COLOMBIA POTENCIA DE LA VIDA	**PROCEDIMIENTO DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**			Agencia de Renovación del Territorio - ART
	TECNOLOGÍAS DE LA INFORMACIÓN			
	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	**Código: PD-TI-05**	**Versión: 03**	**Fecha de publicación: 27-03-2024**

1. OBJETIVO GENERAL DEL PROCEDIMIENTO:	Establecer las actividades para la gestión y clasificación de los incidentes de seguridad y privacidad de la información que se presenten en la Agencia de Renovación del Territorio – ART, con el fin de mitigar, comunicar, gestionar e implementar acciones correctivas y de mejora sobre los eventos e incidentes la confidencialidad, integridad, disponibilidad de los activos de información de la Entidad.
2. ALCANCE	Este procedimiento aplica a todos los activos de información que hacen parte de la operación de la Agencia y a todos los Colaboradores y Terceros cuando sea el caso que tienen acceso a los mismos. Aplica para todos los eventos e incidentes que se presenten en la Agencia de Renovación del Territorio.
3. DEFINICIONES	Las definiciones utilizadas en este procedimiento se encuentran en el documento "Glosario de Seguridad y Privacidad de la Información" Activo de Información Amenaza Análisis de riesgos Confidencialidad Contratista Contro Copias de Seguridad Custodio de activo de información Disponibilidad Evento de seguridad de la información Gestión de incidentes de seguridad de la información Guía Incidente de seguridad Impacto
4. CONDICIONES GENERALES	**1. NORMATIVIDAD APLICABLE** **1.1** Decreto Único Reglamentario 1078 de 2015 Nivel Nacional, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". 1.2 Norma Técnica Colombiana NTC/ISO 27001 versión 2013, Sistemas de Gestión de Seguridad de la Información (SGSI) **2. POLÍTICAS DE OPERACIÓN** 2.1 Todos los Colaboradores y Terceros que tengan algún vínculo contractual o de convenio con la ART, son responsables de reportar los eventos o incidentes que se presenten en los activos de información de la Entidad que se encuentren a su alcance. 2.2 El reporte de eventos o incidentes debe realizarse de acuerdo a los formatos vigentes en la ART. 2.3 Los eventos o incidentes deben ser reportados a la mesa de servicio mediante los canales o puntos de contacto oficializados en la ART. 2.4 Todos los incidentes de seguridad de la información de alto impacto deben ser reportados a las autoridades competentes de acuerdo con los lineamientos emitidos por MinTIC. 2.5 Todos los eventos e incidentes de seguridad deben quedar registrados en el formato: "FM-TI-20 Formato de Gestion Incidentes de Seguridad". 2.6 Todos los incidentes de seguridad de la información deben ser documentados en el formato: FM-TI-14 Formato informe de incidentes de seguridad de la información".

