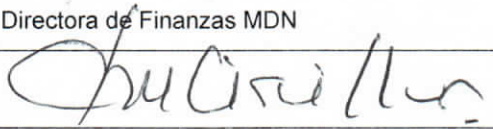
Objetivo: establecer lineamientos sobre las medidas de seguridad en el Sistema Integrado de Información Financiera SIIF Nación, para que los usuarios mitiguen los riesgos asociados en el uso del aplicativo.	
Alcance: desde medidas de seguridad Coordinador SIIF Entidad hasta el seguimiento a las medidas de seguridad. Aplica para las Unidades Ejecutoras del Ministerio de Defensa Nacional. Para los Establecimientos Públicos, Superintendencia de Vigilancia y Seguridad Privada y Policía Nacional cuando así lo requieran.	
Dependencias participantes: Dirección de Finanzas	
Elaborado por:	PD. **Johan Sebastian Reyes Alvarez** SV. **Samuel Tique Martinez**
Revisado por:	PD. **Diandra Marcela Cuestas Beltrán**
Cargo:	Coordinadora Grupo Análisis y Difusión
Firma:	
Aprobado por:	DD. **Clara Inés Chiquillo Díaz**
Cargo:	Directora de Finanzas MDN
Firma:	

HISTÓRICO DE CAMBIOS		
VERSIÓN No.	**FECHA DE EMISIÓN**	**CAMBIOS REALIZADOS**
1	07/10/2019	Emisión inicial

TABLA DE CONTENIDO

1. GENERALIDADES

El Sistema Integrado de Información Financiera SIIF Nación reglamentado mediante el Decreto 1068 del 26 de mayo de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público", lo define como "el sistema que coordina, integra, centraliza y estandariza la gestión financiera pública nacional, brindando información oportuna y confiable para garantizar una mayor eficiencia y seguridad en el uso de los recursos del Presupuesto General de la Nación y de brindar información oportuna y confiable". Las directrices para la operación segura del aplicativo, son trazadas por el Comité Operativo y de Seguridad del SIIF Nación, quien está encargado de su divulgación por parte de la Administración del Sistema, e implantación por parte de las entidades usuarias.

El Comité Operativo y de Seguridad del SIIF Nación está conformado por el Administrador del SIIF Nación, el Subdirector de Análisis y Consolidación Presupuestal de la Dirección General de Presupuesto Público Nacional DGCPPN, el Subdirector de Operaciones de la Dirección General de Crédito Público y Tesoro Nacional DGCPTN, el Subdirector de Ingeniería de Software de la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público MHCP, el Subcontador de Centralización de la Información de la Contaduría General de la Nación CGN y el Asesor de Seguridad del SIIF Nación.

El Comité Operativo y de Seguridad del SIIF Nación está encargado de proponer al Comité Directivo las políticas y estándares que constituyen el modelo de seguridad del SIIF Nación, determinar las pautas para la divulgación, implantación, complementación y mejoramiento permanente del modelo de seguridad del SIIF Nación por parte de las entidades usuarias, solicitar al Administrador del SIIF Nación informes de seguimiento sobre el modelo de seguridad del sistema y evaluar el informe anual de riesgos del SIIF Nación presentado por el Administrador del aplicativo, entre otros.

En las Unidades Ejecutoras, el Coordinador SIIF es el responsable de la creación y administración de usuarios, procesos operativos, de seguridad, de la implantación de las medidas de seguridad señaladas por el Comité de Seguridad y por su parte, los usuarios del Sistema SIIF Nación quienes efectúan las consultas y registros de la gestión financiera en el aplicativo, son los encargados de cumplirlas.

Igualmente y en cumplimiento con lo establecido en la Directiva Permanente "Políticas para el cierre de vigencia fiscal e inicio de la nueva vigencia", se indica que las Inspecciones Generales de las Unidades Ejecutoras, las Oficinas de Control Interno de las Unidades Ejecutoras, los Establecimientos Públicos y la Policía Nacional, deben evaluar y efectuar seguimiento a los lineamientos establecidos en las medidas de seguridad, así como presentar ante la Dirección de Finanzas del Ministerio de Defensa Nacional MDN al inicio de la vigencia fiscal, a más tardar en el mes de febrero, el informe de seguimiento y monitoreo a las medidas de seguridad adoptadas para el SIIF Nación.

Por lo anteriormente expuesto, se hace necesario recabar las Medidas de Seguridad a tener en cuenta en forma permanente por parte del Coordinador SIIF Nación Entidad y los usuarios del Sistema SIIF Nación, en cuanto a los certificados de firmas digitales (TOKEN), la infraestructura tecnológica, los equipos de cómputo, las claves de acceso, la administración de usuarios, el pago a beneficiario final, perfiles y cómo se debe efectuar seguimiento a las mismas.

Cada vez que se presente cambio de Coordinador SIIF Entidad, Delegado, Registrador Usuarios o Soporte Técnico o cuando ingrese un usuario nuevo al Sistema SIIF Nación, se le debe dar a conocer, a la persona que recibe las funciones de estos cargos, la información contemplada en esta Guía.

NOTA 1: informar al Administrador SIIF del cambio de Coordinador SIIF Entidad, Delegado y Soporte Técnico, mediante los formatos que el MHCP tiene establecido para tal fin, e informar a la Dirección de Finanzas del MDN, remitiéndole una copia del formato al correo corporativo finanzas@mindefensa.gov.co, con el fin de actualizar los datos y garantizar que los correos enviados por esta Dirección lleguen al Coordinador SIIF y este se encargue de su difusión dentro de la Unidad y Subunidades Ejecutoras.

Las Oficinas de Control Interno en su rol Control Entidad, pueden hacer seguimiento a la gestión financiera consultando la Guía Financiera No. 56 “Reportes y consultas para seguimiento y auditoria de la actividad financiera”, elaborada por esta Dirección para este efecto.

2. FLUJOGRAMA

No Aplica.

3. DESARROLLO TRANSACCIONAL

No aplica.

4. MEDIDAS DE SEGURIDAD SISTEMA INTEGRADO DE INFORMACIÓN FINANCIERA SIIF NACIÓN

Con el propósito de garantizar la integridad de la información financiera registrada dentro del aplicativo SIIF Nación, a continuación, se dan a conocer aquellas disposiciones que se deben considerar en los diferentes aspectos, para prevenir riesgos y garantizar la óptima utilización del Sistema SIIF Nación. Es pertinente manifestar, que la información registrada en el Sistema SIIF Nación tiene carácter oficial.

4.1 Medidas de seguridad Coordinador SIIF Entidad

Estas medidas son aplicables tanto al Coordinador SIIF, como al Delegado en cada Unidad Ejecutora, así:

1. Implementar y cumplir las políticas y estándares de seguridad del Sistema SIIF Nación señaladas por el Comité de Seguridad, de conformidad con lo establecido en el artículo 2.9.1.1.15 del Decreto 1068 del 26 de mayo de 2015.

2. Responder por la creación de usuarios en el Sistema SIIF Nación, en la respectiva Unidad Ejecutora.

3. Designar una persona a quien se le asigne la cuenta de usuario con perfil “Registrador Usuarios”, quien será el responsable de registrar en el sistema las solicitudes de creación y modificación de los usuarios de la entidad,

autorizados por el Coordinador SIIF de la Entidad. Así mismo, realizar el trámite oportuno para designar uno que lo sustituya en caso de ausencia temporal o definitiva del mismo.

