



**Hacienda**



## **Política de seguridad de la información del SIIF Nación**

**Versión 2.0**



22 de agosto de 2019

## **POLITICAS DE SEGURIDAD DE LA INFORMACION DEL SIIF NACIÓN**

### **1. INTRODUCCIÓN A LAS POLÍTICAS**

Una de las funciones que desarrolla el Ministerio de Hacienda y Crédito Público es el correcto manejo de los recursos públicos, gran parte de los cuales están representados en el Presupuesto General de la Nación, el cual se gestiona utilizando el Sistema Integrado de Información Financiera SIIF NACIÓN.

El Ministerio de Hacienda y Crédito Público consciente que la Información del SIIF NACIÓN es uno de los activos importantes de la institución y del estado colombiano, se ha propuesto como objetivo establecer políticas que normen sobre la seguridad y privacidad de dicha información.

Los elementos enunciados en las presentes Políticas y sus posteriores actualizaciones son de carácter mandatorio para todos usuarios, los órganos de dirección y administración, para los administradores de los componentes funcionales y técnicos del SIIF NACIÓN.

### **2. OBJETIVOS DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN DEL SIIF NACIÓN**

En su conjunto las políticas, los estándares y los procedimientos de seguridad del SIIF NACIÓN, así como su estructura organizacional y tecnológica que los soporta conforman el modelo de seguridad de la información del SIIF NACIÓN.

El modelo de Seguridad de la Información del SIIF NACIÓN permitirá salvaguardar la confidencialidad, integridad y disponibilidad de la información Financiera Pública Nacional.

- ✓ Confidencialidad. Aseguramiento de que la información es accesible sólo para quienes están autorizados.
- ✓ Integridad. Salvaguardia de la exactitud y completitud de la información y sus métodos de procesamiento.
- ✓ Disponibilidad. Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando se requiera.

El objetivo del modelo de seguridad de la información del SIIF - NACIÓN es implantar políticas, estándares y procedimientos que, con el pleno compromiso de los funcionarios de Ministerio de Hacienda y Crédito Público, de los órganos rectores y de los usuarios del sistema, permita que la operación del SIIF NACIÓN sea segura y se disminuyan los riesgos que comprometan la confidencialidad, integridad y disponibilidad del sistema.

Este modelo aplica a toda la información del SIIF - NACIÓN contenida en el sistema y las funcionalidades ofrecidas para su consulta y tratamiento. Así como la información funcional y técnica requerida para la operación y mantenimiento del sistema.

Se debe tener en cuenta que la confidencialidad, integridad y disponibilidad de la información es esencial para que la Administración del SIIF NACIÓN, la Dirección General del Presupuesto Público Nacional y la Dirección General de Crédito Público y Tesoro Nacional del Ministerio de Hacienda y Crédito Público, la Contaduría General de la Nación y las entidades usuarias cumplan con sus objetivos, por tanto el éxito del modelo de seguridad de la información del SIIF NACIÓN depende de su participación activa, de sus sugerencias, guías e iniciativas para que la seguridad de la información sea efectiva y eficiente.

Para asegurar el cumplimiento de los objetivos que se establecen en el presente documento, esta política anticipa y autoriza el diseño de procedimientos operativos detallados y otras medidas administrativas, así como, el desarrollo y la adquisición de los mecanismos preventivos y reactivos, software y otras técnicas de protección.

El modelo debe asegurar todos los recursos del SIIF - NACIÓN que se identifiquen como críticos o sensible por su confidencialidad, integridad y disponibilidad.

### **3. POLÍTICAS DE SEGURIDAD DEL SIIF NACIÓN**

Con el fin de hacer efectivo el proceso para fortalecer la seguridad de la información del SIIF NACIÓN, las políticas definidas, son requisitos de la Administración del SIIF NACIÓN para el desarrollo de las actividades relacionadas con el diseño de controles, análisis de riesgos, controles de acceso e investigaciones y sanciones disciplinarias internas, por acciones contra la información crítica del Sistema o por violaciones a su seguridad.

Toda la información del SIIF Nación debe ser protegida contra acceso no autorizado para mantener su confidencialidad e integridad. Por tanto, se establecerán niveles de requerimientos de protección que serán administrados y controlados de acuerdo con la naturaleza y uso de la información, la cual será clasificada por su dueño, para establecer las medidas de seguridad.

