REFERENCIA	NOMBRE DE AUDITORIA	PROCESO AREA AUDITADA	FECHAS DE REALIZACIÓN (INICIO Y CIERRE)	FECHA DEL INFORME
A-GTI-01	Tecnologías de la Información - Diagnóstico Fase I	Agencia Defensa Jurídica, Secretaria General	Junio y julio de 2014	Julio 23 de 2014

AUDITOR RESPONSABLE
Jorge Andrés Medina Galeano.
EQUIPO DE AUDITORES
No aplica.

1. CRITERIOS:

1.1CALIDAD
No aplica.
1.2CONTROL INTERNO
Los criterios establecidos para evaluar el control interno en el marco de los controles tecnológicos, fueron los estándares internacionales COBIT[1] e ITIL V3[2]. De la misma manera, para la calificación y evaluación del riesgo se utilizó la Guía Metodológica del Sistema de Administración de Riesgos de la ANDJE de noviembre de 2013. Para dar marco de cumplimiento a la obligación de uso de sistemas de información externos y la asignación uno o más usuarios en cada sistema de información, fue necesario consultar la normativa de cada sistema. Estos son: ➢ Decreto 1151 de 2008 y ampliados por el decreto 2693 de 2012. ➢ Decreto 2674 de 2012, ley 734 de 2002 o Código Único Disciplinario, artículo 34, numeral 33, así como la Ley orgánica de presupuesto y decreto 178 de 2003, la cual establece al SIIF Nación como el sistema de información financiera del Estado. ➢ Decreto 3402 de 2007, mediante el que se establece el reporte trimestral de las cuentas de balance en el sistema de información CHIP. ➢ Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, en el que se crea el SIGEP para la gestión del empleo público. ➢ Ley 1150 de 2007 y en el Decreto Ley 019 de 2012, en la que se instituye que la actividad contractual de las entidades que ejecutan recursos públicos debe estar publicada en el SECOP

[1] COBIT: Objetivos de Control para Tecnologías de información y relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology). Conjunto de mejores prácticas para el manejo de información que, si se encuentran implementadas en una entidad, proporciona una seguridad razonable de que el gobierno TI soporta los objetivos del negocio, utilizando los recursos tecnológicos con eficacia para gestionar y reportar información fiable. Creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992.

[2] La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general; ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

- Decreto 3286 de 2004, Artículo 27 Decreto 2844 de 2010 se reglamenta el Sistema de Seguimiento a Proyectos de Inversión, SPI.
- Decreto 3286 de 2004, donde se crea el Sistema de Información de Seguimiento a los Proyectos de Inversión Pública, SUIFP.
- Directiva presidencial No. 21 de septiembre de 2011, Artículo 343 Constitución Nacional, Ley 152 de 1994, Resolución 063 del CONPES 1994, en los que se establece el Sistema de Seguimiento a Metas de Gobierno SISMEG, Incluido en el Sistema Nacional de Evaluación de Gestión y Resultados, SINERGIA.

Para satisfacer los objetivos del negocio, la información contenida en los sistemas de información necesita adaptarse a criterios de control, los cuales son referidos en el estándar COBIT como requerimientos de información del negocio, así:

- La **integridad** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- La **disponibilidad** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
- La **confidencialidad** se refiere a la protección de información sensitiva contra revelación no autorizada.
- La **confiabilidad** se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.
- La **efectividad** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- La **eficiencia** consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
- El **cumplimiento** tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

2. OBJETIVOS:

2.1 CALIDAD

No aplica.

2.2 CONTROL INTERNO

- Evaluar el ambiente de control sobre la información que reposa en los sistemas de información.
- Conceptuar acerca del estado de los riesgos que afectan el cumplimiento de los criterios de la información (confidencialidad, integridad, efectividad, eficiencia, cumplimiento, confiabilidad y disponibilidad).
- Realizar un diagnóstico en controles de seguridad de acceso y gestión en la administración de los usuarios de los sistemas de información que son administrados por entidades externas.

