Agencia Nacional de Infraestructura

Avenida Calle 24A Nro. 59-42 Torre 4 Piso 2.
PBX: 4848860 – www.ani.gov.co
Nit. 830125996-9. Código Postal ANI 110221.

Para contestar cite:
Radicado ANI No.: **20191020128003**
Fecha: **30-08-2019**

MEMORANDO

Bogotá D.C.

PARA: **Dr. LOUIS FRANCOIS KLEYN LÓPEZ**
Presidente

Dr. DIEGO ALEJANDRO MORALES SILVA
Vicepresidente de Planeación, Riesgos y Entorno

Ing. ANDRÉS FRANCISCO BOADA
Coordinador G.I.T. Tecnologías de la Información y las Telecomunicaciones

DE: **GLORIA MARGOTH CABRERA RUBIO**
Jefe Oficina de Control Interno

ASUNTO: Informe de evaluación integral a los componentes de hardware, software y seguridad de la información.

Respetados Señores:

La Oficina de Control Interno, en el mes de agosto de 2019, realizó la auditoría correspondiente a la evaluación integral a los componentes de hardware, software y seguridad de la información.

Las conclusiones y recomendaciones se describen en el capítulo 7 del informe que se anexa a la presente comunicación, con el fin que se coordinen las acciones tendientes a la atención de las recomendaciones realizadas.

Cordial saludo,

GLORIA MARGOTH CABRERA RUBIO
Jefe Oficina de Control Interno

Anexos: Informe 11 folios

cc: 1) DIEGO ALEJANDRO MORALES SILVA (VICE) Vicepresidencia de Planeacion Riesgos y Entorno BOGOTA D.C. -2) ANDRES FRANCISCO BOADA 1 (COOR) GIT de Tecnologias de la Informacion y las Telecomunicaciones BOGOTA D.C.
Proyectó: Juan Diego Toro Bautista – Oficina de Control INterno
VoBo: GLORIA MARGOTH CABRERA RUBIO (JEFE)
Nro Rad Padre:
Nro Borrador: 20191020044907
GADF-F-010

Agencia Nacional de Infraestructura

GOBIERNO DE COLOMBIA

INFORME DE AUDITORÍA




Evaluación integral a los componentes de hardware, software y seguridad de la información.

2019

CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. METODOLOGÍA 3
4. MARCO NORMATIVO 5
5. VERIFICACIÓN DE ANTECEDENTES 5
6. DESARROLLO DEL INFORME 6
6.1. Revisión centros de datos 6
6.1.1. Centro de datos segundo piso 6
6.1.2. Centros de datos pisos sexto, séptimo y octavo 9
6.2. Revisión de políticas, planes y gestión documental 11
6.2.1. Política de Seguridad y Privacidad de la Información 11
6.2.2. Plan Estratégico de Tecnologías de la Información 11
6.2.3. Gestión documental 14
6.3. Tratamiento de incidentes de seguridad 16
6.4. Revisión avance transición del protocolo IPv4 a IPv6 18
6.5. Revisión mantenimientos infraestructura 20
7. CIERRE DE LA AUDITORÍA, CONCLUSIONES Y RECOMENDACIONES 21
7.1. Conclusiones 21
7.2. Recomendaciones 21

1. OBJETIVO

Contribuir con la identificación de oportunidades de mejora, a través de la revisión de los controles y la prevención, para una mayor y mejor utilización de los recursos informáticos, con garantías de integridad, confidencialidad y disponibilidad de la información.

2. ALCANCE

Evaluar la utilización, aprovechamiento y seguridad de la infraestructura dedicada al apoyo tecnológico de la Entidad, a través de la verificación de los planes, políticas y procedimientos relacionados y la revisión de los controles preventivos implementados por el Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, para el periodo comprendido entre el 1 de enero y el 15 de agosto de 2019.

En auditorías anteriores se ha evaluado la infraestructura tecnológica desde los inventarios tecnológicos y los centros de datos, sin embargo, en esta oportunidad el alcance de la auditoría se determinó para revisar los controles implementados para la prevención de ataques y asegurar el correcto funcionamiento de la infraestructura, en los siguientes temas claves:

- Cuarto de datos piso 2
- Transición protocolo IPv4 a IPv6
- Catálogo de servicios
- Mantenimientos
- Pólizas
- Planes, políticas, procedimientos
- Incidentes de seguridad

3. METODOLOGÍA

La metodología empleada por la Oficina de Control Interno fue la usualmente aceptada para la elaboración de este tipo de informes de acuerdo con las normas de auditoría, para lo cual se realizó la planeación y ejecución de trabajo, donde se tuvieron en cuenta los siguientes aspectos:

- *Solicitud de información al Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones:* El día 9 de agosto de 2019, mediante correo electrónico adjunto a los papeles de trabajo, se solicitó la información correspondiente al mapa de ruta de implementación de Arquitectura empresarial de tecnología; el catálogo de servicios de TI; la Estrategia de uso y apropiación de TI; el plan operativo del GIT de Tecnologías de la Información y las Telecomunicaciones; los indicadores del PETI y de los demás aspectos susceptibles de medición de la gestión; los reportes de los incidentes de seguridad para 2018

y 2019, incluyendo el reporte, registro y atención; relación de los contratos suscritos relacionados con mantenimientos correctivos y preventivos al hardware, software y seguridad; relación de las pólizas de corriente débil; y el cronograma y documentación relacionada con la transición del protocolo IPv4 a IPv6.

