AGENCIA DE RENOVACIÓN DEL TERRITORIO	GESTIÓN DE VULNERABILIDADES TÉCNICAS	Código: PD-TI-10
	TECNOLOGÍAS DE LA INFORMACIÓN	Versión: 01
	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha de publicación: 04-03-2023

1. OBJETIVO GENERAL DEL PROCEDIMIENTO:	Realizar una adecuada gestión de vulnerabilidades técnicas que puedan presentarse en las tecnologías de la información que soportan la operación de la Agencia de Renovación del Territorio - ART, con el fin de identificar los controles pertinentes que permitan enfrentar las amenazas informáticas y mitigar los riesgos informáticos a los que se exponen los activos de información.
2. ALCANCE	Inicia con la identificación de las vulnerabilidades asociadas a los activos de información (infraestructura tecnológica, sistemas de información, aplicaciones, **dispositivos de seguridad** y servicios); seguido del análisis de los resultados obtenidos de la aplicación de los controles de mitigación; y finaliza con la entrega de un informe o reporte que determina la gestión del tratamiento realizado sobre las mismas. Aplica para todos los activos de información tecnológicos de la Entidad, colaboradores y terceros, cuando sea su responsabilidad sobre la aplicación de controles que hagan parte de rol de propietario o encargado de los activos mencionados.
3. DEFINICIONES	**Activo de información**: cualquier información o elemento relacionado con el tratamiento de esta (sistemas, hardware, software, sistemas de información, edificios, personas, imagen, etc.) que tenga valor para la Organización. **Control**: medida por la que se modifica el riesgo. [Fuente: ISO Guide 73:2009] Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguarda o contramedida también son utilizados como sinónimos de control. **Riesgo**: efecto en la incertidumbre de los objetivos [ISO/IEC 27000:2018]. Es la calificación de una amenaza desde el punto de vista de la probabilidad de ocurrencia y las consecuencias en caso de materializarse; se maneja con la siguiente fórmula: RIESGO = Probabilidad x Consecuencia. **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas [ISO/IEC 27000].
4. CONDICIONES GENERALES	**1. NORMATIVIDAD APLICABLE** Consultar normograma de la OTI **2. POLÍTICAS DE OPERACIÓN:** 2.1 Es responsabilidad de Seguridad de la Información gestionar las vulnerabilidades técnicas. 2.2 Es responsabilidad de todos los usuarios reportar a Seguridad de la Información las vulnerabilidades identificadas en los activos de información. 2.3 Es responsabilidad de los dueños o propietarios de los activos de información aplicar los controles definidos por Seguridad de la Información para la mitigación de las vulnerabildiades técnicas asociadas a los mismos. 2.4 Es responsabilidad de Seguridad de la Información realizar el seguimiento al tratamiento de las vulnerabilidades técnicas. 2.5 Para llevar acabalidad la gestión de vulnerabilidades técnicas es necesario disponer del inventario de activos de información (acttualizado) que hacen parte de la operación, con sus propietarios y características de los mismos [Ver inventario de activos de información]. 2.6 Se realiza la identificación o detección de las vulnerabilidades técnicas asociadas a los activos de información. Dicha detección puede darse por parte de los colaboradores o terceros de la ART, como de herramientas técnológicas implementadas para tal fin (monitoreo o análisis de vulnerabilidades). 2.7 Se analizan las vulnerabilidades técnicas asociadas a los activos de información y de identifican los controles pertinentes para la mitigación de las mismas. 2.8 Se define y documenta el plan de tratamiento de las vulnerabilidades técnicas identificadas en los activos de información con los controles respectivos, responsables de los mismos (propietarios), fechas de inicio y fin de la implementación. 2.9 Seguridad de la Información debe validar la aplicación del plan de tratamiento de las vulnerabilidades en su totalidad, dando su aprobación o no, conforme a las evidencias obtenidas.