3. ALCANCE:

Se define como alcance de la presente auditoria de diagnóstico los controles implementados a junio 2014, fecha de la auditoria, para la administración de usuarios de los sistemas de información administrados por entidades externas serán:

Sistema	Entidad administradora	Usuario
SIIF	Ministerio de Hacienda y Crédito Público	Grupo Interno de trabajo de Gestión Financiera
CHIP	Contaduría General de la Nación	
SECOP	Departamento Nacional de Planeación	Grupo Contractual
SIGEP	Departamento Administrativo de la Función Pública	Grupo Contractual - Grupo Talento Humano
HOMINIS	Nomina - Procuraduría	Grupo de Talento Humano
SPI	Departamento Nacional de Planeación	Oficina Asesora de Planeación
SUIFP	Departamento Nacional de Planeación	
SISMEG	Departamento Nacional de Planeación	

4. LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA:

El Diagnostico a presentar fue divido en dos fases, en la primera fase se evaluarán los sistemas de información del estado que son administrados por entidades externas pero que por su obligatorio uso, demanda una especial atención por la Agencia. La segunda fase evaluará los controles generales de las responsabilidades propias e inherentes a los sistemas de información internos y a la gestión tecnológica. Esta segunda fase será pospuesta para que el esfuerzo de atender dicha auditoria sea simultánea a la consultoría que se está contratando con un alcance similar.

5. DOCUMENTOS EXAMINADOS:

Para la fase inicial fueron examinados los documentos soportes de cada aplicativo citados en los criterios, así como las páginas web de cada aplicativo, con sus manuales, presentaciones y documentos de referencia.

6. RESUMEN DEL INFORME:

6.1 Elemento de la normas de calidad	Numeral de la Norma	Número de no conformidades
No aplica.		
Total de no conformidades	--	--

6.2 Normas de Control Interno (subsistema, componente, elemento)	Criterio	Número de hallazgos
No hubo hallazgos		
Total de hallazgos	--	**0**

7. INFORME

7.1 CONTENIDO

DIAGNÓSTICO A CONTROLES DE LOS SISTEMAS DE INFORMACIÓN QUE SON ADMINISTRADOS POR ENTIDADES EXTERNAS

Los Controles Generales de Tecnología no sólo dependen de los departamentos de tecnología, ya que garantizar los criterios de la información referidos por estándares nacionales e internacionales tales como: la confidencialidad, integridad, cumplimiento y confiabilidad de la información obedecen al buen uso que le den los usuarios del sistema y por eso es frente a ellos que se establecen los siguientes controles generales:

- Creación de un único usuario del sistema por persona.
- Asignación de un rol definido para el cumplimiento de las funciones a cada usuario.
- Creación del usuario, únicamente bajo la necesidad del cargo y bajo una autorización del líder de proceso respectivo.
- Uso de contraseñas de un alto nivel de complejidad; esto es el uso de caracteres alfa numéricos, el uso de mayúsculas - minúsculas, longitud mínima de 8 caracteres y algunos caracteres especiales.
- Cambio periódico de la contraseña de acceso (3 meses como máximo) y aunque el sistema en algunos casos no lo requiera, se establezca como una buena práctica.
- Inhabilitar los usuarios durante incapacidades, vacaciones o licencias de larga duración.
- No compartir las contraseñas ni usuarios con compañeros o incluso jefes.
- Desactivar el usuario, una vez finalizado el vínculo contractual con la entidad.

Lo anterior permitirá mitigar riesgos tales como perdida de los criterios de la información citados, provenientes de accesos no autorizados o mal intencionados, así como de posibles ataques por identificación de debilidades en el sistema de control de acceso o, modificación de la información de los sistemas con o sin intención.

Dicho lo anterior, para la presente revisión se revisaron ocho (8) sistemas de información citados en el alcance de la auditoria.

De manera general se puede establecer que los sistemas cuentan con controles de acceso y creación de usuarios, sin embargo se deja a la entidad y el área usuaria, algunas responsabilidades sobre el reporte oportuno de creación y eliminación de usuarios del sistema, así como el buen uso y supervisión del acceso otorgado.

