

	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-PD-09
		Fecha: 13/10/2026
	PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES	Versión: 1

LÍDER DE PROCESO
Jefe de la oficina asesora de planeación y tecnologías de la información.
1. OBJETIVO
Establecer los lineamientos y las actividades necesarias para identificar, analizar, priorizar, tratar y verificar de manera periódica las vulnerabilidades técnicas presentes en la infraestructura tecnológica, los sistemas de información y los servicios expuestos o por exponer a internet del IDARTES, con el fin de reducir la superficie de exposición y mitigar los riesgos y daños que se puedan causar a los activos de información de la Entidad.
2. ALCANCE
Inicia con la planificación del ciclo de gestión de vulnerabilidades y la definición del alcance de las evaluaciones o escaneos; continúa con la obtención de las autorizaciones requeridas, la configuración de las herramientas, la ejecución de los escaneos, el análisis y depuración de resultados, la validación de falsos positivos, la clasificación y priorización de los hallazgos, así como con la formulación e implementación de las acciones de remediación; y finaliza con la ejecución de los escaneos de verificación, la validación de las acciones implementadas, el cierre de los casos y la documentación de las lecciones aprendidas.
3. ÁREAS RESPONSABLES
120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN
4. GLOSARIO (TÉRMINOS Y DEFINICIONES ASOCIADOS)
- Activos tecnológicos: Recursos del sistema de información o relacionados con este, necesarios para que la Entidad funcione correctamente, como software, hardware, servicios, datos, personal, proveedores, instalaciones físicas, comunicaciones y equipamiento auxiliar. - Confidencialidad: Garantía de que la información sea accedida únicamente por usuarios y procesos autorizados. - Control: Medida que permite reducir el nivel de un riesgo específico o mantenerlo dentro de límites aceptables. Incluye políticas, procedimientos, prácticas y estructuras organizativas. - CVE – Common Vulnerabilities and Exposures: Identificador único y estandarizado asignado a una vulnerabilidad de seguridad conocida y divulgada públicamente. - CVSS – Common Vulnerability Scoring System: Sistema estándar de puntuación que permite valorar la severidad de una vulnerabilidad en una escala de 0.0 a 10.0, a partir de sus características de explotabilidad e impacto. - Disponibilidad: Garantía de que los usuarios y procesos autorizados tengan acceso a los activos de información cuando los requieran. - Escaneo de vulnerabilidades: Proceso automatizado mediante el cual se examinan los activos tecnológicos con el fin de identificar debilidades conocidas en sus sistemas operativos, servicios, aplicaciones y configuraciones. - Excepción o riesgo aceptado: Decisión formal y documentada de no remediar una vulnerabilidad dentro del plazo establecido, con base en una justificación técnica u operativa, la definición de controles compensatorios, un responsable y una fecha de reevaluación. - Exploit: Código, técnica o secuencia de comandos que aprovecha una vulnerabilidad para provocar un comportamiento no previsto en un sistema de información o recurso tecnológico. - Hardening o aseguramiento: Conjunto de actividades orientadas a reducir la superficie de exposición de un activo tecnológico mediante la eliminación de servicios y cuentas innecesarias, el ajuste de configuraciones y la aplicación de líneas base de seguridad. - Impacto: Daño producido a la Entidad por la materialización de un riesgo sobre los activos tecnológicos o de información. - Inventario de activos de información: Lista ordenada y documentada de los activos de información pertenecientes al IDARTES. - KEV – Known Exploited Vulnerabilities: Catálogo público de vulnerabilidades para las cuales existe evidencia confirmada de explotación activa. Se utiliza como criterio de priorización de la remediación. - Línea base de seguridad: Conjunto mínimo de configuraciones de seguridad definido por la Entidad para un tipo de activo tecnológico, contra el cual se compara su configuración real. - Parche o patch: Actualización publicada por el fabricante de un producto de software o hardware para corregir una vulnerabilidad, un defecto o una falla de funcionamiento. - Plan de remediación: Documento en el que se definen las acciones, los responsables, los recursos y los plazos requeridos para tratar las vulnerabilidades identificadas. - Pruebas de penetración o pentest: Ejercicio autorizado y controlado en el que se intenta explotar las vulnerabilidades identificadas, con el fin de determinar su explotabilidad real y su impacto. - Re-escaneo: Escaneo de verificación que se ejecuta sobre los activos intervenidos, con el fin de comprobar la efectividad de las medidas de remediación implementadas. - Remediación: Acción que elimina de manera definitiva una vulnerabilidad, generalmente mediante la aplicación de un parche, la actualización de una versión o el cambio de una configuración. - Riesgo: Probabilidad o posibilidad de que una amenaza, aprovechando una o varias vulnerabilidades de un sistema, equipo u otro tipo de activo, se concrete y cause daños, perjuicios o pérdidas a la Entidad. - Severidad: Nivel de criticidad asignado a una vulnerabilidad a partir de su puntuación CVSS: crítica, alta, media, baja o informativa. - Sistema de información: Conjunto de datos, aplicaciones y equipos que, de manera conjunta, proveen a la Entidad la información necesaria para la ejecución de sus tareas y la toma de decisiones. - Superficie de exposición o de ataque: Conjunto de puntos de un sistema, aplicación o red a través de los cuales un atacante podría intentar ingresar, extraer información o afectar el servicio. - Terceros: Personas jurídicas o naturales, como proveedores, contratistas o consultores, que proveen servicios o productos a la Entidad. - Vulnerabilidad: Debilidad, falla o deficiencia inherente a los activos de información que puede ser explotada por amenazas y que constituye una fuente de riesgo.
5. CONDICIONES ESPECIALES DE OPERACIÓN
- El procedimiento aplica a los servidores, estaciones de trabajo, dispositivos de red y de seguridad perimetral, bases de datos, sistemas de información, aplicaciones web, servicios en la nube y demás servicios expuestos o que se proyecten exponer a Internet, administrados directamente por IDARTES o por terceros en su nombre. - Toda actividad de escaneo de vulnerabilidades debe contar con autorización previa y escrita del Encargado de Seguridad de la Información de la Oficina Asesora de Planeación y Tecnologías de la Información y debe quedar registrada en la herramienta de mesa de servicios de TI. - Los escaneos se ejecutan fuera del horario laboral del IDARTES, con el fin de minimizar cualquier impacto sobre la disponibilidad de los sistemas. - Frecuencia mínima de escaneo: servicios expuestos a internet, Semestral; infraestructura interna crítica (servidores, bases de datos, dispositivos de red y de seguridad), anual; estaciones de trabajo, anual. Adicionalmente, se debe ejecutar un escaneo antes de la puesta en producción de un nuevo servicio o de un cambio mayor sobre uno existente. - Los informes de escaneo, la matriz GTI-F-27 y el formato GTI-F-28 diligenciados son información de acceso restringido; su consulta se limita al Encargado de Seguridad de la Información, a los Administradores de Tecnologías de la Información y al Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información. Su entrega a terceros requiere la firma previa de un acuerdo de confidencialidad. - No se ejecutan pruebas de explotación (exploits) ni pruebas de penetración sobre ambientes productivos sin autorización expresa y por escrito; cuando se requieran, se realizan preferiblemente sobre ambientes de pruebas equivalentes. - Los contratos y acuerdos con terceros que administren, desarrollen u alojen servicios del IDARTES deben incluir la obligación de atender la gestión de vulnerabilidades y de cumplir los plazos de remediación definidos en el presente procedimiento. - Cuando se identifique una vulnerabilidad crítica que esté siendo explotada activamente, o cuando existan indicios de compromiso de un activo, se debe activar de manera inmediata el procedimiento GTI-PD-02 Gestión de incidentes de seguridad de la información. - Las vulnerabilidades críticas identificadas sobre servicios expuestos a internet deben ser reportadas ante el Computer Security Incident Response Team CSIRT Centro, perteneciente a la Alta Consejería Distrital de TIC, cuando se determine que su explotación pudo afectar la información de la Entidad. - Para el correcto análisis y correlación de los resultados debe existir una única fuente de tiempo (sincronización de relojes) en la plataforma tecnológica de la Entidad.



 ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN		Código: GTI-PD-09
			Fecha: 13/10/2026
	PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES		Versión: 1

- Toda vulnerabilidad que no pueda ser remediada dentro del plazo definido debe tramitarse como excepción (riesgo aceptado) mediante el formato GTI-F-28 de excepción y aceptación de riesgo por vulnerabilidad no remediada, con la justificación técnica, los controles compensatorios implementados, el responsable y la fecha de reevaluación. La excepción aprobada se registra en la hoja Excepciones de la matriz GTI-F-27, se revisa como mínimo cada seis (6) meses y, a su vencimiento, la vulnerabilidad regresa a la actividad 10 o se tramita su prórroga con un nuevo formato GTI-F-28.
- Las fuentes de información para la identificación y priorización de vulnerabilidades son, entre otras: la base de datos CVE / NVD, el catálogo de vulnerabilidades explotadas conocidas (KEV), los boletines de seguridad de los fabricantes y las alertas emitidas por el ColCERT y por el CSIRT Gobierno.
- El presente procedimiento no reemplaza la gestión de incidentes de seguridad de la información; una vulnerabilidad no remediada que se materializa se gestiona como incidente.

Clasificación de la severidad de las vulnerabilidades

La clasificación de las vulnerabilidades identificadas se realiza con base en el puntaje CVSS v3.1 reportado por la herramienta de escaneo, ajustado según la criticidad del activo afectado, su nivel de exposición y la existencia de exploits públicos o de explotación activa:

Severidad: Crítica
Puntaje CVSS v3.1: 9.0 – 10.0
Descripción: Vulnerabilidad que permite la toma de control del activo, la ejecución remota de código o el acceso masivo a información, generalmente sin autenticación previa.
Plazo máximo de remediación: Siete (7) días calendario. Setenta y dos (72) horas cuando el activo esté expuesto a Internet o exista explotación activa.

