MINHACIENDA

CONTADURÍA GENERAL DE LA NACIÓN

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

AUDITORÍA INTERNA DE GESTIÓN
PROCESO GESTIÓN TIC's

PROCEDIMIENTO
GTI-PRC010 "SEGURIDAD DE LA INFORMACIÓN"

Diciembre 21 de 2016

Apreciado Ingeniero

Mauricio Velásquez Mesa, Coordinador GIT de Apoyo Informático

El Grupo Interno de Trabajo (GIT) de Control Interno, en ejercicio de las facultades legales otorgadas por la Ley 87 de 1993, modificada por la Ley 1474 de 2011, el Decreto 2145 de 1999 y sus modificaciones, los Decretos 1537 de 2001, 019, 2482 y 2641 de 2012 y 943 del 21 de mayo de 2014; así como los lineamientos establecidos en la nueva Guía de Auditoria para Entidades Públicas del DAFP, y las Resoluciones CGN 328 de 2005 y 203 de 2015, tiene como función realizar la evaluación independiente al Sistema de Control Interno, a los procesos, procedimientos, actividades y actuaciones de la administración, con el fin de determinar el cumplimiento y la efectividad de la gestión institucional y de los objetivos de la entidad, produciendo recomendaciones para asesorar al representante legal en busca del mejoramiento continuo.

En cumplimiento al Programa General de Auditorías aprobado el 24 de febrero de 2016, por el Comité de Coordinación del Sistema de Control Interno, este GIT adelantó la Evaluación al Procedimiento GTI-PRC010 “Seguridad de la Información”, del proceso Gestión TIC’s, a fin de conocer el grado de cumplimiento de las actividades establecidas para su desarrollo y elevar las recomendaciones que sean necesarias en ejercicio del mejoramiento continuo, lo cual redundará en el cumplimiento de los Objetivos Estratégicos de la Entidad.

Los procedimientos de auditoría se realizaron sobre la base de pruebas selectivas; un procedimiento de esta naturaleza, no puede identificar todas las desviaciones de control, sino solamente aquellas que estén presentes dentro de la muestra evaluada.

Este informe fue presentado en mesa de trabajo del 23 de diciembre de 2016 para la suscripción del respectivo plan de mejoramiento; por tanto es importante que se termine de diligenciar el formato “CYE04-FR-01 Plan de Mejoramiento”, el cual debe ser remitido por correo electrónico a más tardar el 30 de diciembre de 2016.

Cordialmente,

MARITZA VELANDIA CARDOZO
Coordinador GIT de Control Interno

C. C.: Dr. Pedro Bohórquez Ramírez - Contador General de la Nación

Proyectó: José Leonardo Buitrago
Revisó: Maritza Velandia Cardozo

Tabla de Contenido

OBJETIVO

Evaluar el desarrollo y cumplimiento de las actividades descritas en el procedimiento GTI-PRC010 “Seguridad de la Información” del proceso Gestión TIC´s en la Contaduría General de la Nación; así como, la observancia de las políticas y la efectividad de los controles, indicadores y riesgos.

ALCANCE

El GIT de Control Interno, evaluará el cumplimiento de los lineamientos descritos en el procedimiento GTI-PRC010 “Seguridad de la Información” del proceso Gestión TIC´s para la vigencia 2015 y lo corrido de 2016, lo anterior, mediante la verificación de los registros de cada una de las actividades allí descritas, así como de la administración de los riesgos y los indicadores asociados al procedimiento.

