1. OBJETIVO

Registrar los Logs eventos sobre las operaciones que se realizan en los sistemas de información y sistemas operativos, con el objeto de realizar monitoreo de los servicios informáticos que presta la entidad.

2. ALCANCE

El presente documento aplica para todos los sistemas operativos y sistemas de información que tengan sistema de auditoría o Logs de eventos, alojados en la plataforma tecnológica de la entidad.

3. TÉRMINOS Y DEFINICIONES

Log: registro de eventos presentados en los Sistemas de Información y/o dispositivos que permitan tener trazabilidad sobre las acciones que son ejecutadas por sistemas, por usuarios en las bases de datos y dispositivos.

Administración de Log: proceso mediante el cual se realiza la generación, transmisión, almacenamiento, análisis, monitoreo y reporte de los Logs.

Análisis de Log: estudio de los Logs para identificar eventos de interés o suprimir entradas de eventos insignificantes.

Monitoreo de Logs: supervisan la actividad de la red, inspeccionan los eventos del sistema y almacenan diferentes acciones (por ejemplo, cambiar el nombre de un archivo o abrir una aplicación) que ocurren dentro de los sistemas vigilados, contando con la capacidad de consolidar aquellos datos que podrían alertarte sobre una violación de políticas de seguridad.

Evento: una alerta o notificación creada por algún componente de la plataforma tecnológica de la información o herramienta de monitoreo.

Evidencia digital: información con valor probatorio almacenada o transmitida en forma digital.

Incidente: es un evento o serie de eventos de seguridad de la información no deseado o no planeado, que afecte la prestación del servicio o reduzca la calidad de la prestación del servicio o que tenga una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información

Retención de Log: archivar los Logs de eventos como parte de las actividades de administración de la infraestructura de acuerdo a las políticas de respaldo y recuperación de los mismos.

Rotación de Log: proceso que consiste en la eliminación de un registro de logs con el objetivo de permitir la apertura de uno nuevo de acuerdo con la frecuencia de almacenamiento que se tenga establecida y con las políticas de seguridad de almacenamiento.

Activo de información: es todo aquello que posea valor para la organización. ej.: la información física y digital; el software; el hardware; los servicios de información, de comunicaciones, de almacenamiento; las personas, entre otros.

Recurso de Información: término con el cual se designan las aplicaciones y datos que hacen posible el desarrollo.

4. RESPONSABLES

- **Jefe División de Planeación y Sistemas**: es responsable del cumplimiento del procedimiento.
- **Administradores de TI**: es responsables de la administración y gestión de los sistemas de información y servidores supervisar el establecimiento y actualización de los lineamientos, garantizando el cumplimiento del procedimiento.

5. CONDICIONES GENERALES

A. Contar con registros de auditoría y Logs de eventos, permitiría a la entidad poder realizar investigaciones informáticas forenses, cumplir con regulaciones, verificar eventos de seguridad entre otros.

B. Se deben definir actividades que permitan contar con estos rastros de auditoría y controlar su almacenamiento.

C. Activación de logs.

D. Todos los sistemas de información, aplicativos, sistemas operacionales, bases de datos, dispositivos de comunicación, dispositivos de seguridad y servidores, deben contar con los logs o rastros de auditoría que registren las actividades de los usuarios, las excepciones, las fallas y eventos de seguridad.

E. Es responsabilidad de los administradores de TI, estar pendientes de la activación de los logs de auditoría.

F. El encargado del aplicativo debe mantener un inventario de los registros de auditoria existentes por aplicación y su ubicación.

G. Verificación de eventos.

H. Se debe elaborar, conservar y revisar periódicamente los registros acerca de las actividades de los usuarios, excepciones, fallas, y eventos de seguridad de la información.

I. Es responsabilidad de los líderes técnicos de infraestructura y sistemas de información, proveer la información de eventos solicitada por los usuarios.

J. Configurar la rotación de Logs automáticamente en la herramienta del sistema operativo o sistema de información.

6. DESCRIPCIÓN DE ACTIVIDADES

No.	Descripción de la Actividad	Responsables o Rol	Registros
1	**Activación de Logs** Activar el registro de logs y auditorías de los componentes de la plataforma tecnológica para que reporten los eventos cuando aplique. Llevar inventario de logs por aplicativo	Administradores de TI	Inventario de logs y registros de auditoría RT-Fr06 Formato Registro Copias de Seguridad Anual
2	**Verificar los Eventos** Realizar verificación de eventos e informar anomalías que se encuentren en la reunión de control de cambios	Jefe División Planeación y Sistemas Administradores de TI	Acta de Control de Cambios

7. PUNTOS DE CONTROL

Realizar seguimiento y verificación del diligenciamiento del formato RT-Fr06 Formato Registro Copias de Seguridad Anual. Actividad No.1.

8. BASE LEGAL

ISO/IEC 27001: 2013 Estándar Internacional para la seguridad de la información

9. ANEXOS

N.A

10. FORMATOS

RT-Fr06 Formato Registro Copias de Seguridad Anual

11. DOCUMENTOS RELACIONADOS

N.A

12. CONTROL DE CAMBIOS

Control de Cambios

- Ver. 001// Rev. 1// FV. 22 de noviembre de 2021

  Cambios:

  Se solicita la creación del presente procedimiento, con el fin de registrar los Logs eventos sobre las operaciones que se realizan en los sistemas de información y sistemas operativos, con el objeto de realizar monitoreo de los servicios informáticos que presta la entidad.

Justificación:

Responsable: Mary Alexandra Rodriguez Bernal

Fecha: 2021-11-24

ELABORÓ	REVISÓ	APROBÓ
Nombre: Aldair Suarez	Nombre: Diana Rocío Plata Arango	Nombre: Grupo Evaluador de Documentos
Cargo: Profesional Universitario	Cargo: Jefe División de Planeación y Sistemas	No. Acta y Fecha: Acta No. 31 del 22/11/2021.