MANUAL DE PROCEDIMIENTOS PARA REALIZAR EVALUACIONES DE SEGURIDAD INFORMÁTICA

Aprobado con Resolución Administrativa AGETIC/RA/0017/2023, 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: Procedimiento de Evaluación de Seguridad de los Sistemas de Información de Entidades Públicas.

Código del Documento: R.A. AGETIC/RA/0043/2019-AGETIC/RA/0082/2022

CONTROL DE CAMBIOS		
REF.	**VERSIÓN ANTERIOR**	**VERSIÓN ACTUAL**
1	"Procedimiento de Evaluación de seguridad a sistemas de información de entidades públicas". Aprobado mediante Resolución Administrativa AGETIC/RA/0043/2019 de 19 de julio de 2019	Procedimiento de evaluación de seguridad informática a solicitud de Entidades Públicas
2	-	Procedimiento de evaluación de seguridad informática interna
3	-	Procedimiento de evaluación de seguridad informática externa a Entidades Públicas
4	-	Formato de cronograma de evaluación de seguridad informática externa a Entidades Públicas
5	"Manual de procedimientos para realizar evaluaciones de seguridad informática" AGETIC/RA/0082/2022 de 19 de julio de 2022	ACGII-PR01: Se agrega alcance de la evaluación, puesto y cargo del personal para asignar la evaluación. ACGII-PR02: Se agrega alcance de la evaluación, puesto y cargo del personal para asignar la evaluación. ACGII-PR03: Se simplifica el procedimiento en cuanto a coordinación y comunicación con las entidades públicas.

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 realizar evaluaciones de seguridad informática a sistemas de información de las Entidades públicas. Las evaluaciones tienen el objetivo de identificar vulnerabilidades e incidentes informáticos y errores de configuración.

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.
- **f.** Decreto Supremo 2514, Artículo 8, incisos e) y l) 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 con evaluaciones de seguridad informática.

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. Evaluación de seguridad informática,** es la identificación a través de técnicas manuales y automatizadas de vulnerabilidades, incidentes o errores de configuración en sistemas de información.
- **b. Vulnerabilidad informática,** controles técnicos deficientes o inexistentes que pueden ser aprovechadas por actores de amenazas para comprometer la seguridad de la información.
- **c. 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.
- **d. Sistema de información,** conjunto de elementos que permiten administrar, recolectar, recuperar, procesar, almacenar y distribuir información dentro de la infraestructura tecnológica de una entidad.

e. **Acta de coordinación,** documento que establece acuerdos técnicos y operativos para realizar la evaluación de seguridad.
f. **Acta de presentación,** documento que evidencia la presentación de los resultados obtenidos en la evaluación de seguridad a las partes interesadas y establece acuerdos y acciones posteriores.
g. **Prueba de concepto,** evidencia técnica de la identificación de la vulnerabilidad que puede ser reproducida por la parte interesada y útil para verificar posteriormente la solución.
h. **RTIR,** abreviatura de Request Tracker for Incident Response, herramienta de ćodigo abierto para registro y seguimiento de casos de incidentes y vulnerabilidades.

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 de evaluación de seguridad informática a solicitud de Entidades Públicas

