|  |  |  |
| --- | --- | --- |
|  | PROCEDIMIENTO | A-PR-GTI-051 |
| **Versión: 3** |
| Gestión de Llaves criptográficas | | |

# **1. OBJETIVO**

Establecer un proceso para el uso de la criptografía en el cual, la Dirección incluya un enfoque con relación al uso de controles criptográficos en toda la organización, utilizando los principios generales bajo los cuales se deben proteger la información del negocio.

# **2. ALCANCE**

Aplica para todas las dependencias que incluyan dentro de sus procesos el uso de certificados de Función Pública usados por los funcionarios de la Superintendencia Financiera de Colombia que por sus labores requieren el uso de estos elementos Criptográficos.

# **3. DEFINICIONES**

• Algoritmo asimétrico: Es un algoritmo que modifica los datos de un documento con el objeto de alcanzar algunas características de seguridad como autenticación, integridad y confidencialidad. También conocidos como algoritmos de llave pública. Su principal característica es que no se basa en una única llave sino en un par de ellas: una conocida Pública y otra Privada

• Algoritmo: Es un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.

• Certificado de firma digital: Es un mecanismo equivalente a la firma manuscrita que garantiza la identidad y responsabilidad del autor de documento transacción electrónica, así como también permite comprobar la integridad del mismo, es decir que la información no ha sido alterada. Las firmas digitales generadas mediante el uso de certificados digitales, cuentan con el mismo valor probatorio y fuerza obligatoria de una firma manuscrita, aportando un atributo de seguridad jurídica adicional, como lo es la integridad de la información.

• Certificado digital: Es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital.

El certificado digital tiene como función principal autenticar al poseedor, pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información sensible entre las partes.

• Clave: Es el conjunto finito de caracteres alfanuméricos necesarios para el uso del certificado digital, el cual debe ser conocido únicamente por el titular del certificado.

• Entidad Certificadora: Recibe la Solicitud por parte de la Superintendencia Financiera y posteriormente lo emite a nombre del funcionario.

• Entidad de Certificación: Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

• Equipo de Seguridad: Personas que validan el requerimiento y lo autorizan.

• Llave privada: Es uno de los documentos electrónicos que genera el uso de algoritmo asimétrico y que sólo debe ser conocido y resguardado por el propietario del par de llaves (pública/privada). Con esta llave privada se realiza el firmado digital, mismo que codifica el contenido de un mensaje.

• Llave pública: Es uno de los documentos electrónicos que genera el uso de algoritmo asimétrico y que se publica junto con el certificado digital para cifrar información que se desea enviar el propietario de la llave privada. La llave pública se presenta dentro del archivo de requerimiento para presentarlo ante el SAT y obtener un certificado digital.

• Revocación: La revocación es el medio por el cual se cancelará e inhabilitará el certificado digital y se dará por terminado su periodo de confiabilidad; al presentarse alguna de las causas establecidas en la declaración de prácticas de certificación.

• Token: Dispositivo de almacenamiento de certificados digitales (similar a una USB), utilizado para facilitar el proceso de autenticación de usuarios.

• Usuario o Coordinador: Persona que Solicita el certificado o cambio de asignación del mismo desde el área solicitante

# **4. CONDICIONES GENERALES**

4.1. Tramitar la solicitud de las necesidades de certificados de firma digital o certificados digitales. El Grupo de Plataforma de TI se encarga de realizar el proceso de adquisición de los certificados, para lo cual se realiza el inventario de las dependencias de la entidad que en sus procesos utilizan elementos criptográficos.

4.2. Para la solicitud de los certificados de función pública, será necesario que el funcionario adjunte a la solicitud, los documentos requeridos por la entidad certificadora como lo son: la fotocopia de la cédula ampliada al 150%, acta de posesión del funcionario, y formularios de solicitud firmados por el funcionario y por el supervisor del contrato o demás requerimientos que la entidad certificadora solicite.