4. Velar porque se provean los recursos tecnológicos necesarios en cada Unidad y Subunidad Ejecutora, para que los usuarios tengan acceso al Sistema SIIF Nación, de acuerdo con los requisitos exigidos por el MHCP.

5. Firmar las solicitudes de creación y administración de usuarios.

6. Garantizar que toda persona a la cual se le crea una cuenta para el acceso al SIIF Nación, sea capacitada en el uso del aplicativo de acuerdo a las funciones a desempeñar.

7. Verificar que cada usuario que acceda al aplicativo tenga una cuenta de correo institucional.

8. Podrá autorizar la asignación de más de un perfil siempre y cuando no exista incompatibilidad entre perfiles y corresponda a las funciones asignadas.

9. Realizar supervisión a las cuentas de los usuarios en el aplicativo a fin de verificar las que deben estar activas y aquellas que deben ser inhabilitadas teniendo en cuenta las solicitudes realizadas por los usuarios.

10. Definir mecanismos de protección apropiados, los cuales garanticen que sólo debe acceder al Sistema SIIF Nación el personal autorizado, vinculado a la Unidad o Subunidad Ejecutora y que requiera utilizar el sistema para el cumplimiento de sus funciones.

11. Tramitar oportunamente las novedades de usuarios cuando le sean cambiadas las funciones o se retiren temporalmente o permanentemente de la Unidad o Subunidad Ejecutora, tanto en el Sistema SIIF Nación, como a las entidades certificadoras.

12. Velar para que sea verificada en forma periódica la fecha de expiración de los usuarios y de los correspondientes certificados de firmas digitales, así como efectuar los registros de actualización de la fecha en el sistema, con el fin de actualizarlas oportunamente y evitar que se desactiven en fecha críticas, con el fin de garantizar el acceso al Sistema SIIF Nación.

13. Administrar eficaz y eficientemente la asignación de los certificados de firmas digitales para su óptima utilización.

14. Adelantar el proceso de contratación de los certificados de firmas digitales (TOKEN) en forma oportuna, para garantizar la disponibilidad de los mismos y su respectiva renovación (control de expiración). Para el proceso de adquisición de Certificado de Firma Digital – Función Pública (TOKEN) es importante tener en cuenta las especificaciones técnicas definidas en la Circular Externa 004 del 26 de enero de 2017 emitida por el administrador SIIF del MHCP “Firma digital en el aplicativo SIIF Nación”.

15. Reasignar el certificado de firma digital a otro funcionario (adelantando los trámites pertinentes ante la entidad certificadora) en caso de evidenciar que no está siendo utilizado por cambio de funciones o retiro de la entidad.

16. Replicar oportunamente a los usuarios del SIIF Nación, todas las comunicaciones emitidas e informadas tanto por el Administrador del Sistema como por la Dirección de Finanzas del MDN, para que se tenga pleno conocimiento de las acciones a realizar en el sistema SIIF Nación, tanto en el nivel central como en sus respectivas Subunidades.

17. Mantener un archivo documental físico o virtual de los usuarios creados y modificados en el Sistema SIIF Nación.

18. El usuario con el perfil "Registrador de usuarios" debe estar inscrito en la sede electrónica del MHCP para dar trámite a las solicitudes relacionadas con la creación de cuentas de usuarios del sistema, así como la creación y modificación de los usuarios que tengan asignado el perfil ESP- Control Consulta, administración de perfiles y la administración de Coordinadores SIIF Nación.

    (Para mayor información en cuanto al registro en la sede electrónica MHCP, ingrese al portal web www.minhacienda.gov.co/Portales/ Sistema Integrado de Información Financiera SIIF Nación/Ciclo de negocios/ Administración de Usuarios/Guía para Radicación de documentos Admin. Usuarios)

19. Registrar en el sistema SIIF Nación las solicitudes de creación de cuenta de usuario si se allegaron los respectivos soportes documentales mediante correo electrónico a atencioncliente@minhacienda.gov.co, los cuales deberán ser remitidos en un lapso no mayor a tres (3) días hábiles a la Administración SIIF Nación una vez realizada la solicitud en el aplicativo; de no enviarse oportunamente el MHCP a rechazará la solicitud y será necesario reiniciar el trámite.

20. Brindar soporte funcional a los usuarios creados en el aplicativo SIIF Nación de la respectiva Unidad, así mismo, coordinar soporte técnico con la respectiva área de sistemas de la Unidad o Subunidad Ejecutora.

4.2 Medidas de seguridad usuarios SIIF Nación

Es importante dar a conocer las siguientes medidas de seguridad al personal civil y militar que se les asigne cuenta de usuario en el Sistema SIIF Nación y se debe velar por su cumplimiento, estas son:

1. Como usuario del SIIF Nación, debe conocer y aplicar el reglamento de uso del sistema[1], por lo tanto es responsabilidad del usuario el uso adecuado que le dé al Sistema SIIF Nación.

2. Al recibir la cuenta de acceso al sistema SIIF Nación, el usuario debe conocer las responsabilidades e implicaciones de la aceptación de la cuenta de usuario que firma cuando realiza la solicitud de creación de cuenta de usuario. Así mismo, aceptar que es para su uso personal e intransferible; que la información a la que tiene acceso en el sistema es utilizada exclusivamente para el cumplimiento de sus funciones y que conoce las medidas de seguridad respecto al uso del sistema.

3. Asumir la responsabilidad de todos los registros que se hagan en el sistema con su cuenta de usuario.

[1] Reglamento de uso del SIIF Nación del Ministerio de Hacienda y Crédito Público (Aprobado en sesión ordinaria del 26 de febrero de 2013, acta No. 16).

4. El usuario debe conocer los conceptos teóricos relacionados con las funcionalidades a utilizar en el Sistema SIIF Nación.

5. El usuario del Sistema SIIF Nación es responsable por la consistencia, veracidad, oportunidad, confiabilidad, confidencialidad e integridad de los datos registrados en el sistema con su cuenta de usuario y su certificado de firma digital y las implicaciones disciplinarias y legales serán asumidas por el titular de la cuenta de usuario, así como tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

6. Debe mantener la reserva de la información a la que tienen acceso, ya que ésta debe ser utilizada exclusivamente para el cumplimiento de sus funciones. Es una falta Gravísima permitir que personas no autorizadas tengan acceso a información oficial.

7. El usuario debe cuidar la información a la que tiene acceso y evitar su destrucción o utilización indebida. No debe alterar, falsificar, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permita el acceso a ella a personas no autorizadas.

8. Los niveles de acceso al sistema deben estar directamente relacionados con la función que debe realizar cada usuario, de tal manera que se tenga el acceso únicamente a las transacciones requeridas para el cumplimiento de las funciones asignadas a cada usuario, en caso contrario, el jefe inmediato del usuario deberá solicitar al Coordinador SIIF realizar las restricciones correspondientes.

9. El usuario es responsable por el uso de las claves y firmas digitales asignadas. La clave de acceso al Sistema SIIF Nación es personal e intransferible, cuando el usuario la reciba por primera vez debe modificarla inmediatamente.

10. En cuanto a la contraseña, el usuario debe recordar que ésta debe ser modificada cuando el sistema lo solicite y antes de su vencimiento, de lo contrario el usuario será bloqueado por el sistema; por otra parte, el certificado de firma digital debe renovarse con la debida antelación con el fin de no generar traumatismos en el desarrollo de sus funciones. Igualmente, las contraseñas no deberán ser reveladas a otros usuarios.