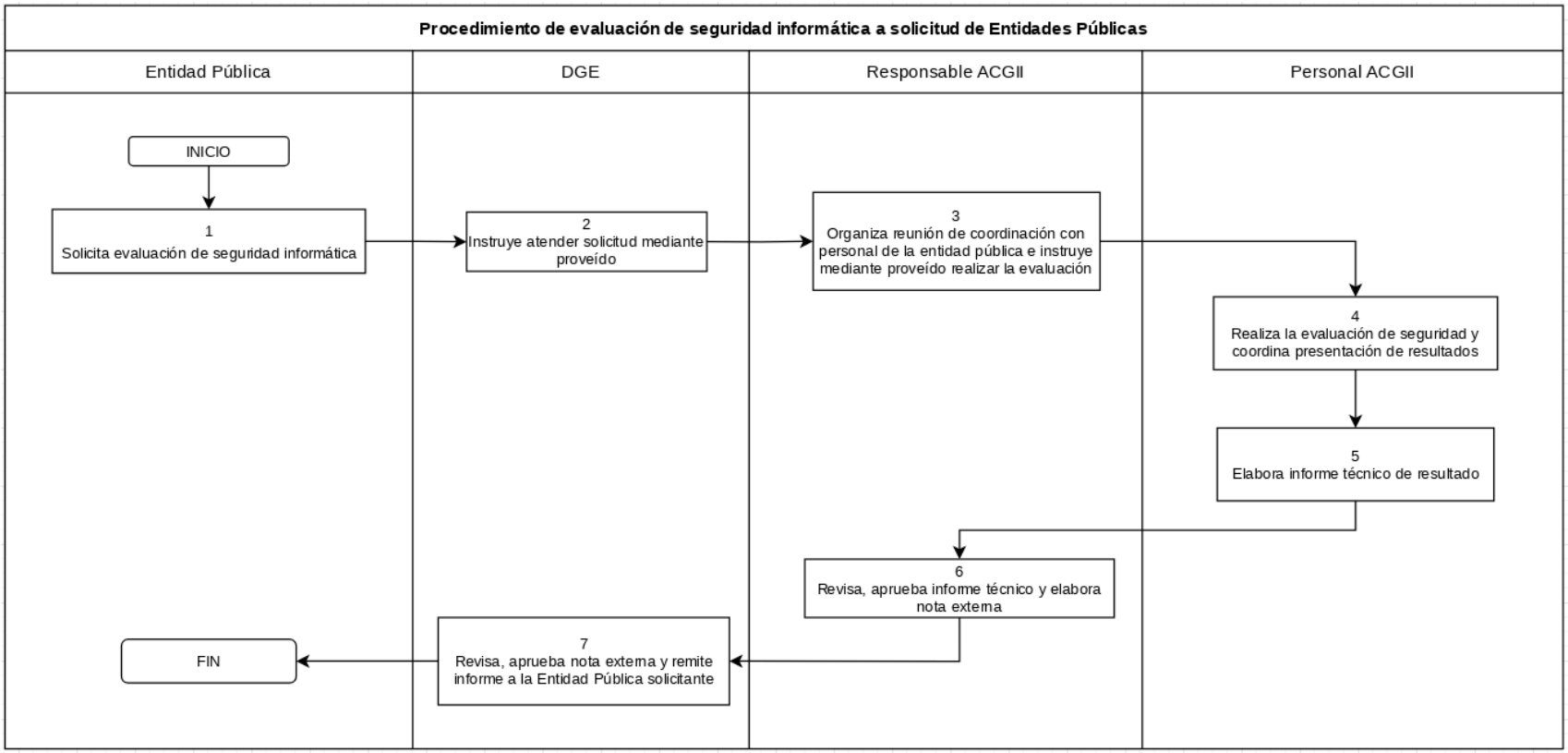
	MANUAL DE PROCEDIMIENTOS AGETIC	**Código:**	ACGII-PR01
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	3
		Páginas:	1 de 2
	Procedimiento de evaluación de seguridad informática a solicitud de Entidades Públicas	**Aprobado con:**	R.A. AGETIC/RA/0017/2023 de 07/03/2023
Objetivo: Establecer las actividades necesarias para atender solicitudes de evaluación de seguridad informática a sistemas de información realizadas por entidades públicas, función del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.			

N°	ACTIVIDAD	RESPONSABLE	SALIDA
1	Solicita evaluación de seguridad informática mediante nota formal dirigido al Director General Ejecutivo de AGETIC.	Entidad pública solicitante	Nota externa
2	Deriva e instruye atender la solicitud mediante proveído al Responsable ACGII.	DGE	Progreso del documento (Flujo)
3	Coordina reunión con el personal de la entidad solicitante, a objeto de establecer la modalidad de evaluación, alcances, requerimientos, persona de contacto y tiempo estimado para realizar la evaluación. Acuerdos que quedan establecidos en acta de coordinación firmada por ambas partes. El Responsable ACGII en función del alcance de la evaluación, puesto y cargo del personal, instruye mediante proveído realizar la evaluación en base a los acuerdos acordados.	Responsable ACGII	Acta de coordinación

	MANUAL DE PROCEDIMIENTOS AGETIC	**Código:**	ACGII-PR01
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	3
		Páginas:	2 de 2
	Procedimiento de evaluación de seguridad informática a solicitud de Entidades Públicas	**Aprobado con:**	R.A. AGETIC/RA/0017/2023 de 07/03/2023

