



MINTRANSPORTE

NIT.899.999.055-4



**TODOS POR UN
NUEVO PAÍS**

PAZ EQUIDAD EDUCACIÓN



MEMORANDO

20181500020083



01-02-2018

Bogotá, 01-02-2018

PARA: Ingeniera Nayibe Cecilia Mendoza Almanza, Coordinadora Grupo Informática

DE: Jefe Oficina de Control Interno

ASUNTO: Informe Auditoría Proceso Gestión Informática

En cumplimiento al plan de gestión de esta Oficina, presento informe de la auditoría realizada por el funcionario Wilson González Tapias al proceso Gestión Informática.

Producto de la auditoría efectuada, anexo envío el informe que contiene algunas observaciones sobre las cuales le solicitamos describir en el cuadro "RESUMEN DE OBSERVACIONES" las acciones, responsables y fechas de cumplimiento tendientes a subsanarlas.

En un término máximo de diez (10) días calendario, contados a partir de la fecha de recibo de este informe, le solicito enviar su respuesta y el cuadro debidamente diligenciado, de conformidad con la circular 20163000041133 del 09/03/2016.

Cordialmente

LUZ STELLA CONDE ROMERO

Anexo: Informe de Auditoria Proceso Gestión de Informática en siete (7) folios

Copia: Doctora Paula Andrea Sánchez Gutiérrez, Secretaria General

Proyectó y elaboró: Marisol Cruz Corredor

Revisó: Dra. Luz Stella Conde

Fecha de elaboración: 01/02/2018

Número de radicado que responde: 20181500020083

Tipo de respuesta

Total () Parcial ()



OFICINA DE CONTROL INTERNO
INFORME DE AUDITORÍA
PROCESO GESTIÓN INFORMATICA
Diciembre 2017

Dependencia y/o Grupo auditado: Grupo de Informática	Dependencia Jerárquica: Secretaría General
Responsable del Proceso: Nayibe Cecilia Mendoza A.- Coordinadora Grupo Informática	Auditoría realizada por: Wilson Gonzalez Tapias – Profesional Especializado
Motivo de la auditoría: Plan de Acción vigencia 2017	
Inicio de la auditoría: 11/12/2017	Terminación de la auditoría: 29/12/2017

Introducción.

En desarrollo de las auditorías programadas en la vigencia 2017 por la Oficina de Control Interno para evaluar el grado de cumplimiento de la gestión en la entidad, se procedió a realizar verificación y análisis del manejo y desarrollo de los procedimientos relacionados con Gestión Tecnológica e Informática, encaminados a determinar su efectividad y el estado de los controles existentes.

1. Objetivo de la auditoría.

- Verificar el cumplimiento de la gestión de los servicios de tecnologías de la información y comunicaciones que contribuyan al logro del objetivo y funciones del Ministerio.
- Verificar estado, soporte preventivo y correctivo a la infraestructura de servidores y funcionario encargado de la administración.
- Verificar Plan de renovación tecnológica y vigencia de la infraestructura actual

2. Alcance.

Evaluación de la gestión desarrollada durante las vigencias 2017 en desarrollo del proceso de Gestión Tecnológica e Informática.

3. Metodología.

La auditoría se desarrollará tomando como referencia la normatividad de funciones asignadas al Grupo de informática de la Secretaría General, procesos y procedimientos del área.

1. OBSERVACIONES Y RECOMENDACIONES.

COPIAS DE SEGURIDAD

Es responsabilidad del administrador DBA - Grupo de Informática contar con las copias de respaldo de los datos y el software del data center y las copias de respaldo de las estaciones de trabajo son responsabilidad del usuario.



Es responsabilidad del DBA confirmar si el Backups automatizado opera correctamente y si la información es recuperable desde el medio de almacenamiento, el cual debe comprobarse en el servidor.

Cada tres meses, la información se debe grabar en cintas magnéticas, de las cuales un juego queda almacenado en el Data Center y otro debe ser enviado a la Bodega de Fontibón para su almacenamiento, prevención y Custodia.

De acuerdo a lo anterior el Grupo de Informática, debe ajustar el procedimiento de acuerdo al protocolo que defina el proveedor dado el nuevo servicio adquirido por la entidad – Alojamiento de la Infraestructura del Datacenter. Para dar cumplimiento al procedimiento toda vez que a Fontibón solo se ha enviado copia de seguridad hasta junio de 2017 para envío.