11. Cuando le sean cambiadas las funciones o se retire temporalmente (vacaciones, licencias, incapacidades) o permanentemente de la Unidad o Subunidad Ejecutora o cualquier evento que le impida hacer uso del sistema, es obligación del usuario SIIF Nación informar la novedad y remitir el formato establecido para la modificación o eliminación, según sea al caso, al Coordinador SIIF Nación Entidad y/o al Registrador para que haga la solicitud de inactivación o eliminación de la cuenta en el Sistema SIIF Nación.

12. Informar a la Administración SIIF Nación sobre cualquier irregularidad en el uso del sistema.

13. Acatar las instrucciones y procedimientos establecidos por la Administración SIIF Nación y el Comité Operativo de Seguridad.

14. Respetar los derechos de autor del MHCP sobre los documentos y material publicado para el uso del sistema, siendo de uso privado y sin fines de lucro, así como las publicaciones realizadas por la Dirección de Finanzas del MDN.

15. Al usuario que se le asigne certificado de firma digital (TOKEN), le sean modificadas las funciones y por lo tanto no requiera hacer uso del dispositivo de criptográfico, dentro de un máximo de cinco días hábiles después de este hecho, deberá tomar contacto con el Registrador de usuarios SIIF Nación quien de acuerdo a la vigencia del dispositivo lo reasignará o le indicará lo que debe realizar.

16. Es responsabilidad de todo usuario del aplicativo conocer las políticas, normas, procedimientos y documentos divulgados por la Administración del SIIF Nación del MHCP, así como de las diferentes Guías Financieras emitidas por la Dirección de Finanzas del MDN, para el uso eficaz, eficiente y seguro del SIIF Nación.

17. Se considera falta gravísima alterar o introducir información que afecte el normal funcionamiento en el sistema (artículo 62 numeral 5 de la ley 1952 de 2019). Las irregularidades en estos registros deberán ser reportadas a las autoridades competentes (jefe inmediato, Oficina de Control Interno o su equivalente, Administrador SIIF del MHCP).

18. Es responsabilidad del funcionario mantener activo y habilitado el usuario asignado del SIIF Nación, para tal fin el aplicativo muestra un mensaje informativo sobre la fecha de expiración de la cuenta de usuario con treinta (30) días de antelación, por tanto, el usuario debe gestionar ante el Coordinador SIIF de la respectiva Unidad y Entidad, la ampliación de dicha fecha. Los usuarios que no utilicen el aplicativo del SIIF Nación en un lapso de quince (15) días serán expirados para lo cual deberá tramitar una solicitud de modificación de su cuenta de usuario, en el evento de que no ingrese al aplicativo durante tres (3) meses, será eliminado del mismo automáticamente. Si se requiere nuevamente su creación, el usuario tramitará la solicitud de creación cuenta de usuario ante el Coordinador SIIF de la Entidad quién deberá seguir el procedimiento para tal fin.

19. El usuario del SIIF debe registrar la gestión financiera pública en línea, tiempo real y en forma oportuna acorde con la operación realizada.

20. Debe dar cumplimiento a lo establecido en el decreto 1068 de 2015 y a los reglamentarios que expida el Comité Directivo del SIIF Nación del MHCP y acatar las instrucciones que expida la Administración del Sistema SIIF Nación, para el buen uso de la aplicación.

21. El usuario tiene derecho a:

    - Recibir un trato respetuoso del personal a cargo de la Administración de SIIF Nación.
    - Recibir asistencia funcional y técnica en cuanto al uso del aplicativo.
    - Recibir de parte de la Coordinación SIIF de la entidad, la capacitación requerida para el uso del aplicativo en la funcionalidad en la cual se va a desempeñar.
    - Solicitar a la Administración del SIIF Nación, el estado en que se encuentren las solicitudes de servicio que realice en la mesa de ayuda del MHCP.
    - Recibir respuesta de la Administración SIIF sobre las solicitudes de servicios realizadas.

- Utilizar para el ejercicio de sus funciones y uso del aplicativo la documentación y material publicado tanto por la Administración del SIIF Nación del MHCP, como por la Dirección de Finanzas del MDN.

4.3 Medidas de seguridad para el ingreso al sistema

Con el propósito de mantener los estándares de seguridad en materia de autenticidad en el Sistema SIIF Nación, los usuarios que están autorizados para ingresar al sistema deben autenticarse indicando el usuario y la contraseña, utilizando el teclado virtual del Sistema SIIF Nación.

Una vez el usuario se autentica, se muestra una página con los "Términos y condiciones de uso del SIIF Nación" en el que solicita al usuario la aceptación de los términos del uso del aplicativo, cuyo marco está establecido en el Decreto 1068 de 2015, el reglamento de uso del sistema y el Código Único Disciplinario.

Los Términos y condiciones de uso del SIIF Nación se describen a continuación:

> *"Usted, "usuario", identificado con el documento número "Nro de documento", está ingresando al Sistema SIIF Nación propiedad del Ministerio de Hacienda y Crédito Público, en nombre de la entidad Unidad Ejecutora "Nombre de la Unidad Ejecutora" ("Código de la Unidad").*
>
> *El ingreso a este sistema solo está permitido a usuarios autorizados, la utilización por usuarios no autorizados está prohibida. El uso no autorizado o inapropiado de este sistema puede causar sanciones disciplinarias y/o acciones civiles y penales.*
>
> *Al utilizar esta cuenta de acceso al SIIF Nación, el usuario acepta que la cuenta de usuario y su contraseña de acceso es para su uso personal e intransferible, que la información a la que tiene acceso es utilizada exclusivamente para el cumplimiento de sus funciones u objeto del contrato, que los registros realizados en el SIIF Nación con esta cuenta de usuario, son de su entera responsabilidad, para tal fin deberá observar lo dispuesto en las políticas de seguridad del SIIF Nación y su reglamento de uso, y en los artículos 38 y 39 de la ley 1952 del 28 de enero del 2019, so pena de incurrir en las faltas consagradas en el libro II, Título único, Capítulo 1 del mismo código.*
>
> *Es de obligatorio cumplimiento por parte del usuario solicitar al Coordinador SIIF de la entidad usuaria la eliminación inmediata de esta cuenta cuando por licencias de un período igual o superior a tres meses, cambio de funciones o retiro definitivo, no necesite hacer uso del sistema. Si usted no es la persona arriba identificada no ingrese al sistema."*

Los usuarios del SIIF Nación son servidores públicos por lo que les aplica la ley 734 de 2002 "Por la cual se expide el Código Disciplinario Único", en especial los artículos 34 y 35, y las faltas consagradas en el libro II, Título único, Capítulo 1 del Código en mención.

4.4 Medidas de seguridad en los TOKEN y certificados digitales

En el Sistema SIIF Nación el certificado de firma digital es utilizado para firmar digitalmente todas las transacciones, permitiendo identificar a la persona que realiza los registros y genera las diferentes consultas y/o reportes, garantizando la autenticidad e integridad de los datos ingresados al aplicativo.

Los Certificados de Firmas Digitales utilizados en el SIIF Nación son del tipo Función Pública (es decir para el ejercicio de funciones públicas por parte de un servidor público), emitidos por una entidad Certificadora, con fundamento en la ley 527 de 1999 "*por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones*", modificado por el decreto ley 19 de 2012 en sus artículos 160 al 163, reglamentada mediante el Decreto Único Reglamentario 1074 de 2015 y demás normas legales vigentes. Este certificado de firma digital contiene datos de la persona y de la empresa en la que labora y son utilizados para comprobar su identidad, sirve aún para identificarse ante terceros y previene suplantación de la identidad en los Sistemas de Información.