Las políticas establecidas incluyen la seguridad de la información del SIIF NACIÓN, la organización de la seguridad y sus responsabilidades, privacidad, capacitación y concientización, planeación de la continuidad del SIIF NACIÓN, reporte de Incidentes, variaciones y pérdidas de efecto, su implantación y programación.

### **3.1 SEGURIDAD DE LA INFORMACIÓN DEL SIIF - NACIÓN**

Los recursos del SIIF Nación que se identifiquen como críticos por su confidencialidad, integridad y disponibilidad deben ser salvaguardados.

El Comité Operativo y de Seguridad del SIIF NACIÓN definirá los niveles de seguridad y participará en el desarrollo de las soluciones para protegerlos.

El Administrador del SIIF Nación con el apoyo del líder de Seguridad del SIIF - NACIÓN establecerá los lineamientos para la protección de esos recursos de acuerdo con los niveles de seguridad establecidos.

La implantación de los controles definidos por la Administración del SIIF NACIÓN podrán ser realizados por la dependencia del Ministerio de Hacienda y Crédito Público competente para tal fin.

### **3.2 ORGANIZACIÓN Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACION DEL SIIF NACIÓN.**

Esta política reconoce que la responsabilidad final de los recursos de información del SIIF NACIÓN está en quienes los “poseen” y “utilizan”.

La responsabilidad específica de asegurar la confidencialidad e integridad de la información sensible en el SIIF Nación, depende de cada persona que utiliza el sistema, archivos y datos, los que supervisan a los usuarios del SIIF NACIÓN, los que poseen los datos o aplicaciones que residen en los equipos, y los que administran, manejan o dan mantenimiento al SIIF NACIÓN.

Esta política define las siguientes responsabilidades para los órganos de dirección y administración, para los usuarios y para los administradores de los componentes funcionales y técnicos del SIIF NACIÓN:

#### **Responsabilidades del Comité Directivo del SIIF NACIÓN**

Las que están establecidas en el artículo 2.9.1.1.9 del decreto 1068 del 26 de mayo de 2015.

#### **Responsabilidades del Comité Operativo y de Seguridad del SIIF NACIÓN**

Las que están establecidas en el artículo 2.9.1.1.11 del decreto 1068 del 26 de mayo de 2015.

## **Responsabilidades del Administrador del SIIF NACIÓN**

El Administrador del sistema es el encargado de ejecutar las funciones a las que se refiere el Artículo 2.9.1.1.13 del 11 del decreto 1068 del 26 de mayo de 2015.

Deberá trabajar con el apoyo del Comité Operativo y de Seguridad del SIIF NACIÓN para cumplir con las siguientes responsabilidades requeridas por esta política:

- Preservar la confidencialidad, integridad y disponibilidad de la información del SIIF NACIÓN.
- Identificar la información crítica del SIIF NACIÓN incluyendo los requerimientos de confidencialidad, integridad y disponibilidad.
- Clasificar la información del SIIF NACIÓN y definir el grupo de usuarios que deben tener acceso a ella.
- Definir los marcos de tiempo aceptables para recuperar la información y sistemas críticos del SIIF NACIÓN e identificar los impactos institucionales en caso de una interrupción extendida.
- Definir la continuidad Institucional del SIIF NACIÓN mediante planes de contingencia de continuidad del negocio y requerimientos de recuperación en caso de desastre.
- Realizar una evaluación anual de riesgos del SIIF NACIÓN para confirmar la confidencialidad, integridad y requerimientos de disponibilidad.
- Definir los requerimientos de seguridad en términos del negocio del SIIF NACIÓN para que el líder técnico del Sistema esté en capacidad de proporcionar un nivel adecuado de protección a sus documentos, datos y aplicaciones críticas de conformidad con los estándares y procedimientos de seguridad del mismo.
- Autorizar todos los privilegios de acceso a la información del SIIF NACIÓN.
- Incluir los requerimientos de seguridad de información y entrenamiento en la creación y refuerzo en la cultura en seguridad de la información, en comunicaciones regulares a los usuarios internos y externos del SIIF NACIÓN y programas de entrenamiento para los nuevos usuarios.
- Liderar la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización del SIIF NACIÓN, hasta la última instancia, incluyendo los incumplimientos a la confidencialidad o integridad de la información.