EVALUACION DE CONTROLES

De conformidad con los resultados obtenidos, en el siguiente cuadro se presenta la metodología de evaluación con sus respectivos comentarios para la adecuada comprensión y correcta implementación del plan de mejoramiento, de acuerdo con la clasificación:

	**INADECUADO** En los procedimientos y pruebas de auditoría, se evidencia que existe un bajo grado de observancia de las políticas, directrices y/o normas vigentes; los controles se están ejecutando pero son muy vulnerables y deben ser objeto de intervención o ajustes que se deben establecer y detallar a través del correspondiente plan de mejoramiento para su seguimiento.
	**ADECUADO CON OPORTUNIDAD DE MEJORA** En los procedimientos y pruebas de auditoría, se evidencia que existe un grado de observancia de las políticas, directrices y/o normas vigentes; los controles se están ejecutando pero presentan oportunidades de mejora que se deben establecer y detallar a través del correspondiente plan de mejoramiento para su seguimiento.
	**SATISFACTORIO** En los procedimientos y pruebas de auditoría, se evidencia que existe un alto grado de observancia de las políticas, directrices y/o normas vigentes; los controles se están ejecutando.

1. Matriz de riesgos del proceso

Actividades de Control	Evaluación del Control	Observaciones
Identificación, valoración, medición, controles y seguimiento.		La evaluación después de la aplicación de los controles sigue siendo extrema y de hacerse realidad podría poner en riesgo la continuidad de los servicios de la entidad. Por tanto se recomienda realizar seguimientos mensuales.

2. Indicadores

Actividades de Control	Evaluación del Control	Observaciones
Implementación, seguimiento y análisis.		Dado que dos (2) de los veintitrés (23) numerales de la política no se cumplen por algunas limitaciones técnicas, el promedio de los últimos siete trimestres es del 91.31%. Se recomiendan medidas preventivas mitigantes del riesgo.

3. Política de Seguridad Informática y Política de Contingencia

Actividades de Control	Evaluación del Control	Observaciones
Nivel de aplicabilidad		Al no existir una ejecución y documentación completa en la parte inicial del procedimiento, no existen garantías de cumplimiento del resto de actividades.

4. Seguridad y Privacidad de la Información – Componente GEL – MSPI

Actividades de Control	Evaluación del Control	Observaciones
Grado de cumplimiento Estrategia GEL		El promedio de aplicabilidad que según la Estrategia GEL se debió alcanzar a 2016 es del 60%, sin embargo el avance estimado de la Contaduría General de la Nación es: 37.5%

5. Incidentes de Seguridad

Actividades de Control	Evaluación del Control	Observaciones
Documentación, análisis, seguimiento y solución.		El resultado en satisfactorio.

CONCLUSIÓN

El GIT de Control Interno concluye que el proceso de Gestión TIC's cumple con el procedimiento documentado GTI-PRC010 "Seguridad de la Información", existiendo varios aspectos susceptibles de mejora, que deben ser ajustados de acuerdo con las observaciones y recomendaciones establecidas en el presente informe.

Se debe tener en cuenta que al ser éste el procedimiento más reciente del proceso Gestión TIC's, es importante adelantar labores de revisión y ajuste permanentes para que las actividades del mismo se adapten a la realidad y las necesidades de la entidad en materia de seguridad de la información sean plenamente cubiertas. Lo anterior debido a que desde la fecha de su creación en julio de 2015, no se han efectuado actualizaciones.

Dada la importancia que tienen los riesgos y los indicadores como mecanismos de medición y control en la gestión del procedimiento, se les debe dar un tratamiento prioritario al interior del proceso, los cuales ameritan ser revaluados y ajustados para su fortalecimiento y así cumplir con los objetivos institucionales de la CGN.

Así mismo, es importante anotar la cordialidad y disponibilidad para atender esta auditoría durante su etapa de ejecución, evidenciándose el compromiso con el Programa General de Auditorías vigencia 2016, aprobado por la alta dirección.

1. Matriz de riesgos del proceso

Una vez detectadas las falencias técnicas en la aplicación SIGI, las cuales impiden el acceso amplio y suficiente a toda la información actualizada y relacionada con los riesgos, el GIT de Control Interno se abstiene de consultar dicha fuente como referente para realizar cualquier tipo de comparación o análisis.