En particular se observó lo siguiente:

1. SIIF - Sistema Integrado de Información Financiera SIIF Nación

Sistema de información del Ministerio de Hacienda y Crédito Público para uso del Grupo Interno de trabajo de Gestión Financiera. Su responsable es el doctor Guillermo Martínez, coordinador del Grupo referido. "*Constituye una iniciativa del Ministerio de Hacienda y Crédito Público que permite a la Nación consolidar la información financiera de las Entidades que conforman el Presupuesto General de la Nación y ejercer el control de la ejecución presupuestal y financiera de las Entidades pertenecientes a la Administración Central Nacional y sus subunidades descentralizada, con el fin de propiciar una mayor eficiencia en el uso de los recursos de la Nación y de brindar información oportuna y confiable*", según informa la página web del Ministerio.

Según el decreto 2674, en el artículo 14 y 15: "*Crear, eliminar, permisos y restricciones, a mantener archivo documental de usuarios, mantener actualizada la información de su delegado, soporte o cambio de funcionario responsable*" son las funciones del coordinador ante la entidad que para el caso de la Agencia, fue delegado en el doctor Guillermo Martínez, coordinador del Grupo Financiero.

El Ministerio de Hacienda y Crédito Público estableció controles para la creación, eliminación y revisión de usuarios del SIIF, debido a que si bien el coordinador del Grupo Financiero se encarga de segregar funciones entre los usuarios, el Ministerio realiza una verificación y aprobación final antes de la creación, verificando que el funcionario o contratista haya realizado una capacitación adecuada sobre el manejo del sistema así como evitando la duplicidad y concentración de funciones.

El ingreso al sistema se realiza con Token Criptográficos, garantizando la seguridad de apertura, adicionalmente se bloquean los usuarios luego de 3 días de inactividad.

El buen uso del usuario depende en exclusiva del funcionario aunque se realizan capacitaciones para incentivar el buen uso y las buenas prácticas.

En el retiro de la entidad de los funcionarios, el coordinador del Grupo Financiero debe reportar tanto al Ministerio para su inactivación, como solicitar la revocación del certificado (Token) a la autoridad certificadora que lo emitió, cuando el usuario deje de requerir el uso del mismo.

2. CHIP - Sistema Integrado de Información Financiera SIIF Nación

"*El Consolidador de Hacienda e Información Pública (CHIP), es un sistema de información diseñado y desarrollado por el Ministerio de Hacienda y Crédito Público - Programa FOSIT, para que con la adecuada reglamentación y estructura procedimental, canalice la información financiera, económica, social y ambiental de los entes públicos hacia los organismos centrales y al público en general bajo la administración y responsabilidad de la Contaduría General de la Nación.*", como lo describe la Contaduría General de la Nación en sus manuales.

Trimestralmente el Grupo Interno de trabajo de Gestión Financiera y específicamente el Contador de la Entidad reporta el balance del periodo inmediatamente anterior.

Para la asignación del único usuario, se requiere notificación y autorización del Representante Legal de la entidad así como del responsable del Área Financiera.

3. SIGEP - Sistema de Información y Gestión del Empleo Público

El sistema "*corresponde al Sistema General de Información Administrativa del Sector Público de que trata la Ley 909 de 2004, es una herramienta tecnológica que sirve de apoyo a las entidades en los procesos de planificación, desarrollo y la gestión del recurso humano al servicio del Estado. Adicionalmente, el SIGEP suministra la información necesaria para la formulación de políticas de organización institucional y recursos humanos. El SIGEP está orientado a cubrir los organismos y entidades de las tres ramas del poder público, organismos de control, organización electoral y organismos autónomos*", como lo presenta el Departamento Administrativo de la Función Pública.

El sistema asigna un rol administrador al Grupo Contractual y otro al Grupo Talento Humano, quienes tendrán el poder de crear usuarios y perfiles necesario para su gestión, implementando controles para limitar el acceso a los módulos funcionario - contratistas.

Según esta descrito en los procedimientos de la página web www.sigep.gov.co, los roles de JEFE DE CONTRATOS y JEFE DE RECURSOS HUMANOS, son solicitados por la entidad al correo soportesigep@dafp.gov.co mediante un formato definido y adjuntando el acto administrativo de posesión. Estos usuarios tendrán la posibilidad de crear nuevos usuarios en el sistema con perfiles tales como Operador de Contratos u Operador de RH, quienes tendrán la potestad de dar de alta o de baja a los contratistas o funcionarios en el sistema.

