 Superintendencia de Notariado y Registro	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION	Código: GTI - PR - 008
	PROCEDIMIENTO: GESTIÓN DE LOGS Y GESTIÓN DE LA CAPACIDAD	Versión: 1
		Fecha: 03/Oct/2025

PROCEDIMIENTO: GESTIÓN DE LOGS Y GESTIÓN DE LA CAPACIDAD	
OBJETIVO:	Definir las actividades que permitan generar trazabilidad sobre las operaciones que se realizan en los sistemas de información, bases de datos y sistemas operativos; y a su vez gestionar la capacidad de los sistemas, de manera que los resultados obtenidos permitan la toma de decisiones estratégicas.
ALCANCE:	Limite Inicial: Activación de los Logs o Registros en los Sistemas de Información
	Limite Final: Acciones, planes de mejora o decisiones estratégicas.
PRODUCTOS:	Logs y/o registros en las aplicaciones activadas Informes de monitoreo de logs y/o de capacidades de los sistemas
RESPONSABLE:	Jefe de Oficina de Tecnologías de la Información


1. GLOSARIO

- **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.
- **Backup / Copia de Seguridad:** Copia de respaldo de una información específica.
- **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.
- **Gestión de Capacidad:** Administrar y monitorear adecuadamente los recursos necesarios para llevar a cabo los servicios de TI, y previendo las necesidades de la Entidad a corto, medio y largo plazo.
- **Incidente:** Uno o una serie de eventos de seguridad de la información inesperados o no deseados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (Se ha impactado por lo menos uno de los pilares de seguridad de la información, disponibilidad, confidencialidad o integridad).
- **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.
- **Retención de Logs:** 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 estos.

2. CONDICIONES GENERALES:

2.1. Normatividad:

- Decreto 338 de 2022 "Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de

 Superintendencia de Notariado y Registro	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION	Código: GTI - PR - 008
		Versión: 1
	PROCEDIMIENTO: GESTIÓN DE LOGS Y GESTIÓN DE LA CAPACIDAD	Fecha: 03/Oct/2025

establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”.

- Decreto 767 del 2022 - “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Resolución 500 del 10 marzo de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.

2.2. Políticas de operación:


1. En caso de que existan servicios tercerizados, estos deberán generar informes mensuales de acuerdo con lo establecido en el presente procedimiento.
2. El Oficial de Seguridad de la Información podrá solicitar los informes de análisis de logs y/o de capacidades a los Gestores de manera aleatoria, con el objetivo de identificar potenciales eventos, incidentes o vulnerabilidades de seguridad u oportunidades de mejora en los sistemas de información.
3. Todos los sistemas de información, dispositivos o bases de datos deberán tener habilitado la generación de logs, los gestores de las plataformas y/o sistemas de información deberán asegurarse de esta configuración y la generación de logs.
4. Los gestores de los sistemas de información/plataformas o infraestructura de seguridad, deberán coordinar con el Gestor de Respaldos, para establecer una estrategia que permita asegurar el respaldo de los logs de sistema y de auditoría de las plataformas a cargo. Lo anterior, de acuerdo con los lineamientos establecidos en el procedimiento Gestión de Copias de Respaldo.

Las demás condiciones y políticas para ejecutar este procedimiento se encuentran en el MANUAL DE GESTIÓN DE LOGS Y GESTIÓN DE LA CAPACIDAD.

DESCRIPCIÓN DE ACTIVIDADES DEL PROCEDIMIENTO:

ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
1 ALMACENAR LOS LOGS	1.1 almacenar los logs de forma automática o manual de acuerdo con el esquema de respaldo definido.	Gestores de Aplicaciones, Servidores, Redes, Bases de Datos y Seguridad	Archivos de logs de la plataforma
2 MONITOREAR PERIÓDICAMENTE LOS LOGS	2.1 Monitorear periódicamente los logs, registros y/o indicadores los sistemas de información, para analizarlos en búsqueda de anomalías, eventos de seguridad y datos relevantes para gestión de capacidad.	Gestores de Aplicaciones, Servidores, Redes, Bases de Datos y Seguridad	Logs en Plataformas.