Severidad: Alta
Puntaje CVSS v3.1: 7.0 – 8.9
Descripción: Vulnerabilidad que permite la escalada de privilegios, la afectación significativa de la disponibilidad o el acceso no autorizado a información sensible.
Plazo máximo de remediación: Quince (15) días calendario.

Severidad: Media
Puntaje CVSS v3.1: 4.0 – 6.9
Descripción: Vulnerabilidad cuya explotación requiere condiciones particulares, acceso previo o interacción del usuario, y cuyo impacto es limitado.
Plazo máximo de remediación: Treinta (30) días calendario.

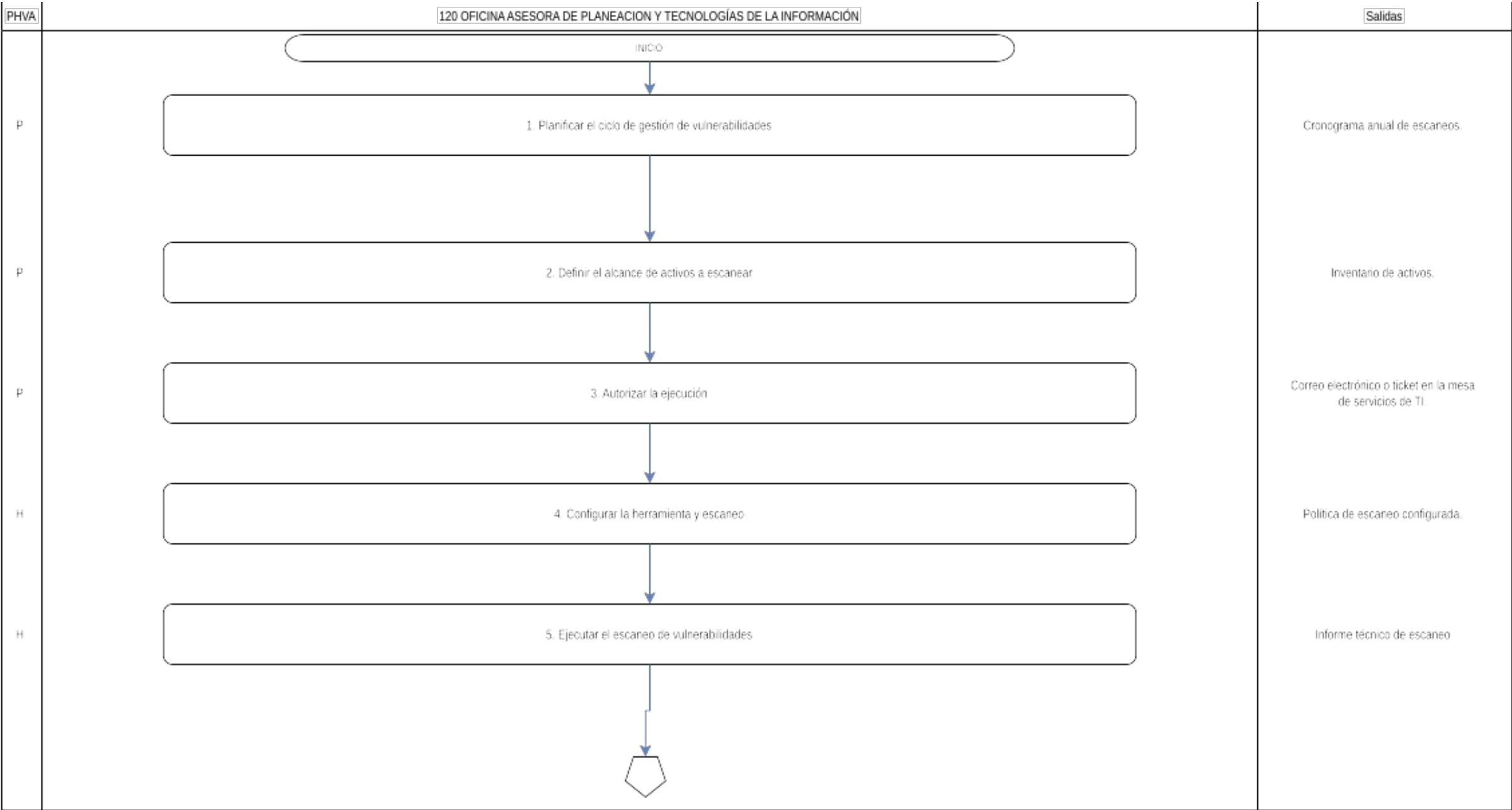
Severidad: Baja
Puntaje CVSS v3.1: 0.1 – 3.9
Descripción: Vulnerabilidad de impacto menor o de difícil explotación, asociada, por lo general, a debilidades de configuración o a divulgación de información no sensible.
Plazo máximo de remediación: Noventa (90) días calendario.