5. DESCRIPCIÓN DEL PROCEDIMIENTO

No.	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE DE REALIZAR LA ACTIVIDAD	PUNTO DE CONTROL	REGISTRO
1.	Reportar el evento o incidente de seguridad de la información a través de la Mesa de ayuda.	Los usuarios que detecten o sospechen de la presencia de un evento o incidente de seguridad de la información reportan a la Oficina de Tecnologías de la Información para su registro y gestión.	Usuario final	No aplica	Numero de solicitud abierta en el sistema de Mesa de Ayuda
2	Registrar y escalar en la herramienta establecida el evento o incidente reportado o identificado en los sitemas de monitoreo y detección de la infraestructura tecnologica.	La Oficina de Tecnologías de la Información detecta en los sistemas de protección, prevención, control y monitoreo de la Agencia amenazas y vulnerabilidades sobre la confidencialidad, la integridad y la disponibilidad de la información, estableciendo un posible incidente de seguridad.	Oficina de Tecnologías de la Informaciónmático	No aplica	Numero de solicitud abierta en el sistema de Mesa de Ayuda
3	Recolectar evidencia del posible incidente de seguridad	Toma la evidencia documental, registro fotografico, logs de los dispositivos de control, seguridad, prevención y detección, y dispositivos forenses(si la Agenica los tiene).por parte de Oficina de Tecnologías de la Información.	Oficina de Tecnologías de la Información Responsable de Seguridad de la Información	No aplica	Registro de evidencias
4	Analizar las Evidencias	Analiza los datos obtenidos, donde se descarta o se afirma un incidente de seguridad.si se descarta un incidente de seguridad, se procede por parte de la Oficina de Tecnologías de la Información a realizar un soporte de mesa de ayuda de acuerdo con el procedimiento "Soporte técnico a usuario final".	Responsable de Seguridad de la Información	No aplica	Evidencias recolectadas cuando es el caso
5	Evaluar el impacto	Evaluan si se puede dar solución al incidente de acuerdo con lo establecido en el procedimiento de "Soporte técnico a usuario final"y pasa a la actividad N°15. Sino se puede dar solución, se evalua que tipo de incidente es el que se presenta, a que recursos o activos de información está afectando, cual es alcance del mismo, que pronóstico tiene de expansión, así como los daños potenciales o reales que se generen.	Oficina de Tecnologías de la Información	✓	Numero de solicitud abierta en el sistema de Mesa de Ayuda
6	Identificar el nivel del incidente	Se identifica el nivel de afectación del incidente de acuerdo a los Niveles de Criticidad del Incidente descritos en la "Guía de Gestión de incidentes de seguridad de la información".	Oficina de Tecnologías de la Información	No aplica	Numero de solicitud abierta en el sistema de Mesa de Ayuda
7	Escalar el incidente	Para buscar una solución al incidente se tiene en cuenta los niveles de escalamientos definidos en la "Guía de gestión de incidentes de seguridad de la información".	Oficina de Tecnologías de la Información	No aplica	Numero de solicitud abierta en el sistema de Mesa de Ayuda
8	Recibir evento o incidente y realizar evlauación.	Realiza análisis del reporte para establecer si es un evento o incidente e iniciar su atención, de acuerdo con las actividades y evidencias reportadas.	Responsable de Seguridad de la Información	No aplica	Numero de solicitud abierta en el sistema de Mesa de Ayuda Informe borrador de eventos o incidentes
9	Establecer las actividades y recomendaciones pertinentes	Definen las estrategias de contención e identifican las fuentes de ataque de ser necesario. Si es un evento finaliza el procedimiento. Si es un incidente continua en la actividad 10.	Gestor TI- Oficina de Tecnologías de la Información	No aplica	Informe borrador de eventos o incidentes
10	Comunicar a las partes interesadas que evento o incidente ha sido solucionado.	Reporta a las partes interesadas los resultados obtenidos y las acciones a seguir.	Responsable de Seguridad de la Información	No aplica	Correo electrónico
11	Informar a las autoridades	Informa a nivel interno y externo a entes como el COLCERT (Grupo de Emergencias Ciberneticas de Colombia), CSIRT de Gobierno y CSIRT PONAL(Equipo de Respuesta ante Incidencias de Seguridad Informática de la Policia Nacional) quienes apoyaran la estrategia de contención, apoyaran la identificacion de fuentes de ataque, y propondran las estrategias de erradicación.	Responsable de Seguridad de la Información Oficina de Tecnologías de la Información	No aplica	Correo electrónico Formatos establecidos por cada Entidad para reporte de los incidentes.
12	Iniciar la estrategia de Contención	Inicia con las actividades para contener el incidente de seguridad y restablecer el servicio.	Responsable de Seguridad de la Información Oficina de Tecnologías de la Información	No aplica	Informe borrador de eventos o incidentes
13	Identificar las fuentes de ataque	El respobale de seguridad de la información en conjunto con los profesionales de la Oficina de Tecnologías de la Información, identifican los tipos de incidentes de acuerdo con lo descrito en la "Guía de gestión de incidentes de seguridad".	Responsable de Seguridad de la Información Oficina de Tecnologías de la Información	No aplica	Informe borrador de eventos o incidentes
14	Establecer la estrategia de Erradicación	Se definen las estrategias de erradicación dependiendo de los factores descritos en la" Guía de gestión de incidentes de seguridad de la información.	Responsable de Seguridad de la Información Oficina de Tecnologías de la Información	No aplica	Informe de Evento o Incidentes.
15	Aplicar los procedimientos de Recuperación si es necesario	En caso de ser necesario se activa el plan de continuidad operativa de acuerdo con lo establecido en el procedimiento "Continuidad operativa".	Responsable de Seguridad de la Información	No aplica	Plan de continuidad operativa

16	Informar al usuario/s afectados	A través de la aplicación de Mesa de ayuda o del correo electronico, la Oficina de Tecnologías de la Información le informa al usuario/s, el reestablecimiento de los recursos tecnologicos afectados y de la normalidad en la operación.	Oficina de Tecnologías de la Información	No aplica	Correo electrónico
17	Documentar evento o incidente de seguridad de Información.	La Mesa de Servicios y el equipo de Seguridad de la Información documentan las soluciones desarrolladas para controlar el incidente de seguridad y la respectiva mitigación de la amenaza.	Equipo de Seguridad de la información Mesa de Servicio	No aplica	Bitacora de incidentes de seguridad.
18	Reportar a las partes interesadas para la aplicación de las acciones.	Se reportan los resultados obtenidos y las acciones a implementar por cada una de las partes interesadas.	Responsable de Seguridad de la Información	No aplica	Informe de Evento o Incidentes.
19	Documentar las lecciones aprendidas.	El responsable de seguridad documenta las lecciones aprendidas en el informe.	Responsable de Seguridad de la Información	No aplica	Informe de Evento o Incidentes.
20	Cierre del incidente	Se realiza cierre del incidente y de los requerimientos solicitados con respecto al incidente, o de cierre requerimiento de mesa de ayuda .	Responsable de Seguridad de la Información Partes interesadas	No aplica	Informe de evento o incidentes.

6. PRODUCTO O SERVICIO QUE SE ENTREGA	Atención oportuna a incidentes de seguridad de la información.
7. DOCUMENTOS ASOCIADOS	1. Caracterización del proceso. 2. Manual de politicas de seguridad de la información 3. Procedimiento "Soporte Técnico a usuario final" 4. Procedimiento para la Continuidad operativa 5. Plan de continuidad operativa (Documento confidencial) 3. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. 4. Mapa de riesgos del proceso

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LOS CAMBIOS
1	15/09/2021	Versión inicial del documento
2	30/11/2022	En la columna rsponsables se cambio el GIT de soporte a Oficina de Tecnologías de la Información y la entrada de la nueva guía de gestión y clasificación de incidentes.
3	13/03/2024	Ajustes en la sección de definiciones para hacer referencia al Glosario general Ajustes generales en los pasos a seguir en el procedimiento

Elaboró	Revisó	Aprobó
Nombre: Yuli Andrea Parra Amaya Cargo: Contratista, Oficina de Tecnologías de la Información Fecha: 10/12/2022	Nombre: Freddy Alejando Aguas Barbosa Cargo: Jefe Oficina de Tecnologías de la Información Fecha: 14/12/2023	Nombre: Freddy Alejando Aguas Barbosa Cargo: Jefe Oficina de Tecnologías de la Información Fecha: 13-03-2024