El uso de una firma digital, según lo establecido en el Parágrafo único Art 28 Ley 527 de 1999, tendrá la misma fuerza y efecto que el uso de una firma manuscrita, aquélla incorpora los siguientes atributos:

a. Es única a la persona que la usa,
b. Es susceptible de ser verificada,
c. Está bajo el control exclusivo de la persona que la usa,
d. Está ligada a la información o mensaje, de tal manera que, si éstos son cambiados, la firma digital es invalidada, y
e. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

Los certificados digitales a utilizar en el sistema SIIF Nación, están almacenados en dispositivos denominados "TOKEN Criptográficos", los cuales protegen el acceso no autorizado al certificado digital.

Las áreas de sistemas deben tener en cuenta lo dispuesto en la "Guía para Actualizar componente de firma digital" dispuesta por el MHCP en la ruta www.minhacienda.gov.co / SIIF Nación / Información de soporte / aspectos técnicos.

De acuerdo con las funciones y las transacciones a utilizar en el Sistema SIIF Nación, se le asigna al funcionario que lo requiere un certificado de firma digital (TOKEN), el funcionario debe conocer las medidas de seguridad a tener en cuenta para su uso, las responsabilidades e implicaciones de la aceptación del certificado digital de acuerdo con las políticas que el suscriptor autorizado haya pactado con la Entidad contratante; a continuación, se menciona algunas políticas a tener en cuenta:

1. El usuario debe consultar la "Declaración de prácticas de Certificación" expedida por la entidad certificadora que emite el certificado digital.

2. El certificado de firma digital – función pública será emitido por la firma certificadora, la cual hará entrega del mismo a través de envío por correo certificado que será entregado de forma personal únicamente a quien se le haya emitido.

3. El usuario al que se le asigna el certificado es el responsable de vigilar, salvaguardar y cuidar que sea utilizado debida y racionalmente, de conformidad con los fines a que han sido destinados. Así mismo, por la custodia, tenencia y conservación del mismo, razón por la cual debe tenerlo siempre en su poder o almacenarlo de manera segura y no permitir el acceso o uso del Dispositivo a otros usuarios.

4. No dejar el certificado de firma digital (TOKEN) conectado al computador, mientras se ausente del puesto de trabajo.

5. El certificado de firma digital es emitido a nombre del usuario, su clave de acceso (PIN) es personal e intransferible. No se debe prestar ni compartir la contraseña de acceso con ninguna persona.

6. Se debe memorizar la CLAVE y no permitir que otras personas la conozcan. La clave es la protección del certificado digital almacenado en el TOKEN y únicamente puede ser cambiada por el suscriptor del certificado.

7. No se debe digitar la clave más de 3 (tres) veces de manera errada, porque bloquea el acceso.

8. El certificado de firma digital debe ser utilizada para consultar y firmar digitalmente las transacciones y la carga de archivos planos en el Sistema SIIF Nación. No se debe someter el TOKEN al contacto con sustancias líquidas, consideraciones extremas de temperatura o humedad que puedan afectar su correcto funcionamiento.

9. El usuario del SIIF Nación que se retire de la Unidad o Subunidad Ejecutora o que por cambio de funciones deje de ser usuario del aplicativo, debe tomar contacto con el Coordinador SIIF o el registrador de usuarios de la respectiva Unidad, para determinar el proceso de entrega del dispositivo de firma digital (TOKEN).

10. En caso que el certificado de firma digital esté próximo a vencer y se requiera su renovación, el usuario deberá tomar contacto con el registrador de usuarios de la respectiva Unidad, para indicarle el trámite correspondiente.

11. Los certificados de firma digital (TOKEN) deben inventariarse, por cuanto son objetos devolutivos. Cuando se termine la vigencia del certificado se debe realizar la devolución (previa coordinación con el registrador de usuarios de la entidad) y realizar las gestiones pertinentes indicadas en el Manual de Procedimientos administrativos y financieros para el manejo de bienes del MDN, emitido por la Dirección de Finanzas del MDN.

12. El usuario es responsable de las transacciones que se firmen o ejecuten con su certificado digital, por lo tanto, es responsable disciplinaria, administrativa, fiscal y penalmente por el uso indebido del certificado.

13. Los usuarios del SIIF Nación que tengan asignado el uso, custodia o administración de un certificado de firma digital a su cargo, son responsables de la pérdida o daño que sufran, cuando no se ocasione por el deterioro natural, por su uso normal o por causa justificada.

14. El usuario es responsable de la pérdida, daño, deterioro, bloqueo o mal uso del certificado de firma digital - TOKEN, de presentarse alguna de estas situaciones, debe contactarse con el Coordinador SIIF Nación Entidad de la respectiva Unidad para la revocación del certificado en forma inmediata. De acuerdo con los lineamientos establecidos en el manual de procedimientos administrativos y financieros para el manejo de bienes del Ministerio de Defensa Nacional la responsabilidad por pérdida, daño, deterioro, disminución, mal uso de bienes, se determinará a través de los procesos que establezcan las normas vigentes que rigen la materia.

4.5 Medidas de seguridad infraestructura tecnológica

El Sistema Integrado de Información Financiera SIIF Nación es un sistema centralizado, soportado sobre una solución WEB administrada por el MHCP. Los usuarios de las entidades accederán al SIIF Nación por medio un Portal Seguro, que a su vez crea una Red Virtual Privada (VPN SSL) donde los datos viajan encriptados y cifrados a través de Internet o la Intranet Gubernamental (GNAP), de esta manera se garantiza que los datos no puedan ser descifrados, leídos o modificados durante su transmisión. Las medidas de seguridad contempladas en este numeral, están a cargo de la Oficina de Informática o Sistemas en cada Unidad o Subunidad Ejecutora:

A continuación, se dan a conocer las medidas de seguridad a tener en cuenta en la infraestructura tecnológica y los documentos dispuestos por el MHCP para orientar en este proceso, los documentos que a continuación se relacionan pueden ser consultados por la ruta: www.minhacienda.gov.co / SIIF Nación / Pestaña Aspectos Técnicos :

1. Documento “Lista de Chequeo para las Entidades” dispuesto por el MHCP el cual tiene como objetivo orientar a los soportes técnicos de cada entidad para que mantenga actualizada las configuraciones que requiere tener la entidad para poder operar el aplicativo SIIF Nación.

2. Documento “Lineamientos para Establecer el Ancho de Banda para Acceder al SIIF Nación”, donde los administradores de las redes de datos encontrarán algunas consideraciones a tener en cuenta en la definición de las necesidades reales de Ancho de Banda.

3. Documento “Esquema de Interconexión para acceder al SIIF Nación” donde los administradores de las redes de datos encontrarán los esquemas de interconexión que deben tener las entidades para acceder al Sistema SIIF Nación.

4. Manual Técnico VPNSSL donde se indican las configuraciones requeridas para acceder al Sistema SIIF Nación a través de una conexión de VPNSSL – Terminal Server.

5. Documento “Recomendaciones Configuración Entidades” donde se encuentran las recomendaciones de configuración en los servidores para que se pueda acceder al SIIF Nación.

6. Documento “Actualización Conectividad” donde se encuentran las instrucciones que debe que se deben realizar al interior de cada Unidad y Subunidad Ejecutora con el fin de habilitar el acceso a SIIF Nación.

7. Para temas de contingencia, tener en cuenta el documento “Canal de Contingencia” en el cuál se explica la manera de realizar el cambio de enlace en caso de que el canal principal (el del MHCP) no esté en servicio.