Objetivo: Establecer las actividades necesarias para atender solicitudes de evaluación de seguridad informática a sistemas de información realizadas por entidades públicas, función del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
4	Realiza la evaluación de seguridad informática conforme a acuerdos de reunión de coordinación, el trabajo es supervisado por el Responsable ACGII. Finalizada la evaluación, el personal ACGII coordina la reunión de presentación de resultados con la persona de contacto de la entidad solicitante.	Personal ACGII	Acta de presentación
5	Elabora informe técnico de resultados de la evaluación de seguridad informática con clasificación confidencial, adjuntando documento de pruebas de concepto, acta de coordinación y presentación, que envía al Responsable ACGII.	Personal ACGII	Informe técnico de resultados
6	Revisa y aprueba informe técnico, elabora nota externa informando a la Máxima Autoridad Ejecutiva de la entidad solicitante la conclusión de la evaluación de seguridad informática, solicitando informar a la AGETIC la solución de vulnerabilidades para que el ACGII proceda con la verificación correspondiente.	Responsable ACGII	Nota externa
7	Revisa y aprueba nota externa, remite informe técnico en sobre cerrado a la entidad solicitante.	DGE	Nota externa remitida


Procedimiento de evaluación de seguridad informática a solicitud de Entidades Públicas
Entidad Pública
DGE
Responsable ACGII
Personal ACGII
INICIO
1
Solicita evaluación de seguridad informática
2
Instruye atender solicitud mediante proveído
3
Organiza reunión de coordinación con personal de la entidad pública e instruye mediante proveído realizar la evaluación
4
Realiza la evaluación de seguridad y coordina presentación de resultados
5
Elabora informe técnico de resultado
6
Revisa, aprueba informe técnico y elabora nota externa
7
Revisa, aprueba nota externa y remite informe a la Entidad Pública solicitante
FIN

9. Procedimiento de evaluación de seguridad informática interna

	MANUAL DE PROCEDIMIENTOS AGETIC	**Código:**	ACGII-PR02
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	1
		Páginas:	1 de 2
	Procedimiento de evaluación de seguridad informática interna	**Aprobado con:**	R.A. AGETIC/RA/0017/2023, de 03/07/2023