Recomendaciones:

- Validar y ajustar el procedimiento de copias de seguridad de acuerdo al servicio adquirido al amparo del acuerdo marco de precio de nube privada II.
- Adelantar las copias de seguridad correspondientes, y remitirlas a Fontibón tal como lo establece en el procedimiento actual.
- Adelantar un plan de pruebas para las cintas que se envían a Fontibón con el fin de mantener la confiabilidad e integridad de la Información contenida en ellas.
- Realizar un plan de pruebas y control para comprobar que el Backups automático que hace el servidor sea eficaz y eficiente en cuanto al tiempo de procesamiento, integridad de la información.

CONTROL DE ACCESO A USUARIOS.

El procedimiento establecido en el sistema de Gestión de Seguridad de la Información, indica que para la creación de usuario nuevo, es necesario que el Directivo solicite la creación en el dominio del Ministerio, la Subdirección de Talento humano debe avalar la creación del nuevo usuario y enviar al encargado de la plataforma el soporte documental de la vinculación con la solicitud de la creación del nuevo usuario.

La Subdirección de Talento Humano envía copia de la solicitud de creación del dominio al profesional encargado del correo electrónico y demás para que el usuario pueda acceder a su cuenta.

Si el usuario (funcionario de planta) deja de estar vinculado con el Ministerio de Transporte, el jefe de área debe informar al Grupo Informática de la misma manera que se hizo la solicitud para agregar la salida de dicho usuario. En este caso al usuario se le revoca el acceso tanto de dominio como de la aplicación en la que tenga acceso, guardando registro de los permisos que tenía pero sin que pueda volver a acceder a sus cuentas.

De acuerdo a lo anterior se pudo establecer que este procedimiento no se viene cumpliendo, toda vez que tanto la Subdirección de Talento Humano como el Grupo de Informática, no mantienen actualizada la información de este procedimiento, dado que existen en el registro de activos, contratistas y exfuncionarios que ya no pertenecen a este Ministerio.



Recomendación:

- Solicitar tanto a la Subdirección del Talento Humano como al Grupo Contratos el reporte de novedades de personal con oportunidad para proceder a gestionar las cuentas de usuario.
- Validar el procedimiento y en caso de requerir ajustes proceder a actualizarlo
- Dar a conocer el documento soporte del proceso gestión tecnológica e informática para que se cumpla cabalmente por los usuarios.
- Las solicitudes de desactivación de usuarios por parte de los jefes de áreas o de quien haya solicitado permisos para un usuario deben ser oportunas, a fin de evitar accesos indebidos a la información.
- Las cuentas que se creen para atender actividades propias de la entidad deben estar asociadas al jefe de la dependencia o su delegado con el fin de hacer seguimiento a la información que se transfiera.

CONCENTRACION DEL MANEJO DE LA INFRAESTRUCTURA TECNOLÓGICA

Se pudo determinar que se tiene concentrada el manejo de toda la infraestructura tecnológica de la entidad en un contratista (acceso, seguridad, instalación sistema, reconfiguración de la red, almacenamiento, Backups entre otros); lo cual indica que se le han asignado muchos perfiles para la administración y manejo de los sistemas del Ministerio; es importante indicar que esta observación ya había sido indicada en informes anteriores.

Existen contratistas de prestación de servicios que por su labor pueden convertirse en cuello de botella en caso que ya no trabajen para el Ministerio.

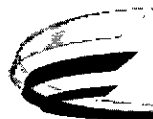
Esto genera dependencia y un alto riesgo en caso que estas personas dejen de pertenecer a la entidad.

Recomendación:

- Desconcentrar estas funciones en funcionarios de planta, capacitándolos a fin de obtener el conocimiento pleno de las herramientas requeridas para desarrollar este trabajo o que puedan ser utilizados como plan de contingencia en caso que estos funcionarios dejen de laborar para este Ministerio.
- Requerir documentación al personal contratista de la infraestructura en operación.

ADMINISTRACIÓN DE SERVICIOS DE RED BASADOS EN SERVIDORES WINDOWS:

- Autenticación Red
- Correo electrónico
- Antivirus e impresión
- APL carpetas publicas
- Servidor Intranet
- Servidor repositorio
- Dexon – Mesa de ayuda
- Orfeo



- Proxy – Acceso a internet
- Galeón
- Validar informe de actualización del sistema de seguridad de la información con el supervisor del contrato.