El Rol de JEFE DE RECURSOS HUMANOS, fue asignado al señor Javier González, quien a la fecha de la revisión, se encarga de crear los usuarios o perfiles necesarios para la gestión del recurso humano en la Agencia. Lo realiza bajo solicitudes y necesidades, sin embargo en este momento sólo son dos usuarios y a la fecha no se ha presentado casos de ausencias o retiros de los usuarios de la Entidad. La doctora Andrea Carolina Carrasco, coordinadora del grupo de Recursos Humanos se posesionó en el cargo posterior a la creación del usuario Javier González.

Para consultar el sistema, Control interno también tiene un usuario asignado a la funcionaria Marcela Villate, sin embargo es exclusivamente de consulta.

4. SECOP - SISTEMA ELECTRONICO DE CONTRATACIÓN PÚBLICA

Sistema que busca impulsar políticas, normas y unificar procesos en materia de compras y contratación pública, articular sus partícipes con lineamientos que sirvan de guía a los administradores públicos en la gestión y ejecución de los recursos, que generen una mayor transparencia y visibilidad de la contratación, así como optimizar los recursos del Estado.

Este sistema administrado por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente adscrita al Departamento Nacional de Planeación implementó estrictos controles para la creación de usuarios tales como:

- Previo a la solicitud de creación de usuarios, se pide que el usuario tome un curso de capacitación y presente un examen de validación o manejo el cual deberá ser aprobado con el 100%.
- Con la aprobación recibirá un código que deberá incluirse en el formato de solicitud de usuario el cual debe ser revisado y aprobado por la persona encargada de ordenadores del gasto, que para el caso de la Agencia es la doctora Isabel Abello Albino, Secretaria General.
- Copia de la resolución debe ser adjuntada y por correo electrónico se envía tanto el usuario como la contraseña.

5. HOMINIS

El Grupo de Talento Humano, área responsable de la generación de la Nómina, adquirió la licencia de uso del sistema HOMINIS en 2013, sin embargo debido a su baja portabilidad y funcionalidad dejó en evidencia la necesidad de contar con un sistema más robusto para la generación de nómina, según informo la coordinadora del grupo.

Para la adquisición de un nuevo sistema o el pago de licencias de uso, se recomienda la inclusión de requerimientos funcionales tales como controles de seguridad de acceso, identificación de usuarios y registros del sistema.

Así mismo, se recomienda establecer dentro del Grupo de trabajo, controles para el correcto uso del sistema y controles tendientes a validar la segregación de funciones en los sistemas.

6. SPI - SEGUIMIENTO A PROYECTOS DE INVERSIÓN y
7. SUIFP - SISTEMA UNIFICADO DE INVERSIONES Y FINANZAS PÚBLICAS

Con el Decreto 3286 de 2004 se crea el Sistema de Información de Seguimiento a los Proyectos de Inversión Pública y se reglamenta el Sistema de Seguimiento a Proyectos de Inversión, con el objeto de que el Departamento Nacional de Planeación mantenga disponible la información de seguimiento a los proyectos de inversión pública para ser consultada permanentemente con fines de control social por todos los interesados, quienes podrán efectuar los comentarios, observaciones, solicitudes o recomendaciones que consideren conducentes

Para tal fin la doctora Diana Carolina Enciso, jefe de la Oficina Asesora de Planeación asumió el rol de usuaria administradora del sistema en la Agencia y por tanto para la creación de su usuario le fue solicitada la resolución de nombramiento.

Cada proyecto debe tener un único gerente al cual le asignan un usuario que para el caso de SUIFP es solicitado a través del jefe de la Oficina Asesora de Planeación, pero para el sistema SPI,

será creado por ella misma con su usuario. Los gerentes de proyecto deben reportar mensualmente el seguimiento del proyecto. En caso de no recibir el seguimiento se reporta al administrador la novedad, de manera que mensualmente se controla la vigencia y actividad de los usuarios.

Para el caso de la agencia, los gerentes de proyecto son los jefes, coordinadores y directivos de la Agencia, por tanto se detecta oportunamente la salida de alguno para reasignación de usuarios. Una vez finalizado el proyecto, el usuario es desactivado automáticamente por el sistema.