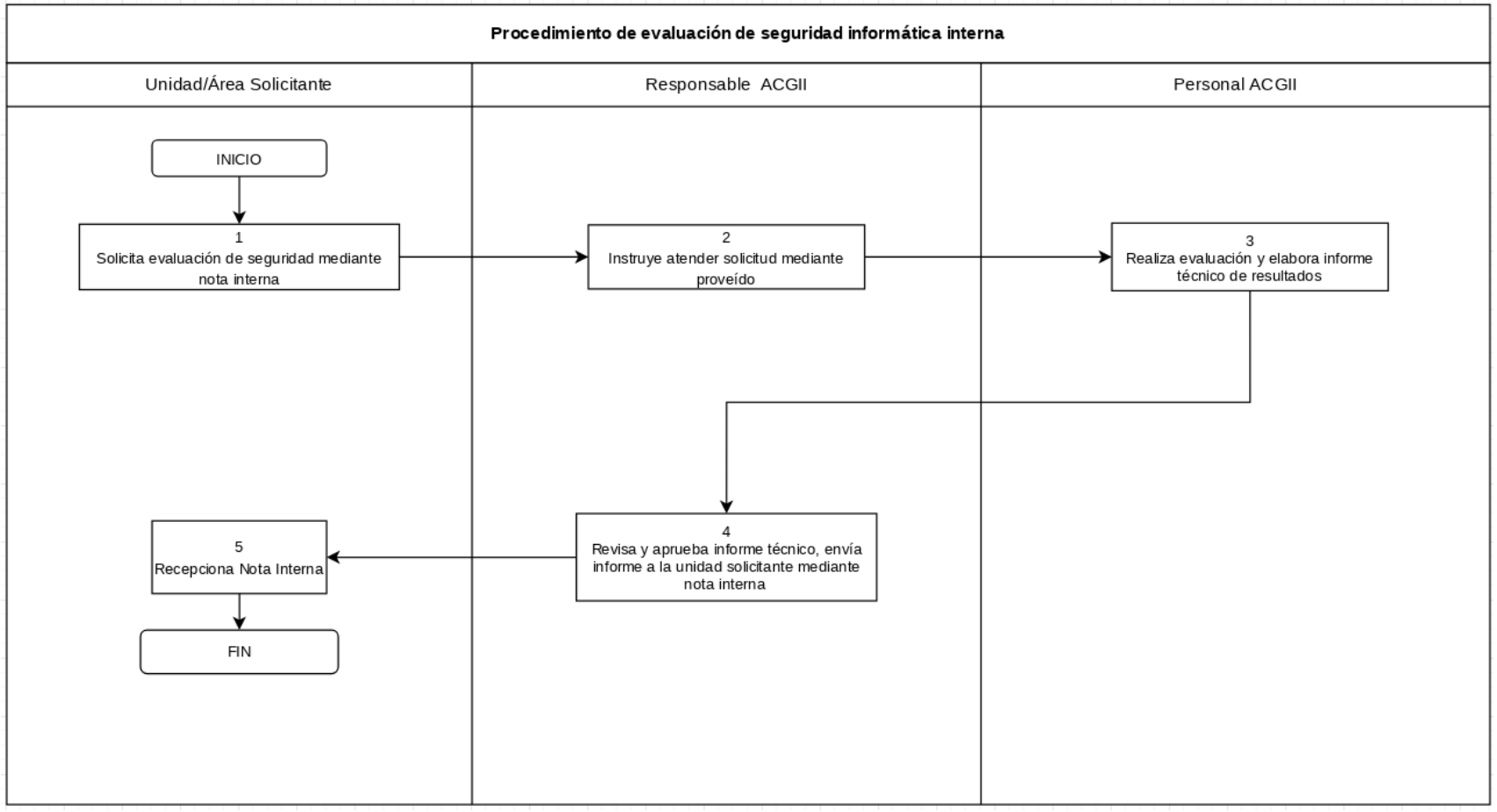
Objetivo: Establecer las actividades necesarias para atender solicitudes de evaluación de seguridad informática internas de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, función del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
1	Solicita evaluación de seguridad informática al Responsable ACGII mediante nota interna según conducto regular.	Unidad/Área solicitante	Nota interna
2	Deriva la solicitud al Personal ACGII considerando el puesto y cargo en función del alcance solicitado de la evaluación, instruyendo mediante proveído atender la solicitud.	Responsable ACGII	Progreso del documento (flujo)
3	Realiza la evaluación de seguridad informática, de ser necesario coordina con la unidad/área solicitante aspectos técnicos y operativos. Finalizada la evaluación, elabora informe técnico de resultados adjuntando documento de pruebas de concepto y envía informe al Responsable ACGII.	Personal ACGII	Informe Técnico de Resultados

	MANUAL DE PROCEDIMIENTOS AGETIC	**Código:**	ACGII-PR02
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	1
		Páginas:	2 de 2
	Procedimiento de evaluación de seguridad informática interna	**Aprobado con:**	R.A. AGETIC/RA/0039/2022, de 20/05/2022

Objetivo: Establecer las actividades necesarias para atender solicitudes de evaluación de seguridad informática internas de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, función del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
4	Revisa y aprueba informe técnico, y comunica mediante nota interna a la Unidad/Área solicitante la conclusión de la evaluación, solicitando informar al ACGII la solución de las vulnerabilidades para proceder con la verificación.	Responsable ACGII	Nota Interna
5	Revisa y aprueba informe técnico y deriva con nota interna a la unidad solicitante.	Unidad/Área solicitante	Progreso del documento (flujo)


Procedimiento de evaluación de seguridad informática interna
Unidad/Área Solicitante
Responsable ACGII
Personal ACGII
INICIO
1
Solicita evaluación de seguridad mediante nota interna
2
Instruye atender solicitud mediante proveído
3
Realiza evaluación y elabora informe técnico de resultados
4
Revisa y aprueba informe técnico, envía informe a la unidad solicitante mediante nota interna
5
Recepciona Nota Interna
FIN