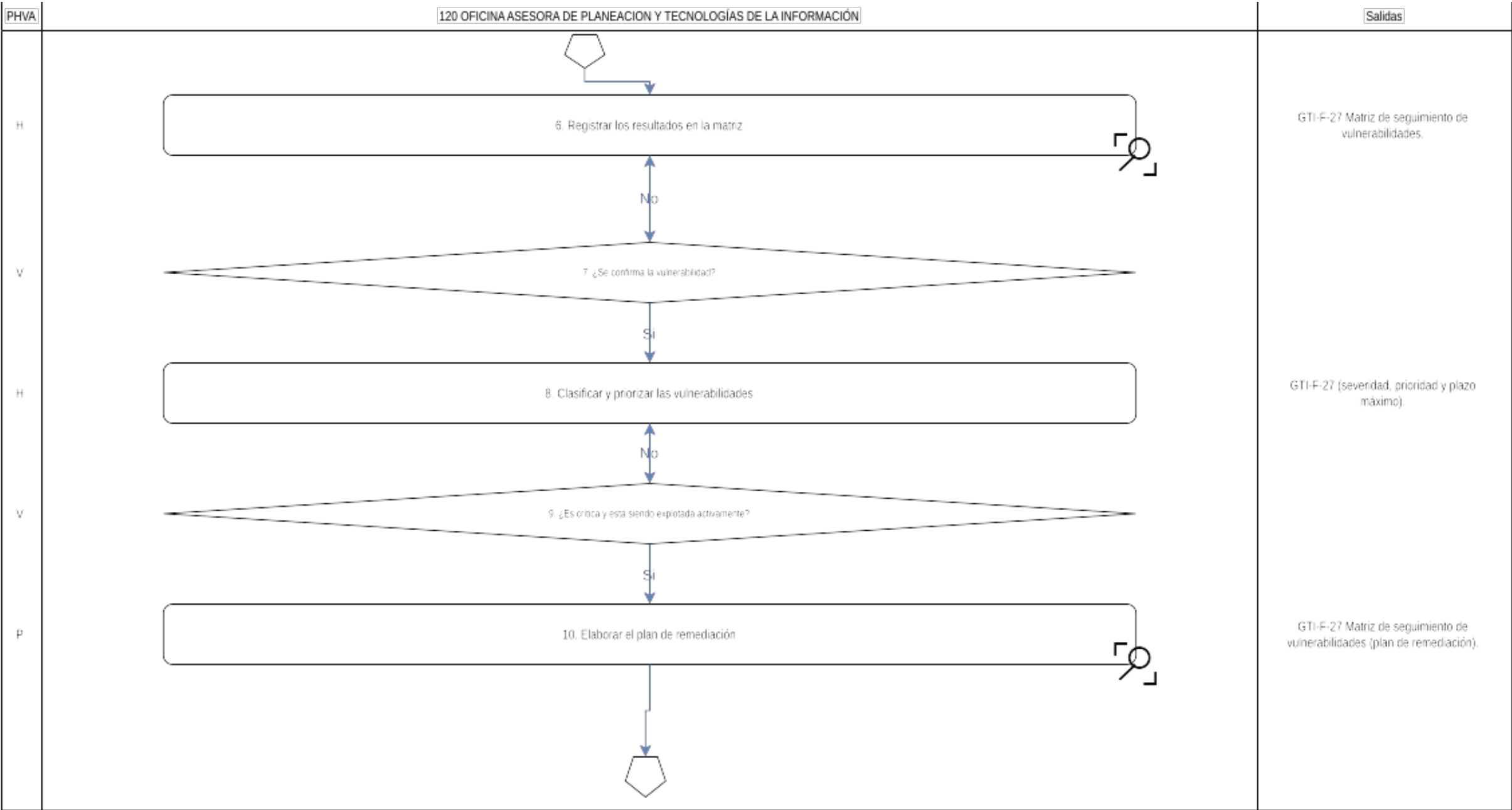
Severidad: Informativa
Puntaje CVSS v3.1: 0.0
Descripción: Hallazgo que no representa un riesgo directo, pero que aporta información útil sobre el activo y su configuración.
Plazo máximo de remediación: Se atiende en el siguiente ciclo de escaneo, según disponibilidad.