8. SISMEG - SISTEMA DE SEGUIMIENTO A METAS DE GOBIERNO

Sistema incluido en el Sistema Nacional de Evaluación de Gestión y Resultado del Departamento Nacional de Planeación, SINERGIA, que a través de la Directiva presidencial No. 21 de septiembre de 2011, artículo 343 Constitución Nacional, Ley 152 de 1994 y la Resolución 063 del CONPES 1994, requiere a las Oficina de Planeación de cada entidad a realizar el reporte mensual de los indicadores de gestión para cada periodo presidencial.

Por tanto, la agencia sólo tiene un usuario, asignado por defecto a la Jefe de la Oficina de Planeación, sin embargo el reporte de los dos indicadores en ocasiones ha sido delegado al personal de la misma oficina pues es una tarea operativa.

7.2 FORTALEZAS

Las entidades han implementado controles para la gestión de usuarios y seguridad de acceso en sus sistemas de información y por tal razón demanda de los administradores y usuarios de la ejecución de actividades de control.

7.3 CUMPLIMIENTO DE PRINCIPIOS

A la fecha, los sistemas de información cuentan con usuarios que tienen acceso suficiente para generar y reportar la información pertinente a cada sistema por parte de la Agencia, sin embargo el alcance de la auditoria busca implementar controles para que la información allí reportada sea integra y confiable.

8. DESCRIPCIÓN DE LA (S) NO CONFORMIDAD (ES) Y/O HALLAZGO (S)

8.1. NO CONFORMIDADES EN SISTEMA DE CALIDAD

REQUISITO DE LA NORMA	NO CONFORMIDAD	OBSERVACIONES
No aplica.	*No aplica.*	*No aplica.*

8.2. HALLAZGOS EN SISTEMA DE CONTROL INTERNO

REQUISITO DE LA NORMA	HALLAZGOS	OBSERVACIONES
En el dominio de COBIT, "Entregar y dar soporte" se establece el objetivo Garantizar la seguridad de los sistemas. Esto en el acceso organizado y en la asignación de un único usuario por persona con contraseñas seguras.		La señorita Luz Johanna Albarracín, funcionaria del Grupo Contractual es la actual encargada del usuario con perfil JEFE DE CONTRATOS. Ella es quien debe gestar los usuarios de los funcionarios contratistas (dar de alta), y para la desactivación del mismo (dar de baja), ingresando algunos datos básicos. Sin embargo en la página web se pudo observar que el perfil de JEFE debe ser asignado a los líderes del proceso y por tal razón la mesa de ayuda del sistema, solicita copia del acta de posesión en el cargo para la creación de dicho usuario. Son los usuarios con perfil de JEFE los citados a crear usuarios con perfiles operativos según la necesidad.
		En los tres siguientes sistemas de información, se identificó una exposición al riesgo de pérdida de integridad y confiablidad de la información, por posibles accesos no autorizados al sistema debido a que las contraseñas no son personales e intransferibles: 1. SIGEP: Para los casos en los que la funcionara usuaria del sistema del Grupo Contractual solicite vacaciones y/o licencias, el usuario del sistema es prestado junto con la contraseña para que el área pueda seguir desarrollando sus funciones respectivas. 2. SECOP: Al ingresar al sistema, cada usuario tiene acceso exclusivo a los procesos de contratación que ingresó el mismo, generando inconvenientes en las ausencias de los funcionarios, pues de requerirse modificar la información por otros ingresada, se deben compartir las contraseñas aun cuando el riesgo de pérdida de integridad y confiabilidad de la información es conocido por los funcionarios. 3. HOMINIS: El sistema actual solo cuenta con un único usuario para la entidad obligando a los funcionarios a compartir la contraseña, perdiendo trazabilidad sobre el uso del mismo.

9. RECOMENDACIONES:

La gestión y administración de usuarios de los diferentes sistemas de información analizados, son asignados a los líderes de cada proceso, sin embargo no son independientes de las gestiones del proceso de Tecnologías de la Información, pues son ellos los citados a generar políticas y directrices para la adecuada gestión de usuarios, de promover el uso de contraseñas seguras, que garanticen la integridad y confiabilidad en la información reportada.