10. Procedimiento de evaluación de seguridad informática externa a Entidades Públicas

	MANUAL DE PROCEDIMIENTOS AGETIC	**Código:**	ACGII-PR03
	AREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	3
		Páginas:	1 de 3
	Procedimiento de evaluación de seguridad informática externa a Entidades Públicas	**Aprobado con:**	R.A. AGETIC/RA/0017/2023, de 07/03/2023

Objetivo: Establecer las actividades necesarias para realizar evaluaciones de seguridad informática externas a sistemas de información de las Entidades Públicas a requerimiento de la AGETIC, en el marco de las funciones del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
1	Elabora informe técnico a la Dirección General Ejecutiva sobre la modalidad y alcance de la evaluación de seguridad informática externa a sistemas de información de las entidades del sector público por un determinado período de tiempo, solicitando autorización conforme las funciones de la AGETIC.	Responsable ACGII	Informe técnico
2	Revisa y autoriza la modalidad y alcance de la evaluación de seguridad, instruyendo mediante proveído proceder con las evaluaciones.	DGE	Progreso del documento (Flujo)

	MANUAL DE PROCEDIMIENTOS AGETIC	**Código:**	ACGII-PR03
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	3
		Páginas:	2 de 3
	Procedimiento de evaluación de seguridad informática externa a Entidades Públicas	**Aprobado con:**	R.A. AGETIC/RA/0017/2023, de 03/07/2023

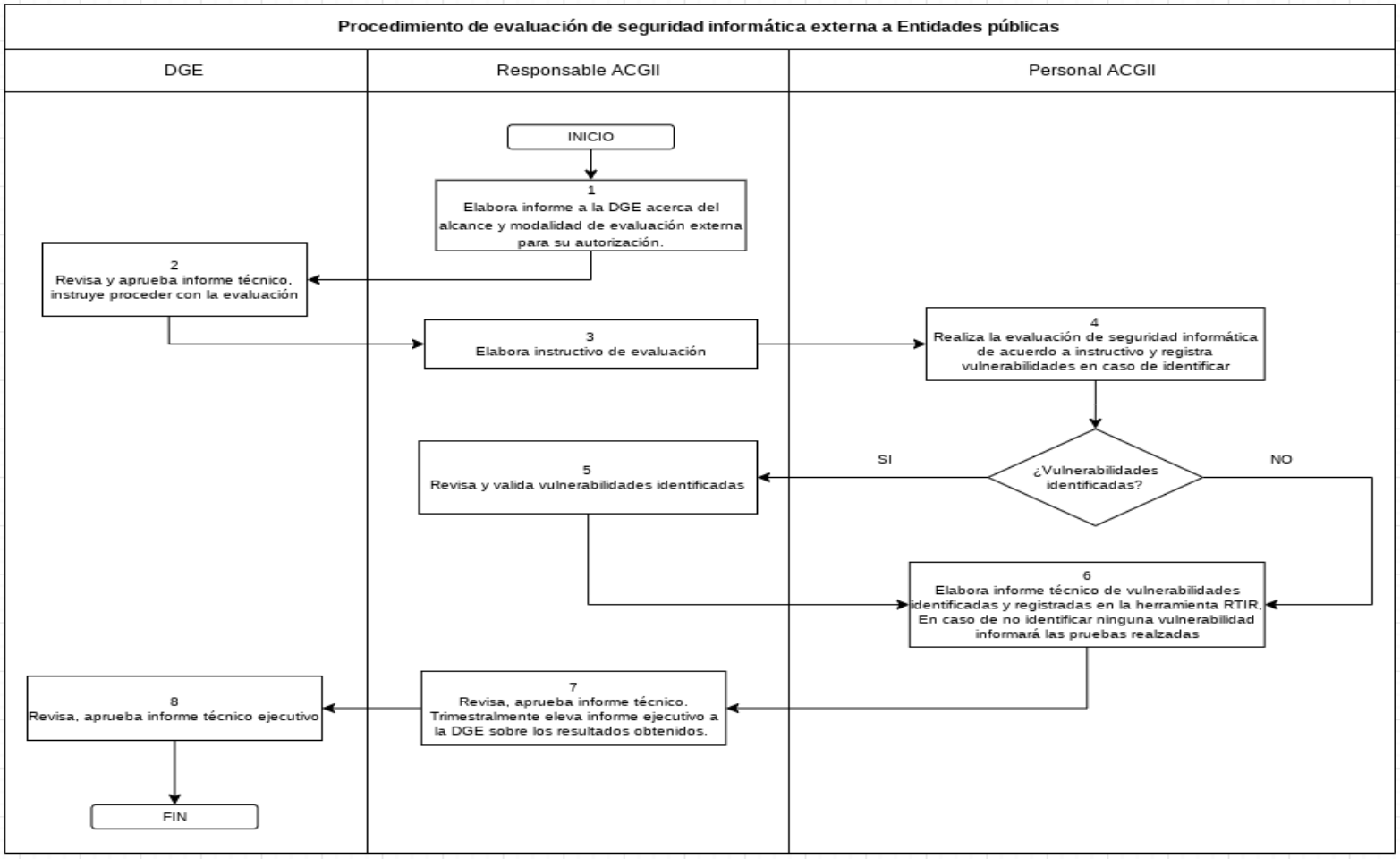
Objetivo: Establecer las actividades necesarias para realizar evaluaciones de seguridad informática externas a sistemas de información de las Entidades Públicas a requerimiento de la AGETIC, en el marco de las funciones del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
3	Instruye al Personal ACGII realizar la evaluación de seguridad informática externa considerando el puesto y cargo. La instrucción incluirá como dato inicial nombres de dominio y tiempo estimado.	Responsable ACGII	Instructivo
4	Realiza la evaluación de seguridad informática externa de acuerdo a instructivo y registra las vulnerabilidades en la herramienta RTIR con respaldo de pruebas de concepto. De no identificar vulnerabilidades (pasa al numeral 6).	Personal ACGII	Registro de vulnerabilidades en la herramienta RTIR
5	De identificar vulnerabilidades, valida las vulnerabilidades registradas en la herramienta RTIR para su gestión respecto a la comunicación, seguimiento y solución con la entidad afectada.	Responsable ACGII	Historial RTIR
6	Finalizada la evaluación elabora informe técnico dirigido al Responsable ACGII describiendo las vulnerabilidades identificadas. De no identificar vulnerabilidades el informe debe detallar las pruebas realizadas.	Personal ACGII	Informe técnico

