



Superintendencia de Notariado y Registro



MANUAL DE GESTIÓN DE CONTROLES CRIPTOGRÁFICOS

Gestión Tecnologías de la Información

**SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO**

Código: GTI - MN - 005	Versión: 1	Fecha: 3/Oct/2025
-------------------------------	-------------------	--------------------------

EQUIPO:

JOSÉ RICARDO ACEVEDO SOLARTE
JEFE OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
JUAN CARLOS VALENZUELA BUITRAGO
PROFESIONAL OFICINA DE TECNOLOGIA DE LA
INFORMACIÓN
SANTIAGO CAMPO VICTORIA
JEFE OFICINA ASESORA DE PLANEACIÓN

SEPTIEMBRE / 2025



República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro



TABLA DE CONTENIDO

INTRODUCCIÓN	4
OBJETIVO	4
ALCANCE	4
GLOSARIO	4
MARCO LEGAL	5
GESTIÓN DE CONTROLES CRIPTOGRÁFICOS	6
DOCUMENTOS ASOCIADOS	8
BIBLIOGRAFÍA	8
TABLA DE FIGURAS	8
TABLA DE TABLAS	8



Superintendencia de Notariado y Registro

INTRODUCCIÓN

En el marco del Sistema de Gestión de Seguridad de la Información (SGSI), la Superintendencia ha desarrollado el Manual de Gestión de Controles Criptográficos para establecer los lineamientos que permitan una gestión adecuada de llaves y controles criptográficos en la entidad, garantizando su correcto uso para la protección de los activos de información.

OBJETIVO

Establecer los lineamientos para una gestión adecuada de llaves y controles criptográficos en la entidad, garantizando su correcto uso para la protección de los activos de información. Esto incluye la gestión de certificados SSL, autenticación VPN, firmas digitales, mecanismos de cifrado, entre otros. De igual manera, este manual complementa las directrices necesarias para ejecutar adecuadamente el **PROCEDIMIENTO DE GESTIÓN DE CONTROLES CRIPTOGRÁFICOS**.

ALCANCE

Los lineamientos definidos en este documento aplican para todas las dependencias de la Superintendencia que tratan información sensible o sistemas de información que la gestione, también al personal encargado de implementar los controles criptográficos en los servicios de red, en la infraestructura y/o los sistemas de información en la Superintendencia que almacenen o transmitan información sensible.

GLOSARIO

- **Activo de Información:** Cualquier dato, documento o recurso digital que tenga valor para la organización y requiera protección.
- **Autenticación:** Proceso de verificación de identidad de un usuario, sistema o entidad antes de conceder acceso a recursos.
- **Certificado Digital:** Documento electrónico emitido por una autoridad certificadora que autentica la identidad de un usuario o sistema.



Superintendencia de Notariado y Registro

- **Certificado SSL (Secure Sockets Layer):** Objetos digitales que autentican la identidad de un sitio web y permiten establecer una conexión encriptada segura, conocida como HTTPS.
- **Cifrado:** Técnica utilizada para convertir datos en un formato ilegible sin una clave de descifrado, con el fin de proteger su confidencialidad.
- **Control Criptográfico:** Medida de seguridad que emplea técnicas criptográficas para proteger la integridad, autenticidad y confidencialidad de los datos.
- **Firma Digital:** Método criptográfico que permite verificar la autenticidad y la integridad de un documento o mensaje digital.
- **Gestión de Criptográficas:** Proceso de creación, distribución, almacenamiento y eliminación segura de claves criptográficas.
- **Seguridad de la Información:** Conjunto de medidas y prácticas destinadas a proteger la confidencialidad, integridad y disponibilidad de la información.
- **SSL (Secure Sockets Layer):** Protocolo de seguridad que permite establecer comunicaciones cifradas entre un cliente y un servidor en internet.
- **VPN (Virtual Private Network):** Tecnología que permite establecer conexiones seguras y cifradas a través de redes públicas como internet.

MARCO LEGAL

- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Resolución No. 02213 del 5 de marzo de 2025 “Por la cual se adopta el uso de firmas digitales, electrónicas y mecánicas en la Superintendencia de Notariado y Registro y se dictan otras disposiciones para fortalecer la gestión documental y administrativa” se solicita amablemente la autorización para el uso del grafo en el sistema DOCU” o la que se encuentre vigente con relación a la adopción de firmas digitales en la SNR.



GESTIÓN DE CONTROLES CRIPTOGRÁFICOS

1. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DE CONTROLES CRIPTOGRÁFICOS

Los roles que participan para llevar a cabo una adecuada gestión de controles criptográficos son los siguientes:

- Jefe de Oficina de Tecnologías de la Información
- Gestor de Controles Criptográficos: Consolidar, actualizar y hacer seguimiento del Listado único de Controles Criptográficos de la Superintendencia de Notariado y Registro, así como el registro de cada actividad asociada con los controles de la Entidad.
- Gestores de Aplicaciones. Funcionarios Oficina de Tecnologías de la Información encargados de aplicar, modificar o eliminar los controles Criptográficos.

Las responsabilidades se encuentran descritas en el desarrollo de este manual y el **PROCEDIMIENTO DE GESTIÓN DE CONTROLES CRIPTOGRÁFICOS**.

2. LINEAMIENTOS GENERALES

Se definen los siguientes lineamientos generales, que buscan orientar una adecuada gestión de controles criptográficos en la Superintendencia de Notariado y Registro:

- La única área autorizada para administrar las soluciones tecnológicas de controles criptográficos es la Oficina de Tecnologías de la Información (OTI).
- La autorización de creación, renovación, modificación o eliminación de un control criptográfico determinado estará bajo la discreción de los gestores de aplicaciones, teniendo en cuenta aspectos como la disponibilidad, el tipo de activo a proteger y la necesidad específica del control solicitado.
- Todas las implementaciones de controles criptográficos deberán documentarse en el **FORMATO LISTADO DE CONTROLES CRIPTOGRÁFICOS**, registrando el propósito, los responsables y cualquier otro dato relevante. La responsabilidad de la consolidación, actualización y seguimiento del Listado único de Controles Criptográficos de la Superintendencia de Notariado y Registro es del Gestor de Controles Criptográficos; quien deberá registrar cada actividad asociada con los controles de la Entidad.



Superintendencia de Notariado y Registro

- Todos los controles vigentes deberán estar documentados en el FORMATO LISTADO DE CONTROLES CRIPTOGRÁFICOS.
- Excepcionalmente la solicitud de creación, renovación, modificación o eliminación de controles Criptográficos podría someterse a aprobación por parte del Coordinador de Infraestructura o del Oficial de Seguridad de la información, cuando a criterio del Gestor de Controles Criptográficos la solicitud pueda afectar de alguna manera la integridad de la información de la SNR.

3. SOLICITUD DE CONTROLES CRIPTOGRÁFICOS

Para solicitar controles criptográficos, se deberá crear un requerimiento en la Mesa de Ayuda, siguiendo lo establecido en el Procedimiento de Mesa de Ayuda Integral. La solicitud debe incluir:

- El tipo de control criptográfico requerido (Certificado SSL, cifrado de base de datos, VPN, firma digital, etc.).
- Los activos de información que se protegerán o sobre los que se aplicará el control.
- La justificación de la necesidad del control.

4. ACTUALIZACIÓN DE CONTROLES CRIPTOGRÁFICOS

Las actualizaciones de controles criptográficos deberán realizarse en función de los siguientes criterios:

- **Vencimiento de llaves o certificados:** Se deberá programar la renovación antes de su fecha de caducidad.
- **Cambios en las tecnologías de cifrado:** La actualización deberá realizarse en función de las recomendaciones internacionales y actualizaciones tecnológicas.
- **Revisión periódica:** Se debe realizar una revisión MENSUAL para asegurar que los controles criptográficos cumplen con los estándares de seguridad vigentes.

El Gestor de Controles Criptográficos mensualmente deberá verificar los vencimientos de los controles y notificar a los usuarios del control con mínimo con 90 días de antelación el vencimiento de los mismos, para tomar las medidas preventivas pertinentes y evitar fallas en el funcionamiento de la entidad.

Los controles criptográficos podrán ser revocados o eliminados bajo las siguientes condiciones:

- **Compromiso de seguridad:** Si se detecta que una clave o certificado ha sido comprometido, deberá revocarse de inmediato.



Superintendencia de Notariado y Registro

- **Obsolescencia tecnológica:** Cuando el control deje de ser compatible con las tecnologías actuales o se considere inseguro.
- **Cambio en la necesidad de protección:** Si el activo deja de requerir protección mediante el control criptográfico.
- **Finalización del vínculo contractual o laboral:** Una vez finalicen los vínculos laborales o contractuales, se revocarán los controles asignados, como el caso de firmas o certificados.

Toda revocación o eliminación debe ser documentada, incluyendo el motivo, el responsable y la fecha de la acción atendiendo las actividades del Procedimiento Gestión de Controles Criptográficos.

DOCUMENTOS ASOCIADOS

Procedimiento Gestión de Controles Criptográficos
Listado de Controles Criptográficos

BIBLIOGRAFÍA

No Aplica.

TABLA DE FIGURAS

No Aplica.

TABLA DE TABLAS

No Aplica.

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.



**Superintendencia de
Notariado y Registro**

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