Por lo anterior se realizan las siguientes recomendaciones generales:

- Incluir dentro de la política de seguridad de la información de la entidad, el compromiso de cada funcionario frente a las conductas y prácticas de seguridad que como usuarios de los sistemas externos y propios debemos asumir.
- Documentar y guardar soporte de las solicitudes y aprobaciones de creación, modificación y eliminación de usuarios para los aplicativos administrados por terceros.
- Propender por la creación de un único usuario del sistema por persona.
- Asignar un rol definido para el cumplimiento de las funciones a cada usuario.
- Creación del usuario, únicamente bajo la necesidad del cargo y bajo una autorización del líder de proceso respectivo.
- Uso de contraseñas de un alto nivel de complejidad; esto es el uso de caracteres alfa numéricos, el uso de mayúsculas - minúsculas, longitud mínima de 8 caracteres y algunos caracteres especiales.
- Cambio periódico de la contraseña de acceso (3 meses como máximo), y aunque el sistema en algunos casos no lo requiera, se establezca como una buena práctica.
- Inhabilitar los usuarios durante incapacidades, vacaciones o licencias de larga duración.
- No compartir las contraseñas ni usuarios con compañeros o incluso jefes.
- Desactivar el usuario, una vez finalizado el vínculo contractual con la entidad.

Recomendaciones específicas:

- SIIF: Debido a los buenos controles implementados por el Ministerio de Hacienda y Crédito Público, se recomienda llevar un registro de las solicitudes realizadas así como de los reportes recibidos para documentar los controles implementados.

- CHIP: A la fecha no se han presentado casos de periodos vacacionales del Contador, por tanto no se han realizado requerimientos sobre nuevos usuarios o se ha tenido la necesidad de compartir el usuario, sin embargo se recomienda tener especial atención frente a estos escenarios en los que se requiera una sustitución parcial o definitiva del funcionario.

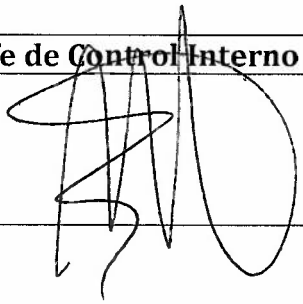
- SIGEP: Solicitar la creación del usuario para la doctora Andrea Carolina Carrasco con perfil de JEFE DE RECURSOS HUMANOS, para que sea ella quien cree y asigne los usuarios y perfiles requeridos en su área. Por lo anterior, se deberá solicitar la modificación del perfil del funcionario Javier González a un perfil operativo.

- SIGEP: Se recomienda realizar un cambio de contraseña del usuario creado y asignado a la doctora Carolina Pineda, coordinadora del grupo de contratación y hacer uso exclusivo de su usuario. Del mismo modo, bajo el procedimiento definido en la página web http://www.sigep.gov.co/docs/Asignacion finalizacion de roles.pdf, crear un usuario con perfil operativo para la funcionaria Luz Johanna Albarracin, a fin de poder realizar sus funciones de dar de alta y baja a los contratistas en el sistema de información.

- SECOP: Verbalmente se recomendó enviar una solicitud escrita al Departamento Nacional de Planeación o a la mesa de ayuda del sistema SECOP en donde se verifique el correcto proceder ante eventos no planeados, para el acceso y modificación de la información por usuarios diferentes a los creadores, de la respuesta se espera tomar medidas preventivas tendientes a mitigar el riesgo identificado.

- HOMINIS: Para la adquisición del nuevo sistema para la generación de la nómina, se recomienda la inclusión de requerimientos funcionales tales como controles de seguridad de acceso, identificación de usuarios y registros del sistema. Así mismo de establecer dentro del Grupo de trabajo, controles tendientes a validar la segregación de funciones en los sistemas así como el correcto uso del sistema.

- SUIFP-SPI: Aunque se identifican controles implícitos en la gestión de usuarios, se recomienda establecer controles tales como los referidos en el informe y en las recomendaciones generales.

Firma Auditor Designado y Equipo Auditor	Firma Jefe de Control Interno ANDJE
	

Versión	Fecha Aprobación	Naturaleza del Cambio
0	08-05-2013	Documento Original.