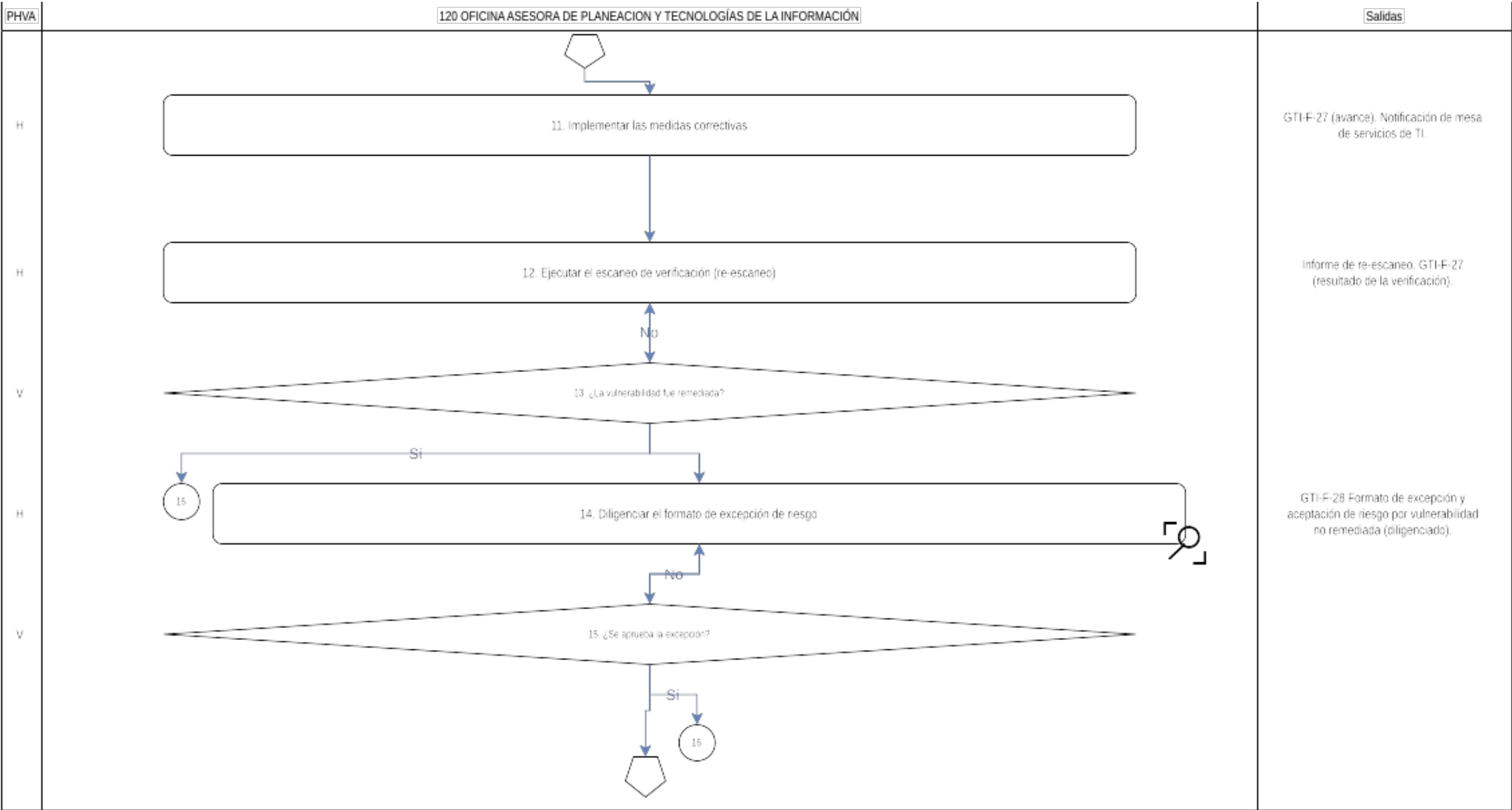
- El Encargado de Seguridad de la Información, con el administrador o responsable del activo, analiza si existe una alternativa técnica viable para remediar la vulnerabilidad dentro del plazo máximo establecido en el formato GTI-F-27.