OBSERVACIÓN

Una vez requerido por correo electrónico, el auditado comunicó que el riesgo relacionado con el procedimiento objeto de esta auditoría es: “Vulnerabilidad en la Integridad y confidencialidad de la información”; el cual, según se consultó posteriormente en el mapa de riesgos, es evaluado como extremo y se controla trimestralmente por medio de la aplicación de la Política de Seguridad Informática, el seguimiento a los planes de contingencia y la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

RECOMENDACIÓN

Aunque a la fecha el riesgo no se ha materializado, se recomienda realizar seguimiento mensual en vez de trimestral, toda vez que la evaluación después de la aplicación de los controles sigue siendo extrema y de hacerse realidad podría poner en riesgo la continuidad de los servicios de la entidad.

2. Indicadores

Una vez detectadas las falencias técnicas en la aplicación SIGI, las cuales impiden el acceso amplio y suficiente a toda la información actualizada y relacionada con los indicadores, el GIT de Control Interno se abstiene de consultar dicha fuente como referente para realizar cualquier tipo de comparación o análisis.

OBSERVACIÓN

Al solicitar información sobre el seguimiento de los indicadores asociados al procedimiento; se observó que el auditado se basa en la "Disponibilidad y Confidencialidad de la Información" para realizar las actividades de medición, las cuales tienen que ver directamente con el análisis de cumplimiento de la Política de Seguridad Informática. A continuación se mencionan los aspectos que llamaron la atención:

Dado que dos (2) de los veintitrés (23) numerales de la política no se cumplen, el promedio de los últimos siete trimestres es del 91.31%.

Una de las actividades que no se cumple es la restauración de archivos desde copias de respaldo previa evaluación del software antivirus; lo anterior teniendo en cuenta los grandes volúmenes de información que manejan las bases de datos y la inmediatez con la que se requieren dichas restauraciones en los servidores de la entidad.

El segundo aspecto por implementar es el fortalecimiento de la seguridad del directorio activo, restringiendo información sensible antes de la debida autenticación en el sistema; para lo anterior, el equipo de soporte se encuentra aplicando las configuraciones pertinentes en equipos y servidores.

RECOMENDACIÓN

Presentadas las razones por las cuales no se ha podido dar cumplimiento a la implementación de las dos (2) actividades anteriormente mencionadas, se recomienda lo siguiente:

Garantizar la verificación antivirus de todos los sistemas en producción antes de la toma de las respectivas copias de respaldo, así como de las estructuras de archivos en donde se realizarán las restauraciones.

Dar celeridad a la actualización de los sistemas operativos, tanto de servidores como de equipos de usuario final, con el objetivo de garantizar la compatibilidad en las configuraciones de autenticación y de seguridad en general.

3. Política de Seguridad Informática y Política de Contingencia

En coherencia con lo plasmado en el flujograma que describe el orden y lógica de las actividades del procedimiento objeto de esta auditoría, se efectuó la revisión del grado de aplicabilidad de la Política de Contingencia, la Política de Seguridad Informática y los demás documentos mencionados a lo largo del diagrama.

OBSERVACIÓN

En lo que tiene que ver con las actividades que corresponden al Grupo de Seguridad de la Información y la Coordinación del GIT de Apoyo Informático, se hallaron los siguientes aspectos que llamaron la atención:

• La Política de Contingencia que se menciona en el procedimiento objeto de esta auditoría, no existe.

• La Política de Seguridad Informática existe y el análisis de cumplimiento de la misma corresponde a la medición del indicador llamado: “Disponibilidad y Confidencialidad de la Información”, tema que fue desarrollado en el numeral dos (2) de este documento.

• El Plan de Mejoramiento que se menciona en el procedimiento como producto de la revisión de la Política de Seguridad y de la Política de Contingencia, no existe.

• El Plan de Seguridad que se menciona en el procedimiento como producto de la construcción del Plan de Mejoramiento del punto anterior, no existe.