8. La conexión al Sistema SIIF Nación se debe realizar en la medida de las posibilidades a través de GNAP, ya que, por ser una red privada no se tiene acceso al público reduciendo los ataques informáticos, además que cuenta con VPNs con una llave de encriptación de 128bit para proteger los datos que ahí se transmiten.

9. El canal de comunicaciones debe estar disponible en un 50% como mínimo para que no se presenten problemas de saturación del mismo, y por consiguiente un mejor desempeño de la solución SIIF Nación.

10. Canal de Contingencia definido por el Administrador SIIF Nación y que se encuentra contemplado en la página web del MHCP, link SIIF Nación / Soportes Técnicos/ Documento SIIF – Canales de Contingencia para SIIF Nación, documento en el cuál se explica la manera de realizar el cambio de enlace en caso de que el canal principal (el del MHCP) no esté en servicio.

11. La Unidad debe garantizar la seguridad en las comunicaciones.

12. Los Usuarios SIIF Nación deben estar conectados a una red switchada.

13. Los enlaces que la Unidad Ejecutora usuaria del SIIF Nación tenga contratados con terceros para transportar información desde y hacia sus regionales, deben proveer el servicio de cifrado.

14. Para tramos contratados no cifrados se debe implementar cifrado sitio a sitio (site to site) a nivel de los enrutadores que posea la Unidad usuaria de SIIF Nación.

15. Si se contrata el cifrado de los enlaces con el carrier, se debe solicitar la administración de las llaves de cifrado y los dispositivos utilizados en esa labor.

16. Las Unidades Ejecutoras usuarias de SIIF Nación que tengan conectadas Subunidades deben garantizar al menos los mismos niveles de seguridad a los provistos por el MHCP.

17. Realizar las configuraciones que recomienda implementar el MHCP en cada componente de la infraestructura informática de la Unidad.

4.6 Medidas de seguridad en los equipos de cómputo

Las medidas de seguridad contempladas en este numeral, están a cargo de la Oficina de Informática o Sistemas en cada Unidad o Subunidad Ejecutora:

1. Las áreas de sistemas o informática deben tener en cuenta el “instructivo Configuración Clientes” dispuesto por el MHCP en la ruta www.minacienda.gov.co / SIIF Nación / Pestaña aspectos técnicos. En este documento se encuentran los requerimientos técnicos que debe cumplir un equipo cliente que va a usar SIIF Nación.

2. Cada Unidad Ejecutora debe tener un contacto técnico para dar soporte a sus usuarios, en la configuración de requisitos para la operación del sistema y para la solución de incidentes.

3. Se debe garantizar que las políticas de seguridad interna no interfieran en el funcionamiento del SIIF Nación.

4. Las Unidades Ejecutoras que se encuentran localizadas en Bogotá deberán contar con la Intranet Gubernamental (GNAP) como canal principal para acceder al SIIF Nación.

5. Se deben disponer políticas de claves fuertes para dichas estaciones de trabajo.

6. Los equipos deben estar ubicados en condiciones ambientales adecuadas para su correcto funcionamiento.

7. Los equipos asignados a SIIF Nación deben estar incluidos dentro de los planes de mantenimiento preventivos y correctivos de la Unidad o Subunidad Ejecutora usuaria de SIIF Nación, así mismo, deben contar con software y antivirus los cuales deben ser institucionales y estar permanentemente actualizados.

8. En caso que se utilicen equipos portátiles como estaciones usuarias del aplicativo, se debe cumplir en éstos todos los requisitos expuestos en los numerales anteriores.

9. Se debe realizar la configuración óptima que le permita percibir un mejor desempeño del aplicativo SIIF Nación.

10. Todo computador que accede al SIIF Nación debe tener habilitado el protector de pantalla con clave personal, que se active máximo a los cinco minutos de no ser utilizado.

11. Una vez se haya ingresado al Sistema SIIF Nación, no se debe dejar la terminal con el aplicativo activo, cuando el usuario no lo esté usando o no esté presente en su puesto de trabajo, para evitar el registro de información a personas no autorizadas.

12. Se deben adelantar las configuraciones dispuestas por el MHCP para el Navegador Internet Explorer.

13. Deben existir procedimientos formales para la administración y configuración de los equipos que se van a utilizar para la funcionalidad del Sistema SIIF Nación.

14. La lógica de negocio de generación y verificación de firma digital del SIIF Nación esta implementada con una tecnología llamada Java, para la cual es necesario garantizar que las estaciones de trabajo de los usuarios del sistema tengan instalada la última versión de esta plataforma tecnológica.

15. Antes de firmar digitalmente las transacciones en el Sistema SIIF Nación o realizar cargas masivas de datos, es necesario tener instalado previamente el controlador o driver del TOKEN.

16. No se deben realizar transacciones en línea con el SIIF Nación desde computadores o lugares públicos, como cafés Internet. No está permitido configurar el aplicativo de SIIF Nación en computadores de uso personal distintos a los asignados en el lugar de trabajo, de hacerlo, es responsabilidad del usuario la pérdida de integridad, confidencialidad, seguridad de la información y deberá asumir las implicaciones disciplinarias y legales que pueda acarrear.

17. Para ingresar al sitio Web del aplicativo SIIF Nación siempre se debe usar la página indicada por la Administración del SIIF Nación.

4.7 Medidas de seguridad con las contraseñas

Los usuarios a los que se les asigne cuenta en el sistema, deben conocer previamente las consideraciones a tener en cuenta en el manejo de las contraseñas. A continuación, se relacionan las medidas de seguridad para el uso de las mismas, así mismo, se recomienda revisar la guía de entrada al sistema publicada por el MHCP en la ruta www.minhacienda.gov.co/ SIIF Nación/Ciclo de negocios/Administración de Seguridad:

1. Para acceder al Sistema SIIF Nación, el titular de la cuenta de usuario debe utilizar la contraseña de acceso. La cuenta de usuario y contraseña, se utilizan como mecanismo de autenticación en el aplicativo.

2. La contraseña es confidencial e intransferible y estrictamente personal, por cual se asumirá que cada vez que se ingrese al SIIF Nación con dicha contraseña, es el titular de la cuenta de usuario quien lo está haciendo, por tanto, los registros que se hagan a nombre de su cuenta de usuario, son de su absoluta responsabilidad.

3. Usar el teclado virtual para escribir las vocales mayúsculas y minúsculas y los números. La ubicación de cada número en el teclado virtual se muestra cada vez en un sitio distinto. Al acercar el cursor al teclado todos los números aparecen con el símbolo *. Para ver los números es necesario alejar el cursor fuera del teclado virtual.

4. El teclado convencional se utiliza para el ingreso de las consonantes mayúsculas, minúsculas y para los símbolos.

5. En el teclado virtual no es posible pegar la contraseña, es necesario ingresarla.

6. El sistema exige cambio de contraseña:

   - ✓ Cuando el usuario es nuevo e ingresa por primera vez al sistema.
   - ✓ A los treinta días de haber cambiado la contraseña.

- Para cambiar la contraseña se debe tener en cuenta que ésta debe tener como mínimo ocho (08) caracteres, debe efectuar la combinación de consonantes, vocales, números, mayúsculas, minúsculas y al menos un carácter especial como: @, ?, -, no usar ninguna de las últimas cinco contraseñas ya utilizadas.

7. No utilizar contraseñas triviales, es decir, comunes y que sean de fácil acceso, como, por ejemplo: fechas de eventos especiales.