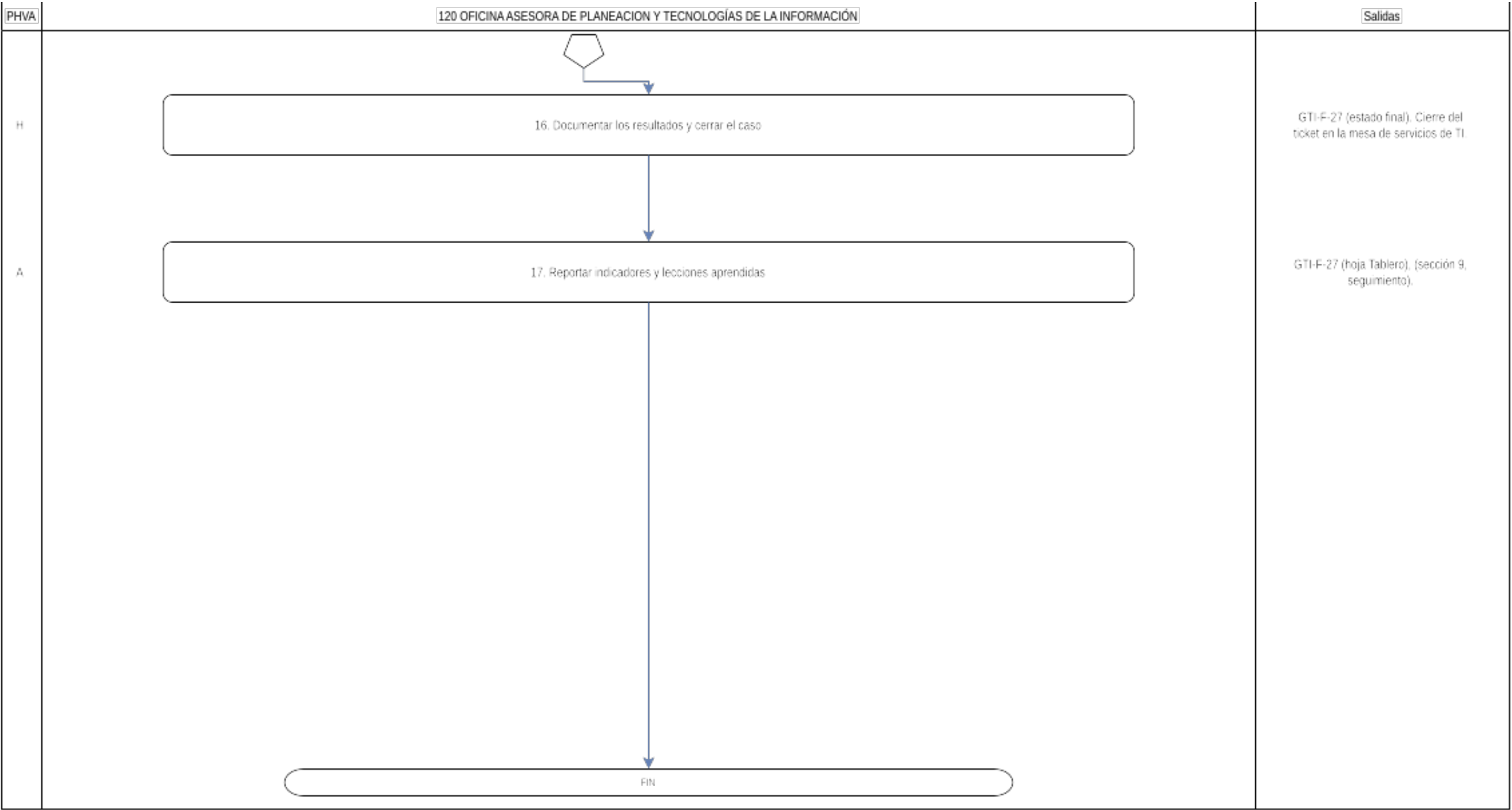
6. RELACIÓN CON OTROS PROCEDIMIENTOS Y PROCESOS				
Procesos que se requieren como proveedor	Que insumos requiero del proveedor	Procedimiento	Que se obtiene del procedimiento	Para quien va dirigido el servicio o producto
TODAS LAS ÁREAS	Inventario actualizado de activos de información y activos tecnológicos, autorización para la ejecución del escaneo, ventanas de mantenimiento e implementación de las medidas correctivas.	PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES	Identificación, priorización y remediación de las vulnerabilidades técnicas presentes en la plataforma tecnológica de la Entidad.	TODAS LAS ÁREAS Reducir la superficie de exposición de la plataforma tecnológica del IDARTES y mejorar continuamente los niveles de seguridad de la información, a partir de ciclos periódicos de identificación, tratamiento y verificación de las vulnerabilidades.
7. DIAGRAMA DE FLUJO				











8. DESCRIPCIÓN DE ACTIVIDADES						
No.	Ciclo PHVA	DESCRIPCIÓN DE ACTIVIDADES Y CONTROLES	RESPONSABLE	ACTORES	TIEMPO (DÍAS/HORAS)	DOCUMENTO / REGISTRO
1	P	Planificar el ciclo de gestión de vulnerabilidades Elaborar y presentar para aprobación el cronograma anual de escaneos, definiendo las frecuencias, los tipos de escaneo (interno / externo, autenticado / no autenticado), las herramientas y los responsables de cada ciclo.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	8 horas	Cronograma anual de escaneos.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN					Código: GTI-PD-09
						Fecha: 13/10/2026
	PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES					Versión: 1

