



# Superintendencia de Notariado y Registro



## MANUAL DE GESTIÓN DE LOGS Y GESTIÓN DE LA CAPACIDAD

### Gestión de Tecnologías de la Información

**SUPERINTENDENCIA**  
DE NOTARIADO Y REGISTRO

<b>Código: GTI - MN - 007</b>	<b>Versión: 1</b>	<b>Fecha: 3/Oct/2025</b>
-------------------------------	-------------------	--------------------------

EQUIPO:

JOSÉ RICARDO ACEVEDO SOLARTE

JEFE OFICINA DE TECNOLOGIA DE LA INFORMACIÓN

JUAN CARLOS VALENZUELA BUITRAGO

PROFESIONAL OFICINA DE TECNOLOGIA DE LA  
INFORMACIÓN

SEPTIEMBRE / 2025



República de Colombia

Ministerio de Justicia y del Derecho

**Superintendencia de Notariado y Registro**

---



## TABLA DE CONTENIDO

<b>INTRODUCCIÓN</b> .....	<b>3</b>
<b>OBJETIVO</b> .....	<b>4</b>
<b>ALCANCE</b> .....	<b>4</b>
<b>GLOSARIO</b> .....	<b>4</b>
<b>MARCO LEGAL</b> .....	<b>5</b>
<b>GESTIÓN DE LOGS</b> .....	<b>5</b>
1. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DE LOGS .....	5
2. LINEAMIENTOS GENERALES PARA LA GESTIÓN DE LOGS .....	6
3. COMPOSICIÓN MÍNIMA DE UN LOG O REGISTRO .....	7
4. ACTIVACIÓN DE LOGS .....	7
5. GESTIÓN DE LOGS O REGISTROS .....	7
6. GESTIÓN Y ANÁLISIS DE LA CAPACIDAD .....	10
<b>DOCUMENTOS ASOCIADOS</b> .....	<b>10</b>
<b>BIBLIOGRAFÍA</b> .....	<b>10</b>
<b>TABLA DE FIGURAS</b> .....	<b>10</b>
<b>TABLA DE TABLAS</b> .....	<b>11</b>

## INTRODUCCIÓN

En el marco del Sistema de Gestión de Seguridad de la Información (SGSI), la Superintendencia ha desarrollado este Manual con el fin de establecer los lineamientos necesarios para crear, archivar y analizar adecuadamente los logs y registros de todos los sistemas de información, permitiendo así realizar



## Superintendencia de Notariado y Registro

monitoreos, investigaciones y verificaciones de posibles eventos de seguridad; cumplir con requerimientos normativos y realizar el análisis de capacidades de las plataformas tecnológicas con base a estos registros.

### OBJETIVO

Definir los lineamientos para gestionar los logs de los sistemas de información de la Superintendencia de Notariado y Registro, así como para realizar una adecuada gestión de la capacidad de estos sistemas y el respectivo monitoreo.

### ALCANCE

Los lineamientos establecidos en este Manual aplican a toda la infraestructura tecnológica de la Superintendencia de Notariado y Registro que tengan la capacidad de generar y/o procesar logs (Servidores, Aplicaciones, Bases de Datos, Infraestructura de Seguridad, Redes entre otros); así como a los funcionarios, contratistas y terceros que la administren.

### GLOSARIO

- **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.
- **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.
- **Gestión (administración) de Log:** Proceso mediante el cual se realiza la generación, transmisión, almacenamiento, análisis, monitoreo y reporte de los Logs.
- **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



## Superintendencia de Notariado y Registro

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.
- **SOC (Security Operations Center, o Centro de Operaciones de Seguridad):** Es un equipo especializado que monitorea, detecta, analiza y responde a amenazas de ciberseguridad en tiempo real dentro de una organización
- **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.

### MARCO LEGAL

- 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 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”.

### GESTIÓN DE LOGS

#### 1. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DE LOGS

Los roles que participan para llevar a cabo una adecuada gestión de Logs y Gestión de Capacidades son los siguientes:



## Superintendencia de Notariado y Registro

- **GESTOR DE APLICACIÓN:** Funcionarios y/o contratistas de la Oficina de Tecnologías de la Información que realizan las actividades de configuración de los sistemas de información para la generación y procesamiento de logs, verificación de eventos e incidentes en la infraestructura de seguridad informática.
- **GESTOR DE BASE DE DATOS:** Funcionarios y/o contratistas de la Oficina de Tecnologías de la Información que realizan las actividades de configuración de las bases de datos para generación de logs, verificación de eventos, incidentes y capacidades en las bases de datos.
- **GESTOR DE INFRAESTRUCTURA:** Funcionarios y/o contratistas de la Oficina de Tecnologías de la Información que realizan las actividades de configuración de la infraestructura de servidores para la generación de logs, verificación de eventos, incidentes y capacidad en la infraestructura de servidores.
- **GESTOR INFRAESTRUCTURA DE SEGURIDAD:** Funcionarios y/o contratistas de la Oficina de Tecnologías de la Información que realizan las actividades de configuración de la infraestructura de seguridad informática para la generación y procesamiento de logs, verificación de eventos e incidentes en la infraestructura de seguridad informática.
- **GESTOR DE REDES:** Funcionarios y/o contratistas de la Oficina de Tecnologías de la Información que realizan las actividades de configuración de la infraestructura de conectividad para la generación y procesamiento de logs, verificación de eventos e incidentes.
- **GESTOR DE RESPALDOS:** Funcionario y/o contratista de la Oficina de Tecnologías de la Información que realiza las actividades de configuración de la infraestructura de respaldos de información para la generación de logs, verificación de eventos e incidentes en la infraestructura de respaldos de información. Apoyar en las tareas de respaldo de los logs de los sistemas de información, conforme a los requerimientos recibidos por parte de los gestores de aplicación.

Otras responsabilidades se encuentran descritas en el desarrollo de este manual en las siguientes secciones.

## 2. LINEAMIENTOS GENERALES PARA LA GESTIÓN DE LOGS

El monitoreo y la gestión de logs provee a la entidad de instrumentos para el análisis y posible toma de decisiones; optimizando los tiempos de investigación, tratando de identificar las causas de posibles incidentes o eventos generados en los sistemas informáticos. Así mismo, constituyen una herramienta primordial para el análisis y gestión de la capacidad de los sistemas de información.

En los desarrollos de los sistemas de información y/o aplicaciones de la Superintendencia de Notariado y Registro (tanto adquiridos como propios), se debe cumplir con requisitos de generación de logs de sistema y de auditoría; así como con las características mínimas de las que trata el presente manual, salvo excepciones documentadas.



### 3. COMPOSICIÓN MÍNIMA DE UN LOG O REGISTRO

Un log o registro emitido por un componente de TI, deberá ser generado como mínimo con la siguiente información:

- Fecha del evento.
- Hora del evento.
- Equipo o sistema donde se realiza el evento.
- Usuario de dominio o usuario local de base de datos.
- Hostname y/o Dirección IP que produce el evento.
- Tipo de evento y archivo que se modifica en el evento (creación, modificación o eliminación de un campo de información).
- Especificaciones o detalles del evento.

### 4. ACTIVACIÓN DE LOGS

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

Es responsabilidad de cada administrador de los componentes anteriores realizar la activación de estos logs.

De igual forma, en los proyectos de desarrollo y mantenimiento de sistemas de información, es requisito obligatorio la creación de los archivos de logs como se indica en el **MANUAL DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**.

### 5. GESTIÓN DE LOGS O REGISTROS

Las actividades relacionadas con la gestión de logs comprenden el respaldo, monitoreo y análisis de los logs.



## Superintendencia de Notariado y Registro

**5.1 Respaldo de Logs o Registros.** Cada administrador de los componentes será responsable de respaldar los logs que estas gestionan y almacenan.

De igual forma, siempre que se ejecuten actividades de depuración sobre los sistemas o bases de datos, los logs deberán ser protegidos y respaldados.

- **NOTA 1:** Si no existe plataforma que gestione o almacene los logs, se deberá respaldar de forma manual la base de datos de logs y/o las configuraciones de cada dispositivo de forma mensual en el repositorio dispuesto para tal fin.
- **NOTA 2:** Los dispositivos que tengan la funcionalidad de colectores de logs o correlacionador de logs, tendrán como plazo máximo la periodicidad trimestral para respaldar sus logs.

Será responsabilidad de cada administrador solicitar el esquema de respaldo con el gestor de respaldos de información, para establecer el que más se adapte a cada sistema, diligenciando el **FORMATO DE CREACIÓN, MODIFICACIÓN Y ELIMINACIÓN DE POLÍTICAS DE RESPALDO** y remitiéndolo conforme con lo dispuesto en el PROCEDIMIENTO MESA DE AYUDA INTEGRAL - MAI

En caso de contar con servicios de un Centro de operaciones de seguridad (SOC), se deben establecer directrices específicas de retención, respaldo y recuperación de los logs y registros de auditorías de los componentes de la plataforma tecnológica, a parte de los servicios de monitoreo y análisis correspondiente.

**5.2 Respaldo de Configuraciones de Equipos de Redes y Seguridad.** Los administradores de las plataformas de seguridad y networking, deberán almacenar mensualmente una copia de configuración de los dispositivos, con el objetivo de prevenir pérdidas sustanciales de información en caso de avería de algún dispositivo o para la ejecución de actividades de rollback en cambios ejecutados en estas plataformas.