Se observó que al no existir una ejecución y documentación completa en la parte inicial del procedimiento, no existen garantías de cumplimiento del resto de actividades; lo anterior teniendo en cuenta que las primeras son insumo indispensable de las que le suceden, como es el caso de las labores que adelanta el oficial de seguridad y los administradores de las plataformas en la administración de herramientas y la gestión de incidentes.

RECOMENDACIÓN

Se deben generar mecanismos que propendan por la revisión y actualización permanente del procedimiento objeto de esta auditoría y afines, toda vez que en cumplimiento de los lineamientos dictados por el Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Estrategia de Gobierno en Línea, la entidad debe desarrollar actividades tendientes a proteger la información y sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada; por tanto se debe dar cumplimiento a todas las políticas y ejecución a todos los planes.

4. Seguridad y Privacidad de la Información – Componente GEL – MSPI

Para verificar el grado de aplicabilidad de los tres logros GEL, se tomaron los lineamientos del marco de referencia establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y se analizaron junto con el auditado teniendo en cuenta la infraestructura, programas y proyectos del GIT de Apoyo Informático.

4.1 Definición del Marco de Seguridad y Privacidad de la Información

Diagnóstico de Seguridad y Privacidad	
Lineamiento	**Aplicabilidad**
LI.ES.01 Las instituciones de la administración pública deben contar con una estrategia de TI que esté alineada con las estrategias sectoriales, el Plan Nacional de Desarrollo, los planes sectoriales, los planes decenales -cuando existan- y los planes estratégicos institucionales. La estrategia de TI debe estar orientada a generar valor y a contribuir al logro de los objetivos estratégicos.	La aplicabilidad de este lineamiento se evidenció en el documento Plan Estratégico de las Tecnologías de la Información (PETI) publicado en la intranet de la entidad, el cual tiene un alcance de cuatro años y está próximo de actualización en la presente vigencia.
LI.ES.02 Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución.	Se observó que actualmente la entidad no ha implementado acciones propias de la arquitectura empresarial.
LI.GO.01 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI que estructure y direccione el flujo de las decisiones de TI, que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución.	Se comprobó que actualmente la entidad no cuenta con un esquema completo de Gobierno de TI. Sin embargo, se observó que existe el Comité de Seguridad de la Información en el cual se apoyan algunas decisiones de TI en relación a la seguridad y privacidad.
LI.GO.04 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el macro-proceso de gestión de TI, según los lineamientos del Modelo Integrado de Planeación y Gestión de la institución, teniendo en cuenta el Modelo de gestión estratégica de TI.	Se observó que actualmente la entidad no ha implementado acciones propias del macro-proceso de Gestión de TI.
LI.ST.14 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el análisis de vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI.	El GIT de Apoyo Informático comunicó que actualmente la entidad no ha implementado acciones propias con respecto al análisis de vulnerabilidades de la infraestructura tecnológica.