### **Responsabilidades del líder de Seguridad del SIIF NACIÓN**

El líder de Seguridad del SIIF NACIÓN deberá trabajar con el apoyo del Comité Operativo y de Seguridad del SIIF NACIÓN para cumplir con las siguientes responsabilidades requeridas por esta política:

- Formar y desarrollar los documentos operativos para el Comité Operativo y de Seguridad del SIIF NACIÓN.
- Promover y mantener un ambiente de cultura en seguridad de la información en los usuarios del SIIF NACIÓN.
- Realizar la capacitación en seguridad de la información del SIIF NACIÓN a los usuarios del SIIF NACIÓN.
- Conducir revisiones periódicas de la seguridad de la información del SIIF NACIÓN, para verificar que estén implantadas apropiadamente las políticas y normas de seguridad.
- Realizar pruebas a los planes de contingencia de continuidad del negocio y requerimientos de recuperación en caso de desastre.
- Solicitar la aprobación a las modificaciones de la Política de seguridad de la información, sus estándares, procesos y procedimientos al Comité Operativo y de Seguridad del SIIF NACIÓN.

### **Responsabilidades del líder técnico del SIIF NACIÓN**

El líder técnico del SIIF NACIÓN deberá trabajar con el apoyo de cada uno de los administradores de los componentes tecnológicos que soportan la operación del sistema para cumplir con las siguientes responsabilidades requeridas por esta política:

- Implementar controles para garantizar la seguridad física y lógica de la infraestructura que soporta la gestión, almacenamiento y procesamiento de información del SIIF NACIÓN.
- Establecer estándares, procedimientos, control de cambios y responsabilidades de administración y seguridad de cada componente tecnológico y físico que soporta la operación del SIIF NACIÓN.
- Establecer los niveles de acceso, limitar y monitorear el acceso a los datos, código fuente, equipos y demás componentes tecnológicos requeridos por el personal técnico para el desarrollo, mantenimiento, administración, operación y soporte del SIIF NACIÓN. En caso que estos niveles de acceso puedan llegar a comprometer la confidencialidad, disponibilidad o integridad

del SIIF Nación, deberá contar con la aprobación del Administrador del SIIF Nación.

- Monitorear y proyectar los requerimientos de ampliación de capacidad operativa del SIIF NACIÓN, a fin de garantizar el procesamiento y almacenamiento requerido.
- Elaborar y realizar pruebas a los planes de contingencia de recuperación en caso de desastre.
- Proporcionar un nivel adecuado de protección a documentos, datos y aplicaciones críticas de conformidad con los estándares y procedimientos de seguridad del SIIF NACIÓN.

### **Responsabilidades del Coordinador SIIF en la entidad usuaria**

Las que están establecidas en el artículo 2.9.1.1.15 del decreto 1068 del 26 de mayo de 2015.

### **Responsabilidades de los usuarios del SIIF NACIÓN**

Los usuarios son todos los funcionarios o contratistas del Estado Colombiano pertenecientes o no al Ministerio de Hacienda y Crédito Público que utilizan información del SIIF NACIÓN para hacer sus funciones, y como tales tienen responsabilidades en su cuidado.

Sus responsabilidades son las establecidas en el artículo 2.9.1.2.12, 2.9.1.2.13, 2.9.1.2.16 del decreto y en el reglamento de uso del SIIF Nación.

### **3.3 PRIVACIDAD**

Todos los usuarios con acceso a información personal almacenada o generada por el SIIF NACIÓN, son llamados a respetar dicha información. Las Direcciones del Ministerio de Hacienda y Crédito Público y las entidades usuarias del SIIF NACIÓN deben cumplir con las regulaciones colombianas emitidas al respecto.

Todo usuario o miembro del SIIF NACIÓN es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información o a los recursos del SIIF NACIÓN a personas o entidades externas.

El acceso a los datos contenidos en el SIIF NACIÓN debe ser clasificado por roles o perfiles de usuario, de tal manera que se tenga el acceso únicamente a los datos requeridos para el cumplimiento de las funciones asignadas al usuario.

El Ministerio de Hacienda y Crédito Público es responsable de la custodia de la base de datos del SIIF Nación y estará a cargo de la Administración del SIIF Nación, cumpliendo con las políticas de seguridad de la información del SIIF Nación contenidas en este documento y la normatividad colombiana vigente de reserva y protección de datos.

Los datos contenidos en la base de datos del SIIF Nación corresponden a los registrados por los usuarios del sistema y son de su responsabilidad, siendo para el uso de las entidades usuarias, órganos de dirección y administración para la gestión financiera pública de acuerdo a sus funciones. De igual manera pueden ser requeridos por los órganos de control y las autoridades judiciales en el ejercicio de sus funciones y competencias legales.