4.3. El Coordinador del área que requiere los certificados de función pública se encarga enviar los requerimientos de certificados de firma digital y/o certificados digitales una vez estén firmadas las autorizaciones, a través de correo electrónico o a través de la plataforma autorizada (según la entidad certificadora lo solicite). Se deberá seguir el procedimiento adicional propio de cada entidad certificadora para esta solicitud.

4.4. Una vez hecha la solicitud, y aprobados los documentos, la entidad certificadora expedirá el certificado en un tiempo no mayor a un (1) día hábil después de aprobada.

4.5. El certificado o firma digital será entregado por la entidad certificadora directamente a cada funcionario en las instalaciones de la Superintendencia Financiera de Colombia.

4.6. Los certificados digitales deben ser cíen por ciento (100%) compatibles con el (Sistema Integrado de información Financiera) del Ministerio de Hacienda.

4.7. Los certificados digitales de Función Pública deben cumplir con las garantías de seguridad: Autenticidad, Integridad, No repudio y Confidencialidad, establecidas en las regulan la materia.

4.8. Las revocaciones de los certificados de función pública deberán cumplir con el procedimiento establecido por la entidad certificadora, para lo cual se deberá enviar un correo al supervisor del contrato y este a su vez iniciar el proceso de acuerdo con las condiciones del contrato.

4.9. La instalación de los certificados será realizada por la mesa de ayuda de la Superfinanciera; en caso de presentar problemas se deberá escalar con la entidad certificadora con el fin de garantizar la disponibilidad de los certificados.

4.10. Suministrar Certificados Digitales Jurídicos, Tipo Token / P12 de acuerdo con las necesidades de la Superintendencia Financiera de Colombia.

4.11. La solicitud de estos se realiza a través del supervisor del contrato, para lo cual es necesario que el administrador de la aplicación haga la solicitud al menos 15 días hábiles antes del vencimiento del certificado. Una vez hecha la solicitud, el supervisor del contrato solicitará los documentos del Representante Legal de la Superfinanciera, requeridos por la entidad certificadora.

4.12. Posteriormente se le informa al Representante Legal de la entidad el procedimiento a seguir, el cual incluye una llamada o correo de confirmación, y posteriormente la entrega personal del certificado.

4.13. Los certificados SSL serán tramitados 8 días hábiles previos a la fecha de vencimiento, para o cual, los administradores deberán generar los respectivos request y enviarlos al Supervisor del Contrato.

4.14. Una vez generados estos request se tramita la solicitud a la entidad certificadora de acuerdo con el procedimiento establecido.

4.15. Una vez hecha la solicitud, y estando dentro de los tiempos establecidos en el contrato, el certificado emitido por la entidad certificadora es entregado a los administradores para su respectiva instalación.

4.16. En la gestión de certificados, cambios o nuevos requerimientos participan: Usuario o Coordinador, Equipo de Seguridad, Entidad Certificadora.

4.17. Para evitar el vencimiento de los certificados, se debe tener en cuenta el A-PI-GTI-069 "Inventario de certificados digitales", el cual está a cargo de cada administrador del certificado y del funcionario del equipo de Seguridad asignado para tal fin.

