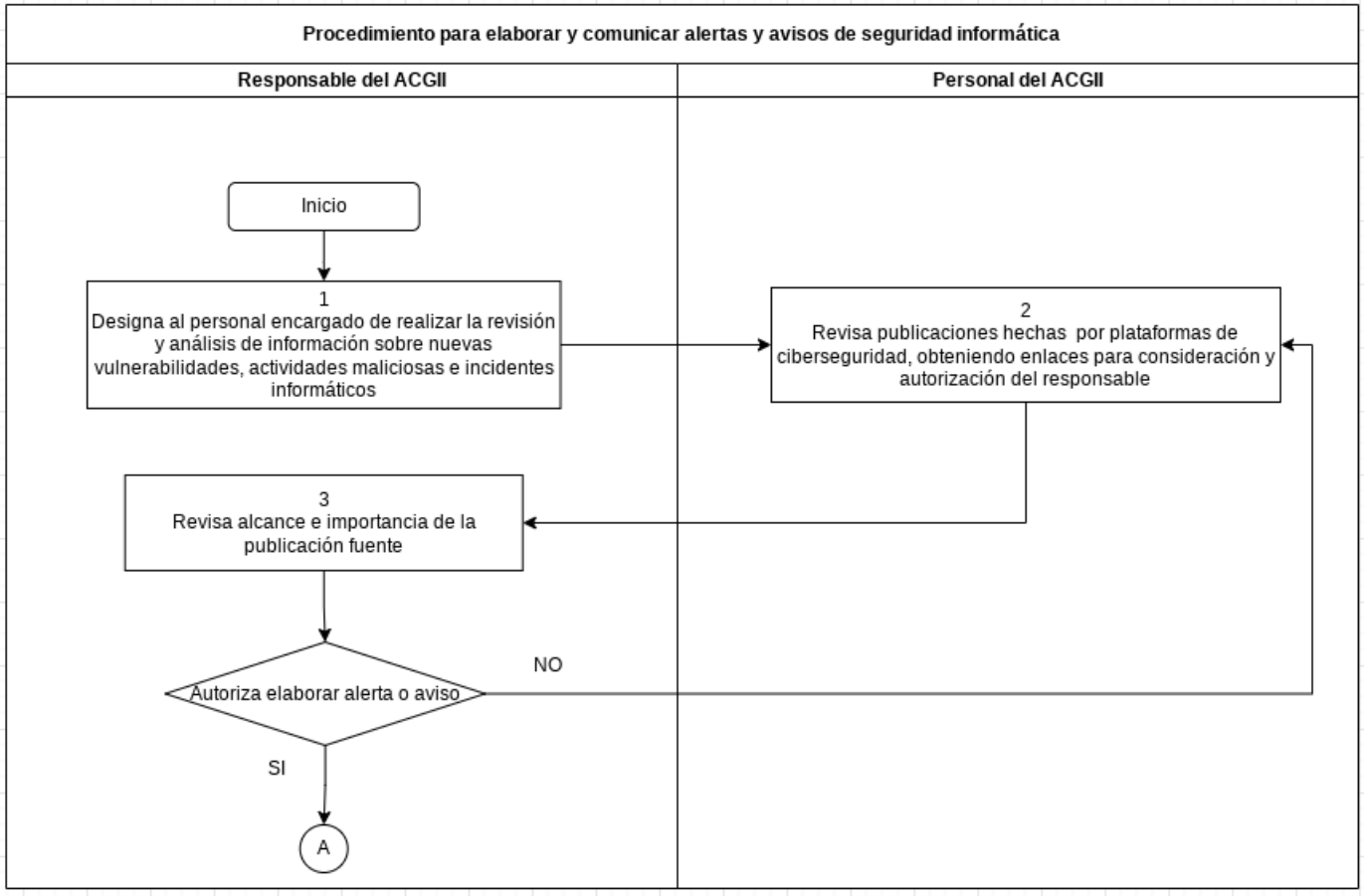
Objetivo: Establecer las actividades necesarias para elaborar y comunicar alertas y avisos de seguridad informática a Responsables de Seguridad de la Información y personal de Tecnologías de Información y Comunicación de las Entidades del sector público. En el marco de políticas y acciones para la prevención de incidentes informáticos que realiza el CGII.