### **3.4 CAPACITACIÓN Y CONCIENTIZACIÓN**

Esta política requiere del desarrollo de un programa efectivo y continuo de capacitación, en la creación de la cultura en seguridad de la información del SIIF NACIÓN para los usuarios del SIIF Nación.

### **3.5 SEGREGACION DE FUNCIONES**

Se debe contar con una definición clara de los roles, así como del nivel de acceso y los privilegios correspondientes, para el acceso al SIIF NACIÓN y los componentes tecnológicos que soportan su operación con el fin de reducir y evitar el uso no autorizado o modificación de la información.

### **3.6 PLANEACIÓN DE CONTINUIDAD DEL SIIF NACIÓN**

Todos los procesos administrativos de la gestión financiera soportados por el SIIF NACIÓN que se hayan identificado como críticos por su disponibilidad, deberán tener un plan de continuidad de negocio completo y probado.

La administración del SIIF NACIÓN con el apoyo del Comité Operativo y de Seguridad es responsable de la preparación y prueba periódica de estos planes.

### **3.7 REPORTE DE INCIDENTES**

Se deberá desarrollar y difundir entre todos los usuarios del SIIF NACIÓN un mecanismo claro y efectivo para reportar incidentes a la seguridad de la información.

Los incidentes deben registrarse exacta y completamente, se deben tomar las acciones correctivas.

A los usuarios, internos y externos, involucrados en el incidente, se le respetará el debido proceso apropiado a cada nivel de incidente.

Los incidentes que involucren acciones legales o disciplinarias, serán remitidos a la instancia que corresponda.

### **3.8 VARIACIONES Y PÉRDIDA DE EFECTO**

Cuando por motivos de negocio o tecnológicos fuera imposible o inapropiado usar los procedimientos de protección de la información en la operación del SIIF NACIÓN, el responsable del área o Coordinador SIIF NACIÓN involucrado deberá buscar una variación y, con la concurrencia del Administrador del SIIF - NACIÓN, adoptar las alternativas que proporcionen igual o mejor nivel de protección las cuales serán sujetas de aprobación por parte del Comité Operativo y de seguridad del SIIF Nación.

### **3.9 IMPLANTACIÓN Y PROGRAMACIÓN**

Para asegurar la obtención de los objetivos que se establecen en el presente documento, esta política anticipa y autoriza el desarrollo de los procedimientos operativos detallados y otras medidas administrativas, así como el desarrollo y la adquisición de los mecanismos preventivos y reactivos, hardware, software y otras técnicas de protección.

Este programa tratará primeramente aquellos recursos de información que sean críticos y en el SIIF NACIÓN, sensibles al contenido o regulados por la ley, por el reglamento o por contrato y para los que se hayan considerado que las protecciones actuales son inadecuadas o inconclusas.

Se iniciarán programas subsecuentes y entrarán en vigor en su orden de importancia e impacto para el SIIF NACIÓN tal y como lo determine el Comité Operativo y de Seguridad del SIIF NACIÓN.

### **3.10 AUDITORIA**

El SIIF Nación podrá ser auditado por la Oficina de Control Interno y las áreas de control del Estado colombiano, los reportes relacionados con la seguridad de la información serán revisados por el Comité Operativo y de Seguridad del SIIF NACIÓN. Al igual que el estado de la implantación de las recomendaciones generadas.

### **4. APROBACION**

El comité directivo del SIIF Nación en concordancia con el literal a) del artículo 2.9.1.1.9 del Decreto 1068 del 26 de mayo de 2015, aprueba esta política de seguridad de la información del SIIF NACIÓN, para ser liberada para su publicación e implantación.