Código de Formato: SIG - FR - 002 Versión: 1 Fecha Aprobación: 09/Jun./2025

 Superintendencia de Notariado y Registro	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION	Código: GTI - PR - 008
		Versión: 1
	PROCEDIMIENTO: GESTIÓN DE LOGS Y GESTIÓN DE LA CAPACIDAD	Fecha: 03/Oct/2025

3 GENERAR INFORMES	3.1 Generar los respectivos informes de gestión de logs y gestión de capacidades.	Gestores de Aplicaciones, Servidores, Redes, Bases de Datos y Seguridad	Informes de Gestión de Logs y Gestión de Capacidad
4 REMITIR INFORMES AL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN.	4.1 Remitir informes de gestión de logs y gestión de capacidades al coordinador correspondiente y al oficial de seguridad de la información.	Gestores de Aplicaciones, Servidores, Redes, Bases de Datos y Seguridad	Ticket de Monitoreo en Plataforma de Mesa de Ayuda.
5 ¿EXISTEN POSIBLES ANOMALÍAS O EVENTOS DE SEGURIDAD DENTRO DE LOS INFORMES?	5.1 ¿Existen posibles anomalías o eventos de seguridad dentro de los informes? Si – Continuar con la actividad 6 No – Pasar a la actividad 7.	Coordinadores Oficina TIC Oficial de Seguridad de la Información	Informe de Análisis de Logs y de Capacidad Incidente documentado en la plataforma de mesa de ayuda.
6 EJECUTAR EL PROCEDIMIENTO DE GESTIÓN DE INCIDENTE	6.1 ejecutar el Procedimiento de Gestión de Incidentes, eventos y vulnerabilidades de seguridad y pasa a la siguiente pregunta.	Coordinadores Oficina TIC Oficial de Seguridad de la Información	Informe de Análisis de Logs y de Capacidad Incidente documentado en la plataforma de mesa de ayuda.
7 ¿EXISTEN ASPECTOS RELACIONADOS CON LA CAPACIDAD DE LA PLATAFORMA?	7.1 ¿Existen aspectos relacionados con la capacidad de la plataforma? Si – Ejecutar actividad 8. No – Fin del procedimiento.	Coordinadores Oficina TIC	Informe de Análisis de Logs y de Capacidad
8 IMPLEMENTAR ACCIONES	8.1 implementar acciones o planes de mejora correspondientes	Coordinadores Oficina TIC Gestores de Sistemas de Información, Infraestructura o Comunicaciones	Documentación de las acciones o planes de mejora formulados e implementados para gestión de capacidad.
9 DOCUMENTAR FIN	9.1 documentar y evidenciar las acciones o planes de mejora correspondientes	Coordinadores Oficina TIC Gestores de Sistemas de Información, Infraestructura o Comunicaciones	Documentación de las acciones o planes de mejora formulados e implementados para gestión de capacidad.



4. DOCUMENTOS ASOCIADOS:

4.1. Documentos internos:

Manual de Gestión de Logs y Gestión de la Capacidad

4.2. Documentos externos:

No Aplica.

 Superintendencia de Notariado y Registro 	PROCESO: GESTION DE TECNOLOGIAS DE LA INFORMACION	Código: GTI - PR - 008
		Versión: 1
	PROCEDIMIENTO: GESTIÓN DE LOGS Y GESTIÓN DE LA CAPACIDAD	Fecha: 03/Oct/2025

VERSIÓN DE CAMBIOS			
Código:	Versión:	Fecha:	Motivo de la actualización:
	1	3 de Octubre de 2025	Se hace necesario ajustar la documentación en el marco del fortalecimiento institucional con el fin de alinearlos al Sistema Integrado de Gestión y el nuevo modelo por procesos de la Entidad.

ELABORACIÓN Y APROBACIÓN			
ELABORÓ	APROBÓ	REVISIÓN METODOLOGICA	Vo. Bo. Oficina Asesora de Planeación
Juan Carlos Valenzuela Buitrago	José Ricardo Acevedo Solarte	Juan Sebastián Ávila	Santiago Campo Victoria
Oficina de tecnología de la Información	Jefe Oficina de Tecnología de la Información	Contratistas OAP	Jefe Oficina Asesora de Planeación
Fecha: 22 de septiembre 2025	Fecha: 25 de septiembre 2025	Fecha: 30 de septiembre 2025	Fecha de Aprobación: 3 de Octubre 2025