**5.3 Monitoreo y Análisis de Logs o Registros.** El monitoreo y análisis de logs se realizará a través de las siguientes tres actividades:

1. Los responsables de la gestión de las aplicaciones, infraestructura, bases de datos y seguridad deben realizar una revisión periódica (al menos una vez al mes) de los registros generados sobre las actividades de los usuarios, excepciones, fallas y posibles eventos o incidentes de seguridad de la información. Como resultado de esta revisión, se deberá generar y emitir un informe al coordinador correspondiente, con copia al Oficial de Seguridad, con el fin de identificar eventos o incidentes de seguridad.

En la ejecución de esta actividad, se debe prestar especial atención a cualquier situación que se considere atípica dentro del sistema o que no corresponda con el comportamiento habitual, ya que



## Superintendencia de Notariado y Registro

podría representar una falla o un incidente de seguridad. Dado que cada administrador conoce la normalidad en la gestión de su plataforma, es su responsabilidad identificar estas anomalías y reportarlas oportunamente.

2. El oficial de seguridad de la información revisará aleatoriamente que los logs se estén almacenando en el repositorio definido. Así mismo, realizará revisiones periódicas a los informes emitidos por los administradores.
3. Si las plataformas generan alguna alerta que pueda representar un evento o incidente de seguridad de la información, deberá realizarse una revisión inmediata de los logs de la plataforma por parte del responsable.

Si en el proceso de la revisión de logs se llegara a encontrar un incidente de seguridad, los administradores deberán realizar el reporte conforme al **PROCEDIMIENTO GESTIÓN DE EVENTOS, INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN**.

**5.4 Retención de Logs o Registros.** Retención de los logs está definido por las siguientes condiciones según las tecnologías disponibles en la entidad:

Tipo de Log	Tiempo recomendado	Justificación
Logs de bases de datos	2 años (servicios críticos) / 2 años (servicios generales)	Para análisis forense y auditoría de seguridad.
Logs de aplicaciones	2 años (servicios críticos) / 2 años (servicios generales)	Depuración. rastreo de errores y transacciones a nivel de aplicación.
Logs de accesos y autenticación	2 años	Detección de accesos no autorizados.
Logs de seguridad (SIEM, firewall, IDS/IPS)	2 años	Importante para respuesta ante incidentes.
Logs de infraestructura (servidores, redes)	2 años	Para troubleshooting (rastreo de errores) y mantenimiento.

*Tabla 1 Tiempos de retención de Logs*



## Superintendencia de Notariado y Registro

Los tiempos establecidos podrán ser actualizados en caso de nuevos requerimientos normativos o de acuerdo a las capacidades y recursos tecnológicos disponibles.

### 6. GESTIÓN Y ANÁLISIS DE LA CAPACIDAD

Los encargados de la gestión de infraestructura, gestión de seguridad informática, gestión de redes, gestión de las bases de datos y los gestores de aplicaciones deberán realizar mensualmente la revisión de la proyección de la capacidad de los componentes tecnológicos relacionados a sus roles, indicando las siguientes características mínimas a través del respectivo informe:

- Estado actual de la capacidad tecnológica (almacenamiento, procesamiento, anomalías y estado de obsolescencia del sistema).
- Cantidad de conexiones, tiempos de respuesta o performance de las aplicaciones en términos de verificar posibles necesidades de escalabilidad.
- Proyección de la capacidad disponible, indicando un estimado para llegar al límite de capacidad con los componentes tecnológicos actuales, considerando el rango de crecimiento en el uso de los recursos.
- Necesidades, novedades y/o recomendaciones generales (si aplica).

Los resultados del análisis y gestión de la capacidad deberán ser informados al coordinador correspondiente, quienes a su vez informarán datos de relevancia al jefe de la Oficina de Tecnologías de la Información, para realizar preventivamente las gestiones administrativas y presupuestales correspondientes.

### DOCUMENTOS ASOCIADOS

Procedimiento Gestión de Logs y Gestión de la Capacidad

### BIBLIOGRAFÍA

No Aplica.

### TABLA DE FIGURAS

No Aplica.



**Superintendencia de  
Notariado y Registro**

**TABLA DE TABLAS**

Tabla 1 Tiempos de retención de Logs ..... 9

<b>VERSIÓN DE CAMBIOS</b>			
<b>Código:</b>	<b>Versión:</b>	<b>Fecha:</b>	<b>Motivo de la actualización:</b>
	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.

<b>ELABORACIÓN Y APROBACIÓN</b>			
<b>ELABORÓ</b>	<b>APROBÓ</b>	<b>REVISIÓN METODOLOGICA</b>	<b>Vo. Bo. Oficina Asesora de Planeación</b>
Juan Carlos Valenzuela Buitrago	José Ricardo Acevedo Solarte	Juan Sebastián Ávila	Santiago Campo Victoria
Oficina de tecnología de la Información y las Comunicaciones	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