5. DESCRIPCIÓN DEL PROCEDIMIENTO

No.	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE DE REALIZAR LA ACTIVIDAD	PUNTO DE CONTROL	REGISTRO
1	Detectar la vulnerabilidad	Se realiza la detección de la vulnerabilidad en los activos de información de manera manual o automática (herramientas de monitoreo o de análisis de vulnerabilidades).	Colaborador Tercero	No Aplica	Log de evento (aplica para detección automática de vulnerabilidades
2	Reportar la vulnerabilidad	Se realiza reporte de la vulnerabilidad por correo electrónico al Oficial de Seguridad de la Información.	Colaborador Tercero	No Aplica	Correo electrónico
3	Recibir el reporte de la vulnerabilidad	Se recibe el correo electrónico con el reporte de la vulnerabilidad por parte de los remitentes.	Seguridad de la Información	No Aplica	Correo electrónico con Formato de control de accesos debidamente diligenciado y firmado
4	Validar la existencia de la vulnerabilidad	Validar y aprobar la existencia de la vulnerabilidad en los activos de información asociados a la misma. ¿Existe la vulnerabilidad en los activos? Si: Registrar la vulnerabilidad y pasar a la actividad 5. No: Informar al solicitante y responable del activo la falsa alarma y no existencia de la vulnerabilidad.	Responsable del Activos de Información		Formato de control de vulnerabilidades técnicas
5	Identificar controles para la mitigación de las vulnerabilidades	Se realiza la identificación de controles para la mitigación de las vulnerabilides identificadas en los activos asociados.	Seguridad de la Información y Responsables de los activos de información	No Aplica	N.A.
6	Definir el plan de tratamiento de las vulnerabilidades	Se define y acuerda el plan de tratamiento de las vulnerabilidades técnicas identificadas en los activos de información.	Seguridad de la Información y Responsables de los activos de información	No Aplica	Plan de tratamiento de vulnerabilidades técnicas

7	Implementar el plan de tratamiento de las vulnerabilidades	Se realiza la implementación del plan de tratamiento de vulnerabilidades técnicas, aplicando los controles pertinentes sobre los activos de información en riesgo o afectados.	Responsables de los activos de información		Evidencias de implementación de controles
8	Informar de la implementación del plan de tratamiento de vulnerabilidades técnicas	Los responsables de los activos de información, informan por correo electrónico al Oficial de Seguridad de la Información sobre la terminación de la implementación del plan de tratamiento acordado, adjuntando las evidencias de la aplicación de los controles con las cuales se han mitigado las vulnerabilidades técnicas identificadas.	Responsable de gestionar la solicitud.	No Aplica	Correo electrónico
9	Verificar el cumplimiento del plan de tratamiento de vulnerabilidades	Se verifica el cumplimiento de la implementación del plan de tratamiento de vulnerabilidades técnicas con sus respectivas evidencias según sea el caso. ¿El plan se cumplió satisfactoriamente? SÍ: Registrar estado de cumplido en el formato de gestión de vulnerabilidades técnicas y continuar en la actividad 10. No: Notificar al responsable de los activos de información la novedad de incumplimiento y volver a la actividad 7	Seguridad de la Información		Plan de tratamiento de vulnerabilidades técnicas
10	Elaborar informe de resultados de gestión de vulnerabilides técnicas	Se revisa de manera general el tratamiento de las vulnerabilidades técnicas realizadas en el mes y se genera el informe respectivo con los resultados obtenidos sobre la mitigación de las vulnerabilidades identificadas.	Responsaltbe de Seguridad Informática Proveedor	No Aplica	Informe de gestión de vulnerabilidades ténicas
11	Fin.				

6. PRODUCTO O SERVICIO QUE SE ENTREGA	1. Registro de control de vulnerabilidades técnicas. 2. Plan de tratamiento de vulnerabilidades técnicas. 3. Informe de gestión de vulnerabilidades técnicas.
7. DOCUMENTOS ASOCIADOS	1. Caracterización del proceso. 2. Manual de políticas de seguridad de la información 3. Matriz de control, registro y seguimiento de vulnerabilidades ténicas 4. Plan de tratamiento de vulnerabilidades técnicas (documento confidencial)

VERSIÓN	**FECHA**	**DESCRIPCIÓN DE LOS CAMBIOS**
1	2/03/2023	Versión inicial del documento

Elaboró	**Revisó**	**Aprobó**
Nombre: Jorge Alberto Camargo - Yuli Andrea Parra Amaya Cargo: Contratistas, Oficina de Tecnologías de la Información Fecha: 28/02/2023	Nombre: Freddy Aguas Cargo: Jefe de Oficina Tecnologías de la Información (E) Fecha: 2/03/2023	Nombre: Freddy Aguas Cargo: Jefe de Oficina Tecnologías de la Información (E) Fecha: 2/03/2023