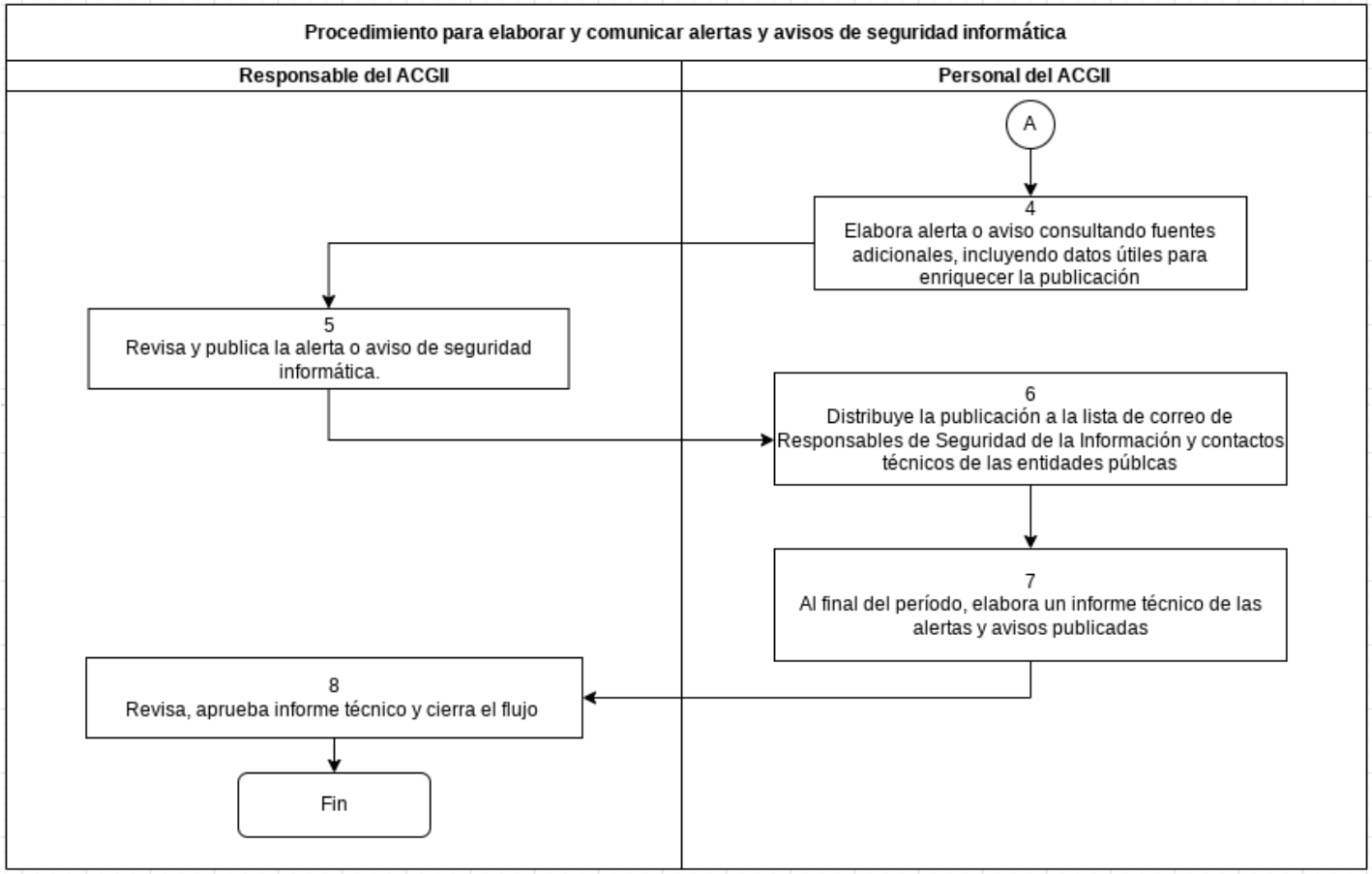
N°	ACTIVIDAD	RESPONSABLE	SALIDA
3	Analiza el alcance e importancia de las publicaciones fuente. Si no autoriza la elaboración de la alerta o aviso (pasa al numeral 2).	Responsable ACGII	Correo electrónico
4	Si se autoriza la alerta o aviso, se elabora la alerta o aviso de seguridad en la página web, consultando fuentes adicionales para incluir datos útiles en la publicación.	Personal ACGII	Contenido elaborado en sitio web del ACGII
5	Revisa y publica la alerta o aviso de seguridad informática.	Responsable ACGII	Contenido publicado en sitio web del ACGII
6	Distribuye la alerta o aviso de seguridad a la lista correo de Responsables de Seguridad de la Información y contactos técnicos de las Entidades Públicas.	Personal ACGII	Lista de correo distribuido

AGETIC Digitalizando Bolivia	**MANUAL DE PROCEDIMIENTOS AGETIC**	**Código:**	ACGII-PR05
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	1
		Páginas:	3 de 3
	Procedimiento para elaborar y comunicar alertas y avisos de seguridad informática	**Aprobado con:**	R.A. AGETIC/RA/0016/2023 de 07/03/2023

Objetivo: Establecer las actividades necesarias para elaborar y comunicar alertas y avisos de seguridad informática a Responsables de Seguridad de la Información y personal de Tecnologías de Información y Comunicación de las Entidades del sector público. En el marco de políticas y acciones para la prevención de incidentes informáticos que realiza el CGII.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
7	Al final del periodo, el personal designado elabora un informe técnico dirigido al Responsable del ACGII informando la publicación de alertas y avisos de seguridad informática aprobadas, que debe incluir enlaces de la publicación y adjuntar las alertas o avisos en formato pdf que se distribuyeron a la lista de correo. De no existir publicaciones en el periodo, el personal designado deberá informar de las revisiones realizadas adjuntando los correos intercambiados con el Responsable ACGII.	Personal ACGII	Informe Técnico
8	Revisa, aprueba nota interna y cierra el flujo.	Responsable ACGII	Progreso del documento (flujo)


Procedimiento para elaborar y comunicar alertas y avisos de seguridad informática
Responsable del ACGII
Personal del ACGII
Inicio
1
Designa al personal encargado de realizar la revisión y análisis de información sobre nuevas vulnerabilidades, actividades maliciosas e incidentes informáticos
2
Revisa publicaciones hechas por plataformas de ciberseguridad, obteniendo enlaces para consideración y autorización del responsable
3
Revisa alcance e importancia de la publicación fuente
Autoriza elaborar alerta o aviso
NO
SI
A


Procedimiento para elaborar y comunicar alertas y avisos de seguridad informática
Responsable del ACGII
Personal del ACGII
A
4
Elabora alerta o aviso consultando fuentes adicionales, incluyendo datos útiles para enriquecer la publicación
5
Revisa y publica la alerta o aviso de seguridad informática.
6
Distribuye la publicación a la lista de correo de Responsables de Seguridad de la Información y contactos técnicos de las entidades públicas
7
Al final del período, elabora un informe técnico de las alertas y avisos publicadas
8
Revisa, aprueba informe técnico y cierra el flujo
Fin