2	P	Definir el alcance de activos a escanear Determinar los activos objeto del escaneo y recopila la información técnica requerida: direcciones IP, segmentos de red, nombres de host, rangos de puertos, URL, versiones y credenciales de escaneo, verificando su correspondencia con el inventario de activos de información.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	8 horas	Inventario de activos.
3	P	Autorizar la ejecución Otorgar la autorización formal para la ejecución del escaneo, acuerda la ventana de ejecución fuera del horario laboral y comunica la programación a los administradores de los servicios y a los terceros involucrados.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información. Proveedores de servicios TI	4 horas	Correo electrónico o ticket en la mesa de servicios de TI.
4	H	Configurar la herramienta y escaneo Configurar la herramienta de escaneo estableciendo el tipo de escaneo, los complementos de detección, los niveles de severidad, las credenciales, las exclusiones y la programación, ajustando las políticas a las necesidades y requisitos del IDARTES.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	4 horas	Política de escaneo configurada.
5	H	Ejecutar el escaneo de vulnerabilidades Ejecutar el escaneo dentro de la ventana autorizada, monitorea su progreso para verificar que se esté llevando a cabo correctamente y documenta cualquier incidencia o error presentado durante la ejecución.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	12 HORAS	Informe técnico de escaneo
6	H	Registrar los resultados en la matriz Registrar cada hallazgo en la hoja Matriz del formato GTI-F-27 Matriz de seguimiento de vulnerabilidades, lo valida técnicamente contra el activo afectado y descarta los falsos positivos, dejando la evidencia de la verificación en la columna de observaciones.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	24 HORAS	GTI-F-27 Matriz de seguimiento de vulnerabilidades.
7	V	¿Se confirma la vulnerabilidad? El Encargado de Seguridad de la Información verifica si el hallazgo corresponde a una vulnerabilidad real del activo evaluado. Si: Continúa en la actividad 8 No: Se devuelve a la actividad 6	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	4 horas	
8	H	Clasificar y priorizar las vulnerabilidades Registrar en la matriz GTI-F-27 el puntaje CVSS, la criticidad del activo, su exposición a internet y la existencia de exploit público o de explotación activa (KEV). Con estos datos la matriz calcula la severidad, la prioridad de atención y el plazo máximo de remediación de cada vulnerabilidad.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	12 horas	GTI-F-27 (severidad, prioridad y plazo máximo).
9	V	¿Es crítica y está siendo explotada activamente? El Encargado de Seguridad de la Información determina si la vulnerabilidad crítica está siendo explotada o si existen indicios de compromiso del activo. Si: Continúa en la actividad 10 No: Se devuelve a la actividad 8	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	2 horas	
10	P	Elaborar el plan de remediación Registrar en la matriz GTI-F-27, para cada vulnerabilidad priorizada, la acción a realizar, el tipo de acción, el área y el responsable de la remediación, cambia el estado a En remediación y comunica el plan a los administradores de los servicios y a los terceros mediante la mesa de servicios de TI.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	24 horas	GTI-F-27 Matriz de seguimiento de vulnerabilidades (plan de remediación).
11	H	Implementar las medidas correctivas Ejecutar las acciones definidas en el plan de remediación: aplicación de parches, actualización de versiones de software, aseguramiento (hardening) y ajuste de configuraciones, cierre de puertos y servicios innecesarios y demás controles requeridos, dentro de los plazos establecidos según la severidad, y reporta el porcentaje de avance en la matriz GTI-F-27.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Administradores de Tecnologías de la Información y proveedores de servicios de TI.	30 días	GTI-F-27 (avance). Notificación de mesa de servicios de TI.
12	H	Ejecutar el escaneo de verificación (re-escaneo) Ejecutar un nuevo escaneo sobre los activos intervenidos para comprobar la efectividad de las medidas implementadas, y registra en la matriz GTI-F-27 la fecha del re-escaneo y el resultado de la verificación.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	12 horas	Informe de re-escaneo. GTI-F-27 (resultado de la verificación).
13	V	¿La vulnerabilidad fue remediada? El Encargado de Seguridad de la Información revisa en la matriz GTI-F-27 el resultado del re-escaneo. Si: Continúa en la actividad 16 No: Se devuelve a la actividad 12	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	4 horas	
14	H	Diligenciar el formato de excepción de riesgo	120 OFICINA ASESORA DE PLANEACION	Administrador del activo, tercero responsable	5 días	GTI-F-28 Formato de excepción y aceptación de



 ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN				Código: GTI-PD-09
					Fecha: 13/10/2026
	PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES				Versión: 1

		Diligenciar las secciones 1 a 7 del formato GTI-F-28 de excepción y aceptación de riesgo por vulnerabilidad no remediada: identificación de la vulnerabilidad y de los activos afectados, justificación de la no remediación, análisis del riesgo residual, controles compensatorios implementados y plan de remediación definitiva.	Y TECNOLOGÍAS DE LA INFORMACIÓN	/ Encargado de Seguridad de la Información (concepto técnico)		riesgo por vulnerabilidad no remediada (diligenciado).
15	V	¿Se aprueba la excepción? El Líder de proceso revisa el formato GTI-F-28 y decide si acepta el riesgo residual; el Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información lo avala. Si: Continúa en la actividad 16 No: Se devuelve a la actividad 14	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Líder de proceso / Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información	3 días	
16	H	Documentar los resultados y cerrar el caso Verificar que la matriz GTI-F-27 esté completa, actualiza la línea base de seguridad de los activos intervenidos, adjunta al ticket la evidencia (informe de re-escaneo o formato GTI-F-27 firmado) y cierra el ticket en la mesa de servicios de TI.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	4 horas	GTI-F-27 (estado final). Cierre del ticket en la mesa de servicios de TI.
17	A	Reportar indicadores y lecciones aprendidas Consolidar y reportar los indicadores de la hoja Tablero de la matriz GTI-F-27 (vulnerabilidades por severidad, porcentaje de remediación dentro del plazo, tiempo promedio de remediación, vulnerabilidades recurrentes y excepciones vigentes), hace seguimiento a la vigencia de las excepciones en la sección 9 del formato GTI-F-27 y en la hoja Excepciones, y define las acciones de mejora para el siguiente ciclo.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de seguridad de la información	12 horas	GTI-F-27 (hoja Tablero), (sección 9, seguimiento).