Esta información fue allegada a esta auditoría el miércoles 14 de agosto de 2019, cumpliendo con la fecha estipulada en el comunicado y atendiendo en completitud el requerimiento.

- *Apertura de la auditoría:* El día 14 de agosto de 2018, mediante acta (Formato EVCI-F-001) adjunta a los papeles de trabajo, se dio apertura al ejercicio auditor, informando el objetivo, alcance, criterios y las fechas de las actividades principales.

- *Entrevista:* El día 14 de agosto de 2019, se efectuó entrevista al líder del GIT de Tecnologías de la Información y las Telecomunicaciones, quien con su equipo dio respuesta a cada uno de los temas relacionados en el alcance de la auditoría sustentando con los respectivos soportes. En el marco de la entrevista se solicitaron evidencias adicionales, con compromiso de entrega para el día 22 de agosto de 2019.

  Esta información fue allegada a esta auditoría el jueves 22 de agosto de 2019, cumpliendo con la fecha estipulada en el comunicado y atendiendo en completitud el requerimiento adicional.

- *Inspección centros de datos:* Los días: viernes 16 de agosto y martes 20 de agosto de 2019, se visitaron los centros de datos de los pisos 6 y 7, y pisos 2 y 8 respectivamente, por parte del apoyo técnico de la auditoría.

- *Socialización de resultados y cierre de la auditoría:* El lunes 26 de agosto de 2019, se socializaron, al líder del Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones, los resultados de la auditoría y se brindó el espacio para las aclaraciones y o allegar soportes para conjurar las eventuales situaciones evidenciadas en el ejercicio auditor. La anterior actividad se encuentra soportada mediante acta que reposa en los papeles de trabajo.

Los resultados de estas actividades se presentan en este informe de auditoría, en el que se incluyen las recomendaciones y las oportunidades de mejora identificadas para afrontar eventuales situaciones de riesgo que comprometan la integridad, confiabilidad y disponibilidad de la información que involucra a la Agencia y sus funcionarios.

4. MARCO NORMATIVO

A continuación, se describe el marco legal e institucional, bajo el cual se realizó la auditoría:

- Constitución Política de Colombia Artículos 1, 2, 23,103,209 y 270
- Ley 87 de 1993, *"Por la cual se establecen normas para el ejercicio de control interno en la entidades y organismos del estado y se dictan otras disposiciones"*.
- Decreto 648 de 2017 Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.
- Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Resolución No. 2710 de 2017 del Ministerio de Tecnologías de la Información y las comunicaciones "Por la cual se establecen lineamientos para la adopción del protocolo IPv6"
- Política de Seguridad y Privacidad de la Información – GICO-PT-001 del 25 de mayo de 2019.
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI 2019-2022 V2 del 30 de mayo de 2019.
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información V2 del 1 de febrero de 2019.
- Caracterización del proceso Gestión de Información y Comunicaciones V6 del 26 de noviembre de 2018.
- Procedimiento identificación de necesidades y soluciones tecnológicas V3 del 6 de julio de 2018.
- Procedimiento Gestión de Cambios V1 del 6 de julio de 2018.

En materia de buenas prácticas y Sistema de Gestión de Seguridad de la Información:

- ISO /IEC 20001:2007
- ISO 27001 e ISO 27002
- COBIT
- ICREA 2011

5. VERIFICACIÓN DE ANTECEDENTES

En lo pertinente al Plan de Mejoramiento Institucional, se precisa que no se evidenciaron hallazgos relacionados al componente de Tecnologías de la Información y Comunicaciones.

De igual manera, en lo relacionado con el Plan de Mejoramiento por Procesos, no se evidenciaron no conformidades.

6. DESARROLLO DEL INFORME

De acuerdo con los apartes anteriores y la metodología aplicada en la auditoría, se elaboró una lista de chequeo, que contemplara todos los temas relevantes para medir el porcentaje de cumplimiento de la normatividad y de las buenas prácticas.

Los capítulos que conforman la auditoría se enuncian a continuación:

1. Revisión centros de datos.
2. Revisión de políticas, planes y gestión documental.
3. Tratamiento de incidentes de seguridad.
4. Revisión avance transición del protocolo IPv4 a IPv6.
5. Revisión mantenimientos preventivos.