8. No usar nombres o palabras completas o que se encuentren en un diccionario.

9. No usar letras o números consecutivos del teclado o que sigan un patrón en el teclado, por ejemplo: poiuy9874.

10. Se debe memorizar la contraseña y nunca compartirla con otras personas.

11. Se debe evitar digitar la contraseña en el Sistema SIIF Nación delante de otras personas.

12. El usuario es el responsable de la correcta utilización de la clave de acceso asignada; en caso de olvido o bloqueo de la respectiva contraseña, el sistema permite a usuarios activos, habilitados y no expirados restablecer la contraseña de acceso, ingresando a la página de acceso del SIIF Nación a través de la dirección www.minhacienda.gov.co y atendiendo las siguientes instrucciones:

    12.1. Ubicar en el menú "Portales" la opción portal Sistema Integrado de Información Financiera - SIIF Nación.
    12.2. Dar clic en acceso. Una vez dado el clic para acceder al sistema, se mostrará las recomendaciones para el uso seguro del sistema y las formas de acceso disponibles.
    12.3. *Conectar el certificado de firma digital al computador en el cual está accediendo.*
    12.4. Seleccionar de la opción "Usuarios externos – Recupera contraseña".

        12.4.1. El sistema le solicitará que se autentique utilizando el certificado digital almacenado en el TOKEN criptográfico, para lo cual debe digitar el PIN de acceso.
        12.4.2. Una vez digitado el PIN correcto, se mostrará la pantalla de solicitar los datos para restaurar la contraseña.
        12.4.3. Diligenciar todos los datos solicitados, seleccionando "Aceptar los términos y condiciones" y luego dar clic en el botón "Restaurar Contraseña".
        12.4.4. En caso que algunos de los datos solicitados no sean correctos, o el usuario no cumpla los requisitos para la contraseña, el sistema mostrará el mensaje de acceso no autorizado.
        12.4.5. Si todos los datos solicitados son correctos se mostrará la página de ingreso al sistema para que acceda con la nueva contraseña.

13. Por ningún motivo un usuario debe aceptar una cuenta de usuario con una contraseña diferente a la enviada a través del correo institucional.

14. No escribir la contraseña en un papel o medio que deje a la vista o fácil acceso de otras personas.

15. Cambiar la contraseña de acceso al Sistema SIIF Nación cuando el sistema lo solicite y antes de que se venza.

16. La contraseña se vence cada treinta (30) días, es importante cambiarla antes del último día del vencimiento, dado que el aplicativo tiene en cuenta además del día, la hora de la última vez en que se realizó este cambio, si en este lapso de tiempo no se cambia, el sistema SIIF Nación automáticamente bloqueará el acceso y se deberá solicitar una nueva contraseña ante la administración SIIF Nación del MHCP.

17. Si la contraseña de acceso al TOKEN es inválida se solicitará nuevamente, sin embargo, se llevará un conteo de intentos fallidos, el cual no debe exceder de más de tres (03) intentos para evitar el bloqueo.

18. Se recomienda para crear una nueva contraseña, generarla a partir de una frase que recuerde usando por ejemplo las primeras o últimas letras de cada palabra, intercalar un carácter especial, no usar todas las letras, remplazarlas por otras similares. Ejemplo: En el mes 03 empiezo mis clases de inglés: E!03emCI.

19. La contraseña se debe cambiar con frecuencia y/o cuando perciba que la saben otras personas.

20. No debe escribir el usuario ni la contraseña de acceso al SIIF Nación en páginas diferentes a la indicada por la Administración del SIIF Nación.

21. No debe suministrar su contraseña, ni información personal, ni sobre su usuario, telefónicamente o por correo o por algún otro medio, aún si le informan que lo están solicitando de su entidad o del SIIF Nación. Si tiene alguna duda contáctese con la Administración SIIF del MHCP al Call Center 6021270.

4.8 Medidas de seguridad en la administración de usuarios

A continuación, se dan a conocer las medidas de seguridad a tener en cuenta en la administración de usuarios, en cumplimiento de las políticas, normas y procedimientos establecidos para la Administración de usuarios del SIIF Nación, así:

1. Permanente control en cuanto a la administración de usuarios del Sistema SIIF Nación en lo atinente a perfiles y restricciones que sean acordes con las funciones desempeñadas.

2. Conocimiento de los documentos relacionados con la Administración de Usuarios.

3. Cualquier cambio bien sea permanente o temporal del usuario debe ser de conocimiento del Coordinador SIIF Nación Entidad para su correspondiente inactivación o eliminación del Sistema.

4. Si un usuario no atiende las medidas de seguridad requeridas en el sistema SIIF Nación debe ser deshabilitado o eliminado.

5. Recabar al personal usuario del Sistema SIIF Nación que son responsables de la confidencialidad e integridad de la información a la cual tiene acceso.

6. Para el registro de usuarios son requisitos fundamentales que el usuario sea un funcionario, contratista o personal militar de la Unidad o Subunidad Ejecutora, que el superior inmediato del funcionario o supervisor del contratista solicite por escrito su creación en el SIIF Nación y señale las restricciones que debe tener, verificar que el perfil asignado en el SIIF Nación sea consistente con las funciones del cargo u obligaciones del contrato, validar que el funcionario o contratista ha recibido previamente capacitación sobre la seguridad y funcionalidad del sistema y en caso que el usuario sea un contratista debe validar que el contrato tenga cláusula de confidencialidad.

7. Se debe contar con la permanente supervisión, de las cuentas de los usuarios en el aplicativo a fin de verificar las que deben estar activas y aquellas que deben ser inhabilitadas teniendo en cuenta las solicitudes realizadas por los usuarios.

8. Se debe revisar la fecha de expiración de los usuarios y registrar la ampliación de esta fecha en el aplicativo SIIF Nación por lo menos tres (3) días hábiles antes de expirar. Es importante realizar esta verificación con el objetivo de evitar que los usuarios queden expirados en fechas críticas.

NOTA 2: las Oficinas de Personal o quien haga sus veces deben procurar en la medida de lo posible que cuando se presenten traslados de personal que labora en el área financiera, contratos, planeación, almacenes y en general los funcionarios que hayan recibido capacitación sobre el Sistema SIIF Nación y tengan experiencia en el manejo del mismo, sean reubicados en las mismas áreas en las que se utiliza dicho aplicativo en la Unidad Ejecutora a la que se trasladan, con el fin de no perder la capacitación ni los conocimientos adquiridos.

4.8.1 Restricciones para asignación de perfiles

Con el fin de mitigar los riesgos en el manejo de los recursos, la Administración del SIIF Nación ha establecido algunas restricciones relacionadas con la asignación de perfiles a un mismo usuario, por lo tanto rechazará aquellas solicitudes de usuarios que involucren alguna de las combinaciones de perfiles no permitidas, las cuales se pueden consultar en la Guía Financiera No. 54 “Administración de Usuarios” emitida por la Dirección de Finanzas del MDN; razón por la cual se debe tener en cuenta los siguiente aspectos al asignar un perfil en el sistema:

1. No es posible tener ninguna combinación que involucre dos perfiles de los siguientes:

   Gestión Presupuesto de gastos
   Gestión Contable
   Pagador Central
   Pagador Regional

2. No es posible la combinación que involucre el perfil Autorizador Endoso con los perfiles Pagador Central o Pagador Regional.

3. No es compatible el perfil ESP- Control Consulta con ningún otro perfil.

4. Para el caso de programación presupuestal, el mismo usuario no puede tener los siguientes perfiles: Programador Presupuestal y Consolidador Presupuestal.

5. No son posibles las siguientes combinaciones:

   Pagador Central y Beneficiario Cuenta
   Pagador Regional y Beneficiario Cuenta
   Gestión Administrativa, Gestión Control Viáticos y/o Gestión Autorizador viáticos

6. El perfil “Registrador Usuarios” se puede combinar con alguno de los perfiles teniendo en cuenta las restricciones antes mencionadas.