	MANUAL DE PROCEDIMIENTOS AGETIC	**Código:**	ACGII-PR03
	ÁREA CENTRO DE GESTIÓN DE INCIDENTES INFORMÁTICOS	**Versión:**	3
		Páginas:	3 de 3
	Procedimiento de evaluación de seguridad informática externa a Entidades Públicas	**Aprobado con:**	R.A. AGETIC/RA/0017/2023, de 07/03/2023

Objetivo: Establecer las actividades necesarias para realizar evaluaciones de seguridad informática externas a sistemas de información de las Entidades Públicas a requerimiento de la AGETIC, en el marco de las funciones del Centro de Gestión de Incidentes Informáticos establecido en D.S. 2514 artículo 8.

N°	ACTIVIDAD	RESPONSABLE	SALIDA
7	Revisa y aprueba informe técnico de resultados de la evaluación. Al final del periodo de evaluación el Responsable ACGII eleva un informe ejecutivo a la DGE sobre los resultados alcanzados.	Responsable ACGII	Progreso del documento (Flujo)
8	Revisa y aprueba informe ejecutivo.	DGE	Progreso del documento (Flujo)


Procedimiento de evaluación de seguridad informática externa a Entidades públicas
DGE
Responsable ACGII
Personal ACGII
INICIO
1
Elabora informe a la DGE acerca del alcance y modalidad de evaluación externa para su autorización.
2
Revisa y aprueba informe técnico, instruye proceder con la evaluación
3
Elabora instructivo de evaluación
4
Realiza la evaluación de seguridad informática de acuerdo a instructivo y registra vulnerabilidades en caso de identificar
¿Vulnerabilidades identificadas?
SI
NO
5
Revisa y valida vulnerabilidades identificadas
6
Elabora informe técnico de vulnerabilidades identificadas y registradas en la herramienta RTIR. En caso de no identificar ninguna vulnerabilidad informará las pruebas realzadas
7
Revisa, aprueba informe técnico. Trimestralmente eleva informe ejecutivo a la DGE sobre los resultados obtenidos.
8
Revisa, aprueba informe técnico ejecutivo
FIN