Plan de Seguridad y Privacidad de la Información	
Lineamiento	**Aplicabilidad**
LI.ES.02 Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial (AE) para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución.	Se observó que actualmente la entidad no ha implementado acciones propias de la arquitectura empresarial.
LI.ES.06 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas: seguridad, continuidad del negocio, gestión de información, adquisición, desarrollo e implantación de sistemas de información, acceso a la tecnología y uso de las facilidades por parte de los usuarios. Así mismo, se debe contar con un proceso integrado entre las instituciones del sector que permita asegurar el cumplimiento y actualización de las políticas y estándares de TI.	Actualmente la entidad no cuenta con un esquema completo de Gobierno de TI. Sin embargo, se observó que se han desarrollado actividades relacionadas con la seguridad de la información, planes de contingencia y continuidad del negocio, y acceso a la información pública por parte de los diferentes usuarios.
LI.ES.08 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe participar de forma activa en la concepción, planeación y desarrollo de los proyectos de la institución que incorporen componentes de TI. Así mismo, debe asegurar la conformidad del proyecto con los lineamientos de la AE definidos para la institución.	Se observó que el GIT de Apoyo Informático participa activamente en la creación y actualización del proyecto de inversión "Fortalecimiento de los Sistemas de Información" el cual incorpora todos los componentes de TI en la entidad.
LI.GO.01 La dirección de Tecnologías y Sistemas de la Información debe definir e implementar un esquema de Gobierno TI que estructure y direccione el flujo de las decisiones de TI, que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución.	Actualmente la entidad no cuenta con un esquema completo de Gobierno de TI. Sin embargo, se observó que existe el Comité de Seguridad de la Información en el cual se apoyan algunas decisiones de TI en relación a la seguridad y privacidad.
LI.GO.04 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el macro-proceso de gestión de TI, según los lineamientos del Modelo Integrado de Planeación y Gestión de la institución, teniendo en cuenta el Modelo de gestión estratégica de TI.	El GIT de Apoyo Informático comunicó que actualmente la entidad no ha implementado acciones propias del macro-proceso de Gestión de TI.
LI.GO.09 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe liderar la planeación, ejecución y seguimiento a los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la institución incluyan componentes de TI y sean liderados por otras áreas. La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá liderar el trabajo sobre el componente de TI conforme con los lineamientos de la AE institucional.	Se observó que el GIT de Apoyo Informático participa activamente en la creación y actualización del proyecto de inversión "Fortalecimiento de los Sistemas de Información" el cual incorpora todos los componentes de TI en la entidad.

LI.SIS.22 En el diseño de sus sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar aquellos componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información.	Se observó que el GIT de Apoyo Informático adelanta labores que propenden por la privacidad de la información a través de controles como: control de acceso, gestión de cuentas de usuario, registro de incidentes y la Política de Usuarios y Contraseñas.

4.2 Implementación del Plan de Seguridad

Gestión de Riesgos de Seguridad y Privacidad de la Información	
Lineamiento	**Aplicabilidad**
LI.INF.15 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los Componentes de información. Estos mecanismos deben ser considerados en el proceso de gestión de dicho Componentes. Los sistemas de información deben implementar los criterios de trazabilidad y auditoría definidos para los Componentes de información que maneja.	Se observó que en el GIT de Apoyo Informático esta implementado un repositorio de datos para el uso de todas las líneas de trabajo. Sin embargo, el acceso y uso de esta herramienta no está disponible aún para toda la entidad.
LI.SIS.22 En el diseño de sus sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar aquellos componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información.	Se comprobó que actualmente se cuenta con una Política de Seguridad Informática que implementa mecanismos de control de acceso.

4.3 Monitoreo y Mejoramiento Continuo

Evaluación del Desempeño	
Lineamiento	**Aplicabilidad**
LI.ES.13 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un tablero de indicadores sectorial y por institución, que permita tener una visión integral de los avances y resultados en el desarrollo de la Estrategia TI.	Se evidenció que actualmente el GIT de Apoyo Informático no cuenta con el monitoreo mencionado.
LI.GO.03 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir y realizar actividades que conduzcan a evaluar, monitorear y direccionar los resultados de las soluciones de TI para apoyar los procesos internos de la institución. Debe además tener un plan específico de atención a aquellos procesos que se encuentren dentro de la lista de no conformidad del marco de las auditorías de control interno y externo de gestión, a fin de cumplir con el compromiso de mejoramiento continuo de la administración pública de la institución.	Se observó que el GIT de Apoyo Informático administra indicadores que monitorean, evalúan y direccionan las soluciones de TI implementadas en el área. Adicionalmente, se comprobó que se han elaborado planes de mejoramiento producto de las auditorías internas de gestión.