Autenticación de red. Aun se presentan situaciones continuas de olvido de contraseñas, existen nombres de máquinas que pertenecen a usuarios que ya han sido trasladados del área, o ya no pertenecen a la entidad.

La oficina de informática debe realizar seguimiento permanente por equipo de cómputo y establecer un mecanismo de control en coordinación con el Grupo de Talento Humano.

Antivirus e impresión. La Oficina de Informática, adelanto las acciones necesarias para evitar posibles afectaciones a los sistemas por virus para ello adelanto contrato de esta herramienta para este soporte.

Carpetas Públicas (Servidor de aplicativos y archivos específicos). En este sitio se publican los ejecutables de aplicativos y sirve como repositorio de información de interés de los usuarios internos. Sin Observaciones.

Servidor de Intranet. En él se publica la información de interés de las dependencias y depende de cada área como mantenerla actualizada. Se observa que algunas dependencias no actualizan su información, situación que afecta las consultas que efectúan los usuarios y por ende la imagen del Ministerio.

La Secretaría General a través del Grupo de Informática, adelanta seguimientos que permiten mantener actualizada la información de forma oportuna, sin embargo aún se presentan casos de áreas o dependencias que no mantienen actualizada la información de la Intranet.

Sirena. Sistema de Información de Recaudo a nivel Nacional. Funciona correctamente.

Galeón. Permite la conectividad con las Direcciones Territoriales. Presenta frecuentes caídas del sistema y los tiempos de respuesta en ocasiones se torna lento.

Servidores tipo UNIX. Se tienen 4 servidores (HP-UX) físicamente 2 equipos donde funcionan las bases de datos de la entidad como son los registros nacionales (RNA, RNC) históricos y nomina entre otros. Estos equipos trabajan con tolerancia a fallas. Sin Observaciones

Los otros 2 equipos LINUX funcionan el aplicativo Orfeo. Se presenta problema de espacio, para ello se debe organizar, optimizar para prevenir caídas del sistema Orfeo.

Se debe garantizar la renovación tecnológica con el fin de atender la obsolescencia de los equipos.

Aun se tienen aplicativos Web dispersos ya que algunas dependencias cuentan con desarrollos de sistemas de información que luego solicitan al Grupo de Informática sean incluidos en los servidores, igualmente, se desarrollan proyectos sin tener en cuenta las directrices del Grupo de Informática.



Sitio Web. En él se publica la información de interés de las dependencias y es responsabilidad de cada área de actualizarla. En algunos LINK las dependencias responsables no mantienen actualizada la información.

La Secretaría General a través del Grupo de informática, debe adelantar mecanismos que permitan mantener su actualización de forma oportuna.

Servidor Aplicativo Oracle.

La plataforma es destinada a los sistemas de información del Ministerio tales como el sistema de información de Nomina (Perno), el sistema de información manifiestos de carga y el sistema de información reposición vehicular por desintegración entre otros. Sin Observación. Sin Observación

SIIRIH. Conformado por el sistema de información de Rutas y horarios y el observatorio de carga. Funciona normalmente.

Galeón. Permite la conectividad con los aplicativos de las Direcciones territoriales (automotores, modulo empresas, escuelas, fondo de reposición) entre otros. Sin observaciones

Service Desk. La herramienta funciona correctamente.

Data Protector. Permite efectuar las copias de seguridad, de las operaciones y bases de datos que se tienen, estas son enviadas periódicamente al archivo del Ministerio en Fontibón, sin embargo la entidad no cuenta con un ambiente de prueba en caso que se necesite recuperar la información, es decir, no se cuenta con una infraestructura para restauración de Backups.

- informe de actualización del sistema de seguridad de la información

No se tiene plan de actualización de seguridad de hardware y software con vigencia de la infraestructura actual que establezcan tiempos de obsolescencia por equipo, servidores y switches entre otros.

Recomendación:

El Grupo de Informática debe contar un plan estratégico de sistema que contemple:

- El estado actual de los elementos de infraestructura TI y aspectos del Ministerio que impacten directamente en la infraestructura actual y las necesidades futuras.
- Proyectar los recursos actuales en la línea de tiempo, además ubicar las tendencias de crecimiento, y las capacidades necesarias para cumplir con los ANS. Relacionar los proyectos e iniciativas de TI futuras y se analizar los recursos necesarios por cada sistema de información y de posible o de reemplazo de infraestructura

2. RIESGOS ASOCIADOS AL PROCESO

- **Pérdida de información.**



Causas: Contaminación por virus informático Daño en servidores. Daño malintencionado Manipulación inadecuada por parte del usuario final o personal no calificado por parte de factor humano. Daño en bases de datos Intrusión de Hackers hurto y/o destrucción de información

Observación: No se ha materializado el riesgo

- **Indisponibilidad de los servicios de información.**

Causas: Falta de fluido eléctrico Daño malintencionado a la infraestructura tecnológica por parte de factor humano, des configuración de equipos Intrusión de Hackers (hurto y destrucción de información Contaminación por virus informático Daño en servidores. Daño en bases de datos, Daño o mal funcionamiento en el equipo de Aire Acondicionado del Centro de Datos, Falla en la Infraestructura Tecnológica del Centro de Datos

Observación: No se ha materializado el riesgo

- **Adquisición de hardware o software no compatibles con la infraestructura computacional de la entidad.**

Causas: Falta de experticia en tecnología del personal encargado de la contratación, No se consulta al proceso de gestión tecnológica para la adquisición de hardware o software.

Observación: No se ha materializado el riesgo

- **Obsolescencia de software y hardware.**

Causas: Falta de planeación presupuestal para la adquisición de hardware y software, Ausencia de un plan de renovación tecnológica, Rechazo a la implementación de nuevas tecnologías por parte del usuario, Falta de respaldo de los proveedores o fabricantes

Observación: No se ha materializado el riesgo

- **Falta de continuidad en el Plan de Tecnologías de la Información y las Comunicaciones TIC.**

Causas: Recorte presupuestal, Cambio en las políticas relacionadas con Tecnologías de la información y las comunicaciones.

Observación: No se ha materializado el riesgo



MINTRANSPORTE



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

Informe de Auditoría Gestión Informática

El Grupo de Informática tuvo un presupuesto asignado para la vigencia 2017 de \$5.000.000.000, de los cuales ejecuto \$4.999.887.508 millones de pesos alcanzando un 100% de su ejecución.


WILSON GONZALEZ TAPIAS
Profesional Especializado



MINTRANSPORTE



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

Informe de Auditoría Gestión Informática

ANEXO 1
CUADRO RESUMEN DE OBSERVACIONES

OBSERVACIONES	RECOMENDACIONES DE CONTROL INTERNO	DEPENDENCIA INVOLUCRADA	ACCIONES	RESPONSABLE	FECHA DE CUMPLIMIENTO
<p>Copias de seguridad. Es responsabilidad del DBA confirmar si el Backups automatizado opera correctamente y si la información es recuperable desde el medio de almacenamiento, el cual debe comprobarse en el servidor.</p> <p>Cada tres meses, la información se debe grabar en cintas magnéticas, de las cuales un juego queda almacenado en el Data Center y otro debe ser enviado a la Bodega de Fontibón para su almacenamiento, prevención y Custodia.</p> <p>De acuerdo a lo anterior el Grupo de Informática, no</p>	<ul style="list-style-type: none">- Validar y ajustar el procedimiento de copias de seguridad de acuerdo al servicio adquirido al amparo del acuerdo marco de precio de nube privada II.- Adelantar las copias de seguridad correspondientes, y remitirlas a Fontibón tal como lo establece en el procedimiento actual.- Adelantar un plan de pruebas para las cintas que se envían a Fontibón con el fin de mantener la confiabilidad e integridad de la Información contenida en ellas.- Realizar un plan de pruebas y control para comprobar que el Backups automático que hace el servidor sea eficaz y eficiente en cuanto al tiempo de procesamiento, integridad de la información.	Secretaria General- Grupo de Informática			