**HISTORIAL DE CAMBIOS**

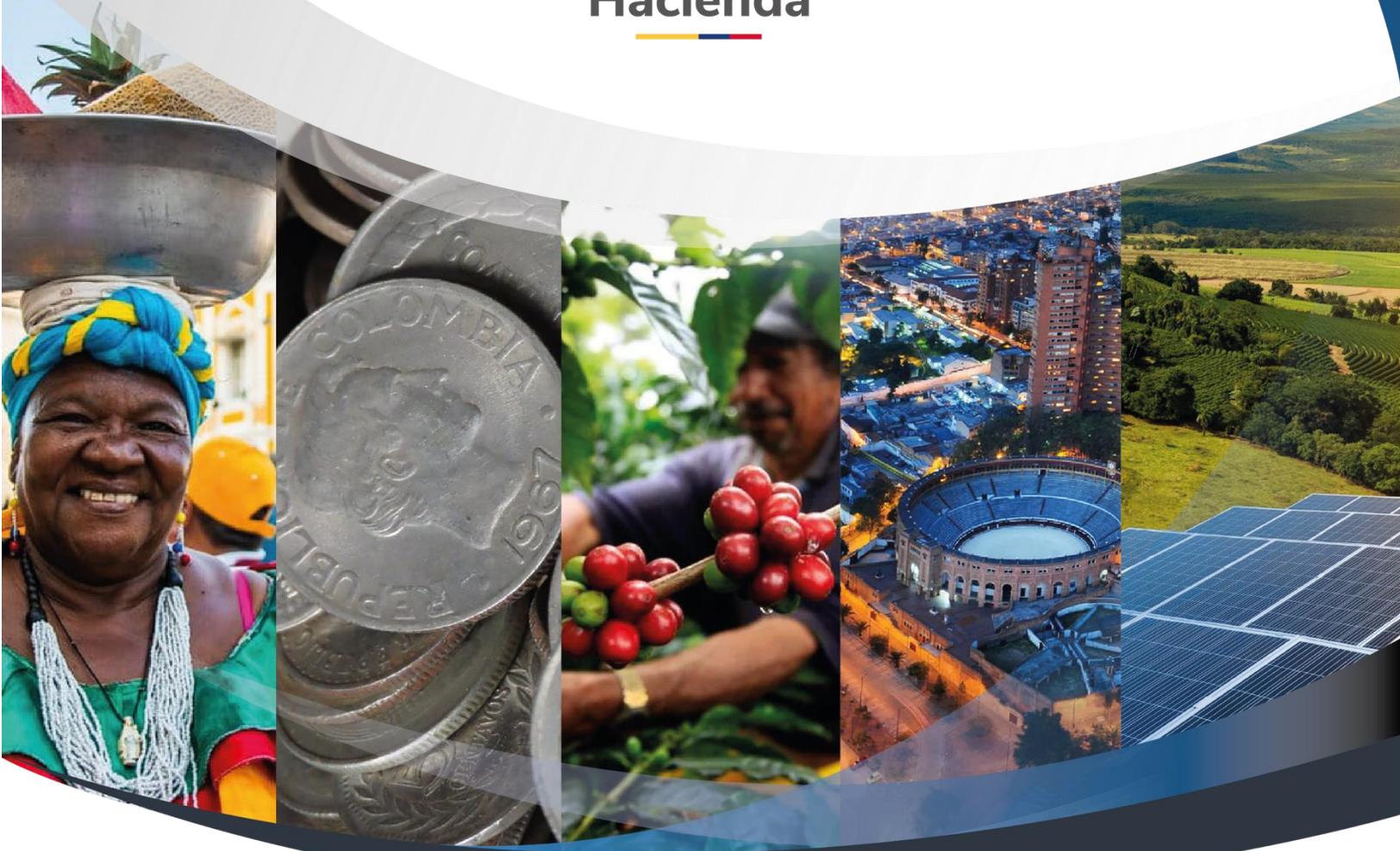
FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
03-09-2013	1	Documento aprobado en sesión ordinaria del 03 de septiembre de 2013 del Comité Directivo del SIIF Nación.
21-03-2019	2	Actualización sobre custodia de datos del SIIF Nación.

**APROBACIÓN**

<b>ELABORADO POR:</b>	<b>Nombre:</b> Administración del SIIF Nación <b>Cargo:</b> Administración del SIIF Nación <b>Fecha:</b> 21-03-2019
<b>REVISADO POR:</b>	<b>Nombre:</b> Comité Operativo y de Seguridad del SIIF Nación <b>Cargo:</b> Comité Operativo y de Seguridad del SIIF Nación <b>Fecha:</b> 21-03-2019
<b>APROBADO POR:</b>	<b>Nombre:</b> Comité Directivo del SIIF Nación <b>Cargo:</b> Comité Directivo del SIIF Nación <b>Fecha:</b> 22-08-2019



# Hacienda



## Ministerio de Hacienda y Crédito Público

Dirección: Carrera 8 No. 6C-38, Bogotá D.C., Colombia

Conmutador: (+57) 601 3 81 17 00

Línea Gratuita: (+57) 01 8000 910071

Correo: [relacionciudadano@minhacienda.gov.co](mailto:relacionciudadano@minhacienda.gov.co)