4.9 Medidas de seguridad en el pago a beneficiario final

A continuación, se dan a conocer las medidas de seguridad a tener en cuenta para el pago a beneficiario final en el Sistema SIIF Nación, así:

1. Registrar cuentas bancarias cuando documentalmente se haya validado su existencia. Certificación bancaria no mayor a 30 días en la que se indique que la cuenta esta activa.

2. Registrar solamente cuentas bancarias que van a ser utilizadas en compromisos.

3. Efectuar registros en el sistema contra soportes documentales.

4. Al usuario que se le asigne el perfil de beneficiario cuenta, debe ser un funcionario del nivel directivo, asesor o ejecutivo. En los eventos que tal designación no sea posible, tal perfil estará en cabeza del funcionario de más alta jerarquía de la dependencia que efectuará el registro.

5. La responsabilidad de los pagos que se hagan a través del sistema SIIF Nación está en cabeza del Ordenador del Gasto y de los usuarios que intervienen en el proceso.

6. Las entidades usuarias del sistema SIIF Nación una vez han ordenado el pago al beneficiario, deberán informarle sobre la realización del mismo al tercero beneficiario, con el fin de que verifiquen el abono en cuenta.

7. El pago a beneficiario final se hará únicamente al registrado en el acto administrativo o en la relación contractual con el cual se afectan las apropiaciones, salvo en los eventos definidos por el Comité de Seguridad del SIIF Nación o en caso que se efectúe el endoso del pago el cual de estar debidamente autorizado por el Ordenador del Gasto.

8. La cuenta bancaria debe estar asociada a un único beneficiario.

9. La información relacionada en el formato “Beneficiario cuenta” debe coincidir con la información registrada en la certificación bancaria.

10. La DGCPTN bloqueará los pagos que no se hagan a beneficiario final, cuando no estén dentro de las excepciones establecidas.

5. INCIDENTE DE SEGURIDAD EN EL PAGO A BENEFICIARIO FINAL

Se entiende como un incidente de seguridad en el pago a beneficiario final el giro de recursos a un beneficiario que no tiene derecho a pago alguno.

Cuando el usuario SIIF detecte un hecho que comprometa el proceso del pago al beneficiario final, se deben tomar medidas correctivas inmediatas. Es responsabilidad de cualquier funcionario informar oportunamente cualquier anomalía que detecte en el uso del Sistema SIIF Nación.

En el evento en que se presente un incidente se debe adelantar el procedimiento descrito a continuación:

1. Informar al superior inmediato.
2. Informar al banco para bloquear el pago.
3. Bloquear el proceso si aún no se ha hecho efectivo el pago.
4. Bloquear a los usuarios que intervinieron en el proceso.
5. Informar a los entes de control interno y externo.
6. Hacer la denuncia respectiva ante la Fiscalía General de la Nación.
7. Informar a la DGCPTN y a la Administración del SIIF Nación.

6. SEGUIMIENTO A LAS MEDIDAS DE SEGURIDAD

Las Oficinas de Control Interno en su rol control entidad en la Organización SIIF de la Unidad son las encargadas de ejercer estricto seguimiento al cumplimiento de las medidas de seguridad establecidas por el Comité de Seguridad del MHCP. Por lo tanto, es importante que dentro de sus planes de auditoría se tenga en cuenta el realizar el seguimiento a las medidas de seguridad del Sistema SIIF Nación.

1. La Oficina de Control Interno o su equivalente debe validar el cumplimiento de las medidas de seguridad instauradas por el Comité de Seguridad del Sistema SIIF Nación.

2. Deben monitorear la adecuada asignación y utilización de los certificados digitales.

3. Las Oficinas de control interno deben ser usuarias del sistema SIIF a través del perfil consulta.

A continuación, se dan a conocer algunos de los aspectos que deben ser verificados, así:

6.1 Creación de usuarios

La Administración del SIIF Nación, del MHCP, es la instancia que valida la creación de los Usuarios del Sistema. El usuario de Control Interno o quien haga sus veces debe validar la siguiente información:

* Forma de vinculación: validar que el usuario es funcionario de planta de la Entidad. Para usuarios Contratistas, se debe verificar la existencia de cláusula de confidencialidad en el contrato.

* Funciones usuario: validar que las funciones que tiene el funcionario sean consistentes con el perfil para el cual aplica en el Sistema SIIF Nación.

* Restricciones: validar si el usuario debe tener acceso a todas las transacciones propias del perfil.

* Capacitación funcional: validar que el usuario ha sido capacitado en aspectos conceptuales y funcionales propios del perfil.

* Condiciones técnicas: se debe validar, que el usuario cuenta con las condiciones tecnológicas adecuadas para el ingreso al SIIF Nación, como red y computador.

* Validación uso aplicativo: verificar que el usuario del SIIF Nación se encuentre activo en el Sistema, siempre y cuando no haya presentado alguna novedad de personal como vacaciones, licencias, incapacidades, traslados, retiros, entre otros.

6.2 Archivo documental

El Coordinador SIIF Entidad debe mantener actualizado el archivo ya sea físico o magnético con los documentos que se establecen en los procedimientos de Administración de usuarios, así:

a. Archivo de Coordinador Entidad

Se debe mantener un archivo actualizado en orden cronológico en forma descendente, con los siguientes formatos:

1. Mis.3.13. Pro.5. Fr.1 “Designación Coordinador SIIF Entidad”.
2. Mis.3.13. Pro.5. Fr.2 “Designación Delegado Coordinador SIIF Entidad”
3. Mis.3.13. Pro.5. Fr.3 “Designación Soporte Técnico SIIF Entidad”
4. Mis.3.13. Pro.5. Fr.4 “Actualización Datos Coordinador SIIF Entidad / Delegado / Soporte Técnico SIIF Nación Entidad”, (cuando aplique).

b. Archivo de Hojas de Vida Usuarios

Se debe mantener un archivo actualizado por Usuario con los siguientes documentos:

1. Mis.3.13.Pro.5.FR.6 Solicitud creación cuenta de usuario SIIF Nación II.
2. Mis.3.13.Pro.5.FR.8 Solicitud modificación cuenta de usuario SIIF Nación II, cuando aplique.
3. Fotocopia de la cédula de ciudadanía.
4. Certificado de Funciones del Usuario.
5. Certificación laboral.
6. Si el usuario es Contratista, el contrato debe contener la cláusula de confidencialidad y las funciones relacionadas con el Sistema SIIF Nación para que pueda ser usuario del sistema.

c. Mantenimiento del Archivo.

Continuamente se deben realizar inspecciones al inventario del archivo, con el fin de identificar documentos faltantes relacionados en el numeral anterior, de los usuarios creados en el Sistema SIIF Nación.

7. INCUMPLIMIENTO MEDIDAS DE SEGURIDAD

El incumplimiento de las medidas de seguridad del Sistema SIIF Nación, podrá acarrear sanciones disciplinarias dentro de los términos establecidos en el Código Único Disciplinario, sin perjuicio de las demás acciones legales.

8. AUTOCONTROL

No se debe olvidar que uno de los principios en los que se basa el control de las acciones es el "Autocontrol", el cual debe ostentar cada servidor público para controlar su trabajo, detectar desviaciones y efectuar correctivos, de conformidad con lo dispuesto en los Sistema de Gestión de Calidad para cada Unidad o Subunidad Ejecutora.