MINTRANSPORTE



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

Informe de Auditoría Gestión Informática

viene cumpliendo con este procedimiento toda vez que a Fontibón solo se ha enviado copia de seguridad hasta junio de 2017 para envío.					
<p>Control de acceso a usuarios.</p> <p>El procedimiento establecido en el sistema de Gestión de Seguridad de la Información, indica que para la creación de usuario nuevo, es necesario que el Directivo solicite la creación en el dominio del Ministerio, la Subdirección de Talento humano debe avalar la creación del nuevo usuario y enviar al encargado de la plataforma el soporte documental de la vinculación con la solicitud de la creación del nuevo usuario.</p> <p>De acuerdo a lo anterior se pudo establecer que este procedimiento no viene cumpliendo, toda vez que</p>	<ul style="list-style-type: none">-Solicitar tanto a la Subdirección del Talento Humano como al Grupo Contratos el reporte de novedades de personal con oportunidad para proceder a gestionar las cuentas de usuario.-Validar el procedimiento y en caso de requerir ajustes proceder a actualizarlo-Dar a conocer el documento soporte del proceso gestión tecnológica e informática para que se cumpla cabalmente por los usuarios.-Las solicitudes de desactivación de usuarios por parte de los jefes de áreas o de quien haya solicitado permisos para un usuario deben ser oportunas, a fin de evitar accesos indebidos a la información.-Las cuentas que se creen para atender actividades propias de la entidad deben estar asociadas al jefe de la dependencia o su delegado con el fin de hacer seguimiento a la información que se transfiera.	Secretaria General- Grupo de Informática			



MINTRANSPORTE



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

Informe de Auditoría Gestión Informática

<p>tanto la Subdirección de Talento Humano como el Grupo de Informática, no mantienen actualizada la información de este procedimiento, dado que existen en el registro de activos contratistas, exfuncionarios que ya no pertenecen a este Ministerio.</p>					
<p>Concentración del manejo de la infraestructura tecnológica</p> <p>Se pudo determinar que se tiene concentrada el manejo de toda la infraestructura tecnológica de la entidad en un contratista (acceso, seguridad, instalación sistema, reconfiguración de la red, almacenamiento, Backups entre otros); lo cual indica que se le han asignado muchos perfiles para la administración y manejo de los sistemas del Ministerio; es importante</p>	<p>-Desconcentrar estas funciones en funcionarios de planta, capacitándolos a fin de obtener el conocimiento pleno de las herramientas requeridas para desarrollar este trabajo o que puedan ser utilizados como plan de contingencia en caso que estos funcionarios dejen de laborar para este Ministerio.</p> <p>-Requerir documentación al personal contratista de la infraestructura en operación.</p>	<p>Secretaria General- Grupo de Informática</p>			



MINTRANSPORTE



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

Informe de Auditoría Gestión Informática

indicar que esta observación ya había sido indicada en informes anteriores. Esto genera dependencia y un alto riesgo en caso que estas personas dejen de pertenecer a la entidad.					
Administración de servicios de red basados en servidores windows: Autenticación de red. Aun se presentan situaciones continuas de olvido de contraseñas, existen nombres de máquinas que pertenecen a usuarios que ya han sido trasladados del área, o ya no pertenecen a la entidad. Servidor de Intranet. En él se publica la información de interés de las dependencias y depende de cada área como mantenerla actualizada. Se observa que algunas dependencias no	<ul style="list-style-type: none">-Realizar seguimiento permanente por equipo de cómputo y establecer un mecanismo de control en coordinación con el Grupo de Talento Humano-Se debe garantizar la renovación tecnológica con el fin de atender la obsolescencia de los equipos-La Secretaría General a través del Grupo de informática, debe adelantar mecanismos que permitan mantener su actualización de forma oportuna	Secretaría General-Grupo de Informática			



MINTRANSPORTE



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

Informe de Auditoría Gestión Informática

<p>actualizan su información.</p> <p>-Aun se tienen aplicativos Web dispersos ya que algunas dependencias cuentan con desarrollos de sistemas de información que luego solicitan al Grupo de Informática sean incluidos en los servidores, igualmente, se desarrollan proyectos sin tener en cuenta las directrices del Grupo de Informática.</p> <p>Sitio Web. En él se publica la información de interés de las dependencias y es responsabilidad de cada área de actualizarla. En algunos LINK las dependencias responsables no mantienen actualizada la información</p> <p>Data Protector. Permite efectuar las copias de seguridad, de las operaciones y bases de</p>					
--	--	--	--	--	--



MINTRANSPORTE



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

Informe de Auditoría Gestión Informática

datos que se tienen, estas son enviadas periódicamente al archivo del Ministerio en Fontibón, sin embargo la entidad no cuenta con un ambiente de prueba en caso que se necesite recuperar la información, es decir, no se cuenta con una infraestructura para restauración de Backups.					
---	--	--	--	--	--