9. POSIBLES PRODUCTOS O SERVICIOS NO CONFORME

ACTIVIDAD	PRODUCTO Y/O SERVICIO	CRITERIO DE ACEPTACIÓN	CORRECCIÓN	REGISTRO
6. Registrar los resultados en la matriz: Registrar cada hallazgo en la hoja Matriz del formato GTI-F-27 Matriz de seguimiento de vulnerabilidades, lo valida técnicamente contra el activo afectado y descarta los falsos positivos, dejando la evidencia de la verificación en la columna de observaciones.	GTI-F-27 Matriz de seguimiento de vulnerabilidades.	Calidad: La información registrada y actualizada en la matriz de seguimiento de vulnerabilidades Confiable: La información actualizada proporcionan la trazabilidad, la gestión y la gestión realizada.	Remediación de vulnerabilidades identificadas.	GTI-F-27 Matriz de seguimiento de vulnerabilidades.
10. Elaborar el plan de remediación: Registrar en la matriz GTI-F-27, para cada vulnerabilidad priorizada, la acción a realizar, el tipo de acción, el área y el responsable de la remediación, cambia el estado a En remediación y comunica el plan a los administradores de los servicios y a los terceros mediante la mesa de servicios de TI.	GTI-F-27 Matriz de seguimiento de vulnerabilidades (plan de remediación).	Calidad: La información registrada y actualizada en la matriz de seguimiento de vulnerabilidades Confiable: La información actualizada proporcionan la trazabilidad, la gestión y la gestión realizada.	Remediación de vulnerabilidades identificadas.	GTI-F-27 Matriz de seguimiento de vulnerabilidades.
14. Diligenciar el formato de excepción de riesgo: Diligenciar las secciones 1 a 7 del formato GTI-F-28 de excepción y aceptación de riesgo por vulnerabilidad no remediada: identificación de la vulnerabilidad y de los activos afectados, justificación de la no remediación, análisis del riesgo residual, controles compensatorios implementados y plan de remediación definitiva.	GTI-F-28 Formato de excepción y aceptación de riesgo por vulnerabilidad no remediada (diligenciado).	Calidad: La información registrada y actualizada en el formato de excepción justifica el riesgo asumido. Confiable: La información actualizada proporcionan la trazabilidad, la gestión y la gestión realizada.	Justificación del riesgo asumido.	GTI-F-28 Formato de excepción y aceptación de riesgo por vulnerabilidad no remediada.

10. DOCUMENTOS ASOCIADOS

Los documentos asociados del presente procedimiento se pueden acceder a través del mapa de procesos.

11. NORMATIVA ASOCIADA

Ver la normativa asociada, en el normograma de la entidad.

12. RECURSOS

Herramienta de escaneo de vulnerabilidades adquirida o dispuesta por la Entidad.
GLPI, aplicativo de la mesa de servicios de TI.
Encargado de Seguridad de la Información.
Administradores de Tecnologías de la Información.
Administradores de servicios de TI y terceros proveedores.

13. ANEXOS

No.	NOMBRE DEL ANEXO
-	Sin información.

||
||
||



 ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA RECREACIÓN Y DEPORTE Instituto Distrital de las Artes	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN		Código: GTI-PD-09
			Fecha: 13/10/2026
	PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES		Versión: 1

14. CONTROL DE CAMBIOS		
VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS

15. CONTROL DE APROBACIÓN			
ESTADO	FECHA	NOMBRE	CARGO
ELABORÓ	2026-10-12	MARYURY FORERO BOHORQUEZ	ENLACE MIPG
REVISÓ	2026-10-12	MARYURY FORERO BOHORQUEZ	REFERENTE MIPG
APROBÓ	2026-10-13	DANIEL SANCHEZ ROJAS	LIDER DE PROCESO
AVALÓ	2026-10-13	DANIEL SANCHEZ ROJAS	JEFE DE LA OFICINA ASESORA DE PLANEACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN

16. COLABORADORES	
NOMBRE	
JONATHAN GONZALEZ BOLANOS	
ANDRES FELIPE CUBILLOS GARCIA	