9. ABREVIATURAS, UNIDADES DE MEDIDA Y EXPRESIONES ACEPTADAS

Se encuentran señaladas dentro del cuerpo del documento para dar mayor claridad al lector del mismo.

10. NOTAS Y ADVERTENCIAS

Se encuentran señaladas dentro del cuerpo del documento para dar mayor claridad al lector del mismo.

11. DOCUMENTOS ASOCIADOS

11.1 Ley 527 de agosto 18 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."

11.2 Ley 734 de febrero 5 de 2002 "Por la cual se expide el Código Disciplinario Único".

11.3 Ley 1273 de enero 5 de enero de 2009: "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

11.4 Decreto Ley 19 de 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública"

11.5 Decreto 1068 del 26 de mayo de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público".

11.6 Circular Externa del Ministerio de Hacienda y Crédito Público No. 43 del 29 de julio de 2011, por concepto del pago a beneficiario final SIIF Nación.

11.7 Circular Externa del Ministerio de Hacienda y Crédito Público No. 005 del 23 de enero de 2012, mediante la cual se informan el prerrequisito para el uso de las firmas digitales.

11.8 Circular Externa del Ministerio de Hacienda y Crédito Público No. 006 del 8 de febrero de 2012, por concepto de firma digital en el aplicativo SIIF Nación.

11.9 Circular Externa del Ministerio de Hacienda y Crédito Público No. 32 del 24 de septiembre de 2012, mediante la cual se informan los correos del SIIF Nación.

11.10 Circular Externa del Ministerio de Hacienda y Crédito Público No. 23 del 22 de marzo de 2013, por concepto del reglamento de uso del SIIF Nación.

11.11 Circular Externa No. 054 Cambios y mejoras en actualización de versión SIIF Nación octubre 4 de 2013 – Ministerio de Hacienda y Crédito Público.

11.12 Circular Externa No. 024 Cambios entrada al sistema 3 de abril de 2014 – Ministerio de Hacienda y Crédito Público.

11.13 Circular Externa No. 026 Actualización de versión del SIIF Nación 7 de abril de 2014 – Ministerio de Hacienda y Crédito Público.

11.14 Circular Externa No. 002 Pago a Beneficiario final a través del SIIF Nación 08 de enero de 2016 – Ministerio de Hacienda y Crédito Público.

11.15 Circular 022 Cambios y mejoras en actualización de versión del SIIF Nación del 09 de abril de 2016- Ministerio de Hacienda y Crédito Público.

11.16 Circular 038 Cambio de contraseña del 13 de junio de 2016- Ministerio de Hacienda y Crédito Público.

11.17 Circular Externa del Ministerio de Hacienda y Crédito Público No. 004 del 26 de enero de 2017, Firma digital en el aplicativo SIIF Nación.

11.18 Circular Externa del Ministerio de Hacienda y Crédito Público No. 037 del 30 de octubre de 2017 Cambios y Mejoras en Actualización de Versión del SIIF Nación.

11.19 Circular Externa del Ministerio de Hacienda y Crédito Público No. 037 del 31 de agosto de 2018, cambios y mejoras en actualización de versión del SIIF Nación.

11.20 Circular Externa del Ministerio de Hacienda y Crédito Público No. 055 del 12 de diciembre de 2018, Compatibilidad de perfiles de usuario

11.21 Circular Externa del Ministerio de Hacienda y Crédito Público No. 014 del 02 de abril de 2019, Radicación de documentos soporte administración de usuarios.

11.22 Guía firma digital en el SIIF Nación Problemas Frecuentes del 16 de septiembre de 2013 Ministerio de Hacienda y Crédito Público.

11.23 Guía de instalación prerrequisitos para el uso de certificados digitales del 9 de julio de 2018 - Ministerio de Hacienda y Crédito Público.

11.24 Guía de uso Certificados y Firma Digital en el SIIF Nación del 09 de julio de 2018 - Ministerio de Hacienda y Crédito Público.

11.25 Guía Entrada al Sistema 18 de marzo de 2019– Ministerio de Hacienda y Crédito Público.

11.26 Guía de posibles errores Radicación Administración de Usuarios 28 de marzo de 2019– Ministerio de Hacienda y Crédito Público.

11.27 Guía Radicación de Documentos Administración de Usuarios 10 de abril de 2019– Ministerio de Hacienda y Crédito Público.

11.28 Políticas de Seguridad de la información del SIIF Nación del 15 de agosto de 2013, Ministerio de Hacienda y Crédito Público.

11.29 Recomendaciones de seguridad SIIF NACIÓN - Ministerio de Hacienda y Crédito Público.

11.30 Directiva Permanente “Políticas para el cierre de vigencia fiscal e inicio de la nueva vigencia” de la Dirección de Finanzas del Ministerio de Defensa Nacional.

11.31 Reglamento de uso del SIIF Nación del 15 de febrero de 2013 - Ministerio de Hacienda y Crédito Público.

11.32 Reglamento de uso del SIIF Nación del Ministerio de Hacienda y Crédito Público (Aprobado en sesión ordinaria del 26 de febrero de 2013, acta No. 16).

11.33 SIIF Instructivo Configuración Clientes 21 de agosto de 2018 – Ministerio de Hacienda y Crédito Público.

11.34 SIIF Lista de chequeo para las Entidades 21 de agosto de 2018 – Ministerio de Hacienda y Crédito Público.

11.35 SIIF – Canales de Contingencia para SIIF Nación 8 de agosto de 2018 - Ministerio de Hacienda y Crédito Público.

11.36 SIIF Guía para - actualizar el componente de firma digital 16 de agosto del 2018 - Ministerio de Hacienda y Crédito Público.

11.37 SIIF – Canales de Contingencia para SIIF Nación 8 de agosto del 2018 – Ministerio de Hacienda y Crédito Público.

11.38 SIIF – Lineamientos para Establecer el Ancho de Banda para Acceder al SIIF Nación – Ministerio de Hacienda y Crédito Público.

11.39 SIIF – Esquema de Interconexión para acceder al SIIF Nación 8 de agosto del 2018 – Ministerio de Hacienda y Crédito Público.

11.40 SIIF Manual Técnico VPNSSL 1 de agosto del 2018 - Ministerio de Hacienda y Crédito Público.

11.41 SIIF – Recomendaciones Configuración Entidades 25 de julio del 2018 - Ministerio de Hacienda y Crédito Público.

11.42 Guía Financiera No. 54 “Administración de Usuarios”.

11.43 Guía Financiera No. 56 “Reportes y consultas para seguimiento y auditoria de la actividad financiera”.

12. ANEXOS

No Aplica.

13. DEFINICIONES

13.1. Carrier: operadores de telecomunicaciones propietarios de las redes troncales de Internet y responsables del transporte de los datos.

13.2. Encriptación: es un proceso para convertir la información a un formato más seguro, consiste en volver ilegible información considera importante.

13.3. GNAP: red de alta velocidad del Estado Colombiano. Es una red privada de última tecnología que interconecta a las instituciones públicas a altas velocidades, con altos niveles de disponibilidad y seguridad, la cual facilita la gestión pública y optimiza los servicios que se entregan a los ciudadanos

13.4. Red Switchada: utilización de switch en la red, lo que permite un aumento del rendimiento, el enlace de diversas tecnologías y facilidad de administración.

13.5. Sede Electrónica: espacio digital disponible dentro de la página del Ministerio de Hacienda y Crédito Público, destinado a la radicación de soportes de administración de usuarios SIIF Nación, seguimiento de radicados, entre otras funcionalidades.

13.6. Switch: es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red.