|  |
| --- |
|  |
| **5. DESARROLLO** |
| |  |  |  |  | | --- | --- | --- | --- | | **No.** | **Actividad** | **Responsable** | **Documento** | | 1 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Realizar el inventario de las dependencias de la entidad que en sus procesos utilizan elementos criptográficos. | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Grupo de Seguridad de TI | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | A-PI-GTI-069 Inventario de certificados digitales | | | 2 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Verificar fecha de vencimiento o estado de los Certificados Digitales (Emisión, Renovación, Gestionado) en la matriz establecida cada inicio de semana o día hábil siguiente a esta   Notifica por correo a los responsables el estado o las novedades de los certificados digitales.   Registrar el seguimiento en la Matriz. | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Grupo de Seguridad de TI | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | A-PI-GTI-069 Inventario certificados digitales  Correo | | | 3 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Solicitud nueva (si aplica)   Notificar por correo electrónico al responsable de generar Request y al solicitante del Certificado a la entidad certificadora, con copia al Grupo de seguridad de acuerdo con el tipo de certificado.   Si es de Persona Jurídica 15 días hábiles previos a la fecha de vencimiento Si es SSL notificar 8 días hábiles previos a la fecha de vencimiento. | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Grupo de Seguridad de TI | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Correo | | | 4 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Realizar el proceso de adquisición de los certificados | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Grupo de plataforma de TI | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | | 5 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Remitir los documentos requeridos por la entidad certificadora | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Funcionario | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | | 6 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Enviar los requerimientos de certificados de firma digital y/o certificados digitales una vez estén firmadas las autorizaciones | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Coordinador del área | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Correo | | | 7 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Revisa, aprueba solicitud y expide certificado | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Entidad certificadora | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | | 8 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Entrega del certificado al funcionario en las instalaciones de la SFC | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Entidad certificadora Funcionario | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Certificado | | | 9 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Instalación del certificado correcta  SI:  Continua siguiente paso No: Escalar con la entidad certificadora con el fin de garantizar la disponibilidad de los certificados. | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Analista de Mesa de ayuda  Entidad certificadora | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | | 10 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Solicitar documentos del Representante Legal de la Superfinanciera, requeridos por la entidad certificadora | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Supervisor del contrato | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | | 11 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Solicitar documentos del Representante Legal de la Superfinanciera, requeridos por la entidad certificadora | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Supervisor del contrato | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Correo / llamada telefónica | | | 12 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Registrar el seguimiento en la Matriz de vigencia de certificados indicando si se renovó o se agregó uno nuevo. | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Grupo de seguridad de TI | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | A-PI-GTI-069 Inventario de certificados digitales | | | 13 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Actualizar la Matriz de certificados validando que todos los certificados se encuentren en estado renovados o gestionados y genera un nuevo inventario para el año siguiente | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | Grupo de Seguridad de TI | | |  |  |  |  | | --- | --- | --- | --- | |  |  |  | A-PI-GTI-069 Inventario de certificados digitales | | |
|  |
| **6. DOCUMENTOS DE REFERENCIA** |
| |  | | --- | |  | |
|  |
| **7. HISTORIAL DE CAMBIOS** |
| |  |  |  | | --- | --- | --- | | **Versión** | **Fecha** | **Cambios** | | 1 | 29/Nov/2019 | Versión inicial. | | 2 | 10/Dic/2019 | Se ajusta documento. | | 3 | 21/Oct/2021 | En la condición 4.17. se hace referencia al Inventario de certificados digitales antes Matriz de vigencia de certificados Se incluyen actividades 2,3, 12,13, que hacen referencia al seguimiento del Inventario de certificados digitales | |
|  |

|  |  |  |
| --- | --- | --- |
| **Elaboró** | **Revisó** | **Aprobó** |
| |  |  | | --- | --- | | **Nombre:** | Liana Beatriz Prada Aragon | | **Cargo:** | PROFESIONAL UNIVERSITARIO | | **Fecha:** | 21/Oct/2021 | | |  |  | | --- | --- | | **Nombre:** | Oscar Osorio Gomez | | **Cargo:** | SUBDIRECTOR TECNICO | | **Fecha:** | 21/Oct/2021 | | |  |  | | --- | --- | | **Nombre:** | Jose Humberto Vélez Gutierrez | | **Cargo:** | DIRECTOR DE TECNOLOGIA | | **Fecha:** | 22/Oct/2021 | |

Copia no Controlada: Si este documento se encuentra impreso no se garantiza su vigencia, puesto que la versión vigente reposa en el aplicativo del SGI.

Nota: De acuerdo con los criterios de accesibilidad establecidos en el Anexo 1 de la Resolución 1519 de 2020, con el objetivo de ser consultados fácilmente por cualquier ciudadano, siendo certificados por cada líder de proceso.