6.1. Revisión centros de datos

La Entidad cuenta con 4 centros de datos: uno principal ubicado en el segundo piso y 3 auxiliares en los pisos 6, 7 y 8 (dividido en 2 cuartos). Consecuente con lo manifestado en el alcance de la auditoría, en los últimos tres ejercicios anteriores (auditorías) se ha realizado la verificación completa de la infraestructura de los centros de cómputo, obteniendo sendos resultados favorables, razón por la cual, en la presente auditoría se efectuó una inspección a temas principales, como: aseo y organización, verificación del acceso restringido, revisión de equipos portátiles para extinción de incendios y disposición del cableado estructurado en los racks, obedeciendo a que son precisamente estos temas, los que pueden generar la materialización del riesgo *de indisponibilidad de los recursos tecnológicos*.

6.1.1. Centro de datos segundo piso

En visita de inspección al centro de cómputo del segundo piso se evidenció que la puerta del centro de datos permanece abierta y bloqueada para que no se cierre con el extintor destinado a ese centro de cómputo, tal y como se puede apreciar en las siguientes fotos:

Adicionalmente se evidenció que el equipo de aire acondicionado no funciona y la puerta del cuarto donde se encuentra ubicado, también está abierto; de igual forma se observan objetos que no le pertenecen, como se puede apreciar en la siguiente imagen.

Lo anterior genera las siguientes situaciones, algunas que aumentan la probabilidad de materialización del riesgo de indisponibilidad de los recursos tecnológicos:

a. En reemplazo del equipo de ventilación se le deja la labor a los disipadores de calor de los racks, los cuales deben emplear toda su potencia. El ruido generado por los disipadores de calor de los racks alcanza los 80db, valor que dobla el ruido cotidiano que se percibe en una oficina. Este parecería un impacto menor, sin embargo, la alta exposición a este ruido constante puede causar problemas auditivos, en especial a quienes ocupan las oficinas que colindan con el centro de datos.

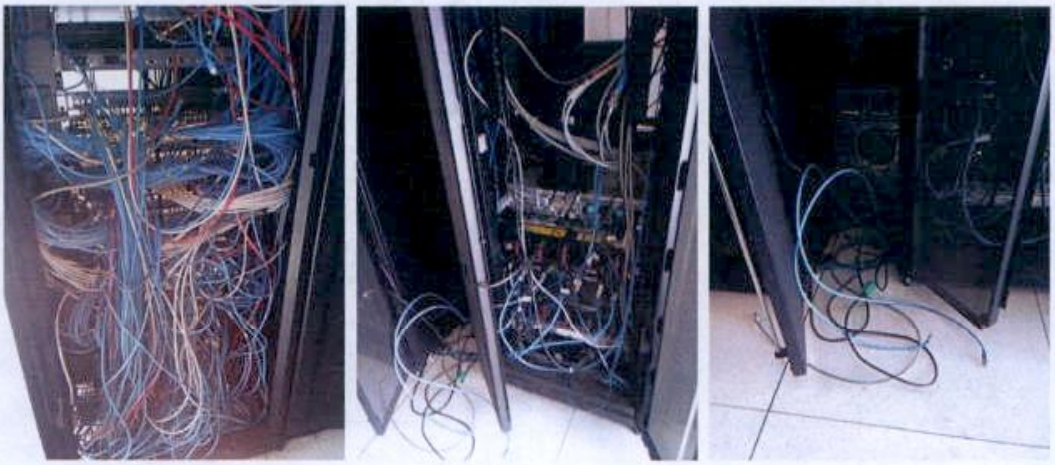
Muestra tomada con un sonómetro no profesional

b. El daño del equipo de refrigeración del centro de datos y la insuficiencia de la fuente de ventilación actual se refleja en la alta sensación térmica del cuarto por encima de los 35° C, lo cual puede ocasionar recalentamiento en los servidores, equipos de cómputo, de red y de comunicaciones, contenidos en este centro. De igual manera, genera amenaza de incendio y por ende la materialización del riesgo de indisponibilidad de los recursos tecnológicos.

c. Por último, el daño del equipo de refrigeración hace necesario mantener la puerta del centro de datos abierta de manera permanente, lo cual impide tener el control del acceso biométrico, a pesar de que este último se encuentra en perfecto estado, no está cumpliendo con el fin de controlar el acceso a personal ajeno. Lo anterior se agrava en virtud de la cercanía con las ventanillas de archivo y correspondencia que atienden a diario un gran volumen de personas externas, que pueden de manera accidental o malintencionada ocasionar un mal funcionamiento o la perdida parcial o total de información sensible. De igual manera, esta situación incrementa el riesgo de indisponibilidad de los recursos tecnológicos.

Finalmente, se observa desorganización en el cableado estructurado y equipos de cómputo por fuera de los racks, lo cual puede generar mal funcionamiento de los equipos clientes de la organización, aumenta la amenaza de desconexión de máquinas accidentalmente y dificulta la identificación de

fallas en las comunicaciones y eleva el tiempo de solución para daños relacionados con los puntