AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

GUÍA DE GESTIÓN DE LOGS DE AUDITORÍA

BOGOTÁ D.C. JUNIO DE 2021

TABLA DE CONTENIDO

1. OBJETIVO

Esta guía tiene como objetivo, dar a conocer las directrices en la gestión de logs de auditoría de los servicios tecnológicos de la ARN.

2. ALCANCE

Aplica para toda la infraestructura tecnológica de la ARN que cuente con registro de logs incluyendo sistemas de información o aplicativos.

3. DEFINICIONES

ADMINISTRACIÓN DE LOG: Proceso mediante el cual se realiza la creación, transmisión, almacenamiento, análisis, monitoreo y reporte de los Logs.
ANÁLISIS DE LOG: Estudio de los Logs para determinan si se han presentado eventos de alto impacto o se requiere suprimir entradas de eventos de bajo impacto.
EVENTO: Es una alerta o notificación creada por algún elemento de la arquitectura tecnológica de la información o por herramientas de monitoreo.
EVIDENCIA DIGITAL: Información que contiene valor probatorio almacenada o transmitida de forma digital.
INCIDENTE: Es un evento o conjunto de eventos de seguridad de la información, que afectan o reducen la calidad de la prestación del servicio y tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
LOG: Registro de los eventos que ocurren en los sistemas informáticos cuando un usuario o proceso se encuentran activos y se produce un evento el cual genera un rastro de lo ocurrido.
RETENCIÓN DE LOG: proceso que consiste en guardar los logs de eventos como parte de la administración de la infraestructura de acuerdo con políticas de respaldo y recuperación.
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.

4. CONDICIONES GENERALES

Se deben precisar acciones que permitan el registro y almacenamiento de logs con el fin de controlar su integridad, confidencialidad, disponibilidad y su seguridad durante el almacenamiento.

La auditoría de logs es una herramienta sistemática independiente, objetiva y documentada que permite obtener información sobre el cumplimiento de los objetivos de toda la infraestructura tecnológica de la entidad.

5. RESPONSABLE

La Oficina de Tecnologías de la Información, delega en cada líder funcional o líder técnico de los servicios tecnológicos, la parametrización de las herramientas de recolección de logs para respaldo de las auditorias.

La Oficina de Tecnologías de la Información de la ARN será la responsable de autorizar los permisos de acceso a las herramientas que se utilizan para la recolección de logs.

6. FASES DE LA AUDITORIA DE LOGS

6.1 PLANEACIÓN DE LA AUDITORÍA DE LOGS

Las auditorías de logs se deben realizar periódicamente de acuerdo con las necesidades de la Entidad, para ello se requiere determinar los recursos financieros, humanos y físicos, y los procesos teniendo en cuenta los cambios en el entorno de la infraestructura tecnológica, los controles internos que se tengan para evaluar, guardar y analizar los logs.

6.2 IMPLEMENTACIÓN DE LA AUDITORÍA

Consiste en configurar los módulos de auditoria en los diferentes servicios de la infraestructura tecnológica, sistemas de información o aplicativos.

En esta fase se procede a realizar la recolección de la información de todos los eventos que son registrados a través de cada sistema, aplicación o servicio de TI.

6.2.1 ACTIVACIÓN DE LOGS.

En los sistemas de información de la entidad como son: aplicativos, sistemas operativos, bases de datos, hardware de comunicación, infraestructura de seguridad y servidores, entre otros, se requiere realizar la activación de los logs para llevar la trazabilidad de todos los eventos que suceden en el trascurso de su procesamiento de información, lo cual genera un registro de todas las actividades de la infraestructura, usuarios, excepciones, fallas y eventos de seguridad de información que presenten.

Los responsables de los aplicativos y manejo de los servidores o equipos de infraestructura tecnológica de la entidad deben mantener un inventario de todos los registros de auditoria de logs existentes por su aplicación, servidor o hardware de infraestructura con su respectiva ubicación.

6.2.2 DESCRIPTORES DE LOGS PARA LOS SISTEMAS DE INFORMACIÓN SIRR-SARA Y ARPA

Dentro de los sistemas de información misionales de la ARN se pueden identificar los siguientes descriptores de logs teniendo en cuenta el estándar ISO 27002: 2015

a. Identificación (ID) de usuario.
b. Actividades del sistema.
c. Fechas, tiempos y detalles de eventos clave.
d. Registro de transacciones ejecutadas por usuarios en las aplicaciones.

6.3 EJECUCIÓN DE LA AUDITORÍA

Una vez configurado el módulo de auditoría y según la programación de Jobs se realiza la recolección de eventos. El administrador funcional debe hacer revisión periódica de los logs para hacer depuración y análisis de los eventos presentados.

6.3.1 VERIFICACIÓN DE EVENTOS

Se deben crear, guardar y analizar durante periodos establecidos los registros acerca de las actividades de los usuarios, transaccionalidad, servidores, excepciones, y eventos de seguridad de la información.

Es responsabilidad de los dueños de los procesos involucrados y propietarios de la información, solicitar, verificar y conocer cuales eventos han ocurrido sobre los sistemas informáticos que tratan la información de la entidad.

Es responsabilidad de los administradores de la infraestructura tecnología y de los administradores de los sistemas de información, entregar la información de eventos solicitada por los dueños de los procesos o dueños de la información cuando sea solicitada.

6.4 MONITOREO DE LA AUDITORÍA

El monitoreo de la auditoria es la última fase en la cual se revisarán todos los objetivos trazados, en donde se analizarán todas las actividades que se cumplieron y las que no se alcanzaron.

Los resultados obtenidos están encaminados a proponer las acciones de mejora necesarias y la toma de decisiones.

Estas revisiones se deben realizar de forma permanente para contar con un seguimiento adecuado.

7. MEDIR EL DESEMPEÑO DE AUDITORÍA DE LOGS

- Evaluar la función de auditorías de logs.
- Identificar acciones de mejoramiento.
- Identificar las necesidades de entrenamiento.

8. RESPALDO Y RESTAURACIÓN DE ARCHIVOS DE AUDITORÍA

Es responsabilidad de los administradores de la infraestructura y de los administradores de los sistemas de información implementar un plan para el respaldo de logs de auditoría teniendo en cuenta todos los componentes con los que cuenta la arquitectura tecnológica de la entidad.

Se deben crear políticas de seguridad de la información estableciendo directrices de conservación, copiado y restablecimiento de los logs y los registros de auditorías de toda la infraestructura de la plataforma tecnológica cuando sea necesario, esto con el fin de asegurar que se cuenta con evidencia ante algún incidente de seguridad.

Como política final para la disposición de respaldo y restauración se debe aplicar un borrado seguro de los logs obsoletos, por cumplimiento del tiempo de retención el cual puede programarse de forma automática.