LI.GO.12 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el monitoreo y evaluación de desempeño de la gestión de TI a partir de las mediciones de los indicadores del macro-proceso de Gestión TI.	Aunque se observó que en el GIT de Apoyo Informático se aplican indicadores de gestión, éstos no están relacionados a un macro-proceso de Gestión de TI.
LI.GO.13 La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar áreas con oportunidad de mejora, de acuerdo con los criterios de calidad establecidos en el Modelo Integrado de Planeación y Gestión de la institución, de modo que pueda focalizar esfuerzos en el mejoramiento de los procesos de TI para contribuir con el cumplimiento de las metas institucionales y del sector.	Se observó que el GIT de Apoyo Informático anualmente solicita a las diferentes áreas las necesidades en materia de tecnología para elaborar el Plan Anual de Adquisiciones, además se evidenció el uso del documento "Ficha de Viabilidad Técnica" donde se especifican y justifican las oportunidades de mejora en cuanto a la renovación de la plataforma tecnológica.

OBSERVACIÓN

Una vez realizado el análisis de aplicabilidad de los lineamientos que conforman los tres logros GEL establecidos en el MSPI, se obtuvieron los siguientes resultados a través de estimaciones porcentuales de avance según el detalle informado por el auditado en las tablas anteriores:

Definición del Marco de Seguridad y Privacidad de la Información: (37.5%)

Diagnóstico de Seguridad y Privacidad	
Lineamiento	**Aplicabilidad**
LI.ES.01	100%
LI.ES.02	10%
LI.GO.01	10%
LI.GO.04	10%
LI.ST.14	0%

Plan de Seguridad y Privacidad de la Información	
Lineamiento	**Aplicabilidad**
LI.ES.02	10%
LI.ES.06	10%
LI.ES.08	100%
LI.GO.01	10%
LI.GO.04	10%
LI.GO.09	100%
LI.SIS.22	80%

Implementación del Plan de Seguridad: (20%)

Gestión de Riesgos de Seguridad y Privacidad de la Información	
Lineamiento	**Aplicabilidad**
LI.INF.15	10%
LI.SIS.22	30%

Monitoreo y Mejoramiento Continuo: (55%)

Evaluación del Desempeño	
Lineamiento	**Aplicabilidad**
LI.ES.13	0%
LI.GO.03	100%
LI.GO.12	20%
LI.GO.13	100%

El promedio de aplicabilidad que según la Estrategia GEL se debió alcanzar a 2016 es del 60%, sin embargo el avance estimado de la Contaduría General de la Nación es: 37.5%

RECOMENDACIÓN

Se deben generar estrategias orientadas a la implementación de los lineamientos dictados en el marco de referencia del MSPI para el fortalecimiento del componente GEL llamado “Seguridad y Privacidad de la Información”, especialmente en lo que tiene que ver con Arquitectura Empresarial, macro-proceso de Gestión de TI, esquema de Gobierno de TI, análisis de vulnerabilidades, cifrado de información y definición de un oficial de seguridad.

Así mismo, se recomienda elaborar un cronograma dedicado para el avance y cumplimiento de la estrategia GEL de la entidad, el cual sea objeto de seguimiento mensual en las reuniones internas del GIT de Apoyo Informático y del Equipo Operativo.

6. Incidentes de Seguridad

Se realizó visita a la oficina del GIT de Apoyo informático y se revisaron los registros de los incidentes de seguridad correspondientes a las vigencias especificadas en el alcance.

Se observaron dos (2) incidentes de seguridad, el primero ocurrido del 20 de agosto de 2015 sobre el correo electrónico de la entidad en la modalidad de “phishing” y el segundo efectuado el 15 de julio de 2016 sobre la red de datos de la entidad producido por una actualización que el firewall no realizó a completitud.

En ambos casos se observó completitud en la documentación del caso, así como del análisis y solución aplicados para que el incidente no afectara los sistemas, la infraestructura tecnológica o la información que administra la entidad.

El resultado en satisfactorio.