Superintendencia de Sociedades

PROCEDIMIENTO DE GESTIÓN DE LOGS Y REGISTROS DE AUDITORÍA

1. INFORMACIÓN GENERAL.

1.1.	**OBJETIVO**	Registrar eventos y generar trazabilidad sobre las operaciones que se realizan en los sistemas de información y sistemas operativos, con el objeto de realizar monitoreo de los servicios informáticos.
1.2.	**RESPONSABLE**	Coordinador del Grupo de Sistemas y Arquitectura de Tecnología o quien este encargue.
1.3.	**ALCANCE**	Aplica para el acceso a la plataforma tecnológica que cuenten con Sistemas operativos, o Dispositivos de red o dispositivos de seguridad de propiedad de la Superintendencia de Sociedades**.**
1.4.	**DEFINICIONES**	**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. **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. **Log:** Es el registro de las acciones y de los acontecimientos que ocurren en un sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar. Rastro de lo que se está ejecutando sobre la plataforma tecnológica.

	Recurso de Información: Término con el cual se designan las aplicaciones y datos que hacen posible el desarrollo del negocio de la Superintendencia de Sociedades. **Retención de Log:** Archivar los logs de eventos como parte de las actividades de administración de la infraestructura de acuerdo con las políticas de respaldo y recuperación de los mismos. **Rotación de Log:** Cerrar un registro de log y abrir uno nuevo de acuerdo con un periodo establecido o teniendo en cuenta la capacidad de almacenamiento disponible en el servidor (local o remoto).

2. CONDICIONES GENERALES

Contar con rastros de auditoría permite a la entidad llevar a cabo investigaciones especiales, garantizar el cumplimiento de normativas y verificar eventos de seguridad, entre otros aspectos. Para ello, es fundamental definir actividades que aseguren la generación, conservación y gestión adecuada de estos registros.

Con el fin de monitorear y alertar sobre posibles ataques informáticos y riesgos de ciberseguridad, es imprescindible activar los logs de auditoría en la infraestructura tecnológica. Esta medida es esencial para la protección de los sistemas y debe implementarse conforme a los lineamientos del dominio de Arquitectura de Seguridad, establecidos en la Arquitectura Empresarial V3.

2.1. Activación de logs.

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

Los Coordinadores de la Dirección de Tecnología de la Información y las Comunicaciones son responsables de supervisar la activación de los logs de auditoría en las plataformas tecnológicas y sistemas de información a su cargo.

En los proyectos de desarrollo de sistemas, se debe cumplir con el modelo 2.19 *Modelo de Gestión de Rastros de Auditoría* para la correcta generación de archivos de auditoría (*logs*).

Además, debe mantenerse un inventario actualizado de los registros de auditoría existentes en las plataformas tecnológicas y sistemas de información, incluyendo su nombre y ubicación.

2.2. Verificación de eventos.

En caso de presentarse incidentes o eventos que generen indisponibilidad de las plataformas tecnológicas y sistemas de información se deben revisar los registros acerca de las actividades de los usuarios, excepciones, fallas, y eventos de seguridad de la información.

Si existe una herramienta de monitoreo y alertamiento, es responsabilidad de los líderes técnicos de infraestructura y sistemas de información, estar atentos a los eventos de seguridad que se alerten y establecer las correcciones requeridas.

2.3. Respaldo y restauración de archivos de auditoria.

Es responsabilidad de los líderes técnicos de las diferentes Coordinaciones de la Dirección de Tecnología de la Información y las Comunicaciones coordinar el plan de respaldo de información que incluya los logs de auditoria por medio de la herramienta con que se cuente.

En caso de contar con un Centro de operaciones de seguridad (SOC), se deben establecer directrices de retención, respaldo y recuperación de los logs y registros de auditorias de los componentes de la plataforma tecnológica.

El Coordinador de Seguridad e Informática Forense debe coordinar con el SOC las directrices de retención, respaldo y recuperación, y cuando estas se cumplan, aplicar un backup histórico y realizar el borrado en las plataformas tecnológicas y sistemas de información, de los registros de logs consolidados en el backup histórico.

2.4. Parametrización de herramientas utilizada para el monitoreo y alertamiento.

En caso de contar con un Centro de operaciones de seguridad (SOC), el Coordinador de Seguridad e Informática Forense será el responsable de la definición de los logs que ingresaran al sistema de monitoreo (SIEM Security Information Event Management) y el Coordinador de Sistemas y Arquitectura Tecnológica será el responsable de asignar el funcionario encargado de entregar los datos para la conexión de los logs a esta herramienta. Generar correo o acta de entrega de información de logs.

El Coordinador de Sistemas y Arquitectura Tecnológica será el responsable de autorizar permisos de acceso a la herramienta que se utilice para el respaldo de logs de auditoria, para efectos de revisiones e investigaciones.

3. DESCRIPCIÓN DE LA ACTIVIDAD

Símbolo	Nombre del símbolo	Función
	Inicio/Fin	Se utiliza para indicar en donde comienza o finaliza el procedimiento.
	Actividad	Se utiliza para representar la ejecución de una actividad al interior del proceso.
	Decisión	Se utiliza para indicar que se debe evaluar una condición y plantear la selección de una alternativa.
	Conector de actividades	Se utiliza para conectar dos actividades o puntos del flujograma (solo se emplea si las actividades o puntos están en la misma página del flujograma)
	Conector de página	Se utiliza para conectar dos actividades o puntos del flujograma (solo se emplea si las actividades o puntos están páginas diferentes del flujograma)
	Proceso predefinido	Se utiliza para indicar que hay un proceso predefinido para la ejecución de una actividad.

Flujograma	Descripción	Responsable	Documentos o formatos	Puntos de control
	Inicio			
	Activación de logs. Activar los logs y auditorias de los componentes de la plataforma tecnológica para que registro los eventos cuando estos sucedan. Llevar inventario de logs por servidores y aplicativos	Coordinadores de la Dirección de Tecnología de la Información y las comunicaciones.	Inventario de logs y registros de auditoria	
	Verificación de eventos. Para los incidentes o eventos que generen indisponibilidad de las plataformas tecnológicas y sistemas de información se deben revisar los registros acerca de las actividades de los usuarios, excepciones, fallas, y eventos de seguridad de la información. Se debe estar atentos al alertamiento que se genere por las diferentes herramientas de monitoreo que existan.	Líderes de la Plataforma Tecnológica y sistemas de información	Herramienta utilizada	
	Respaldo y restauración de archivos de Auditoria. Involucrar en el plan de respaldos y pruebas de restauración los logs y registros de auditoria. Emitir y revisar trimestralmente los informes generados por la herramienta de respaldo.	Líderes de los grupos de trabajo de las Coordinadores de la Dirección de Tecnología de la Información y las comunicaciones	Plan de respaldo y restauración. Informes de la herramienta de respaldo de información	**XX**
	Parametrización de herramientas utilizadas para el monitoreo y alertamiento. Coordinar la parametrización de las herramientas de monitoreo y alertamiento y los permisos de acceso.	Coordinadores de Seguridad e Informática Forense y de Sistemas y Arquitectura Tecnológica	Correo o Actas de entrega de información de LOGS	**XX**
	FIN			

4. ANEXOS Y REGISTROS

- Herramienta utilizada para respaldo de información.
- Plan de respaldo y restauración de información.
- Herramientas de monitoreo y alertamiento.
- Correos o actas de entrega de logs.

5. CONTROL DE CAMBIOS.

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	24-02-2014	13-11-2017	Creación del documento	Director de informática y desarrollo
002	04-12-2017	31-07-2021	Se actualizó lo concerniente a: definición de actividades (activación de logs, Verificación de eventos, respaldo y restauración de logs y registros de auditoria, Parametrización de herramienta usada para la gestión de logs).	Coordinador Grupo de Sistemas y Arquitectura y Tecnología.
003	01-08-2021		Se actualizaron actividades de todos los numerales y se asignaron responsabilidades sobre la gestión de logs. Se involucran las herramientas de monitoreo y alertamiento.	Director de Tecnología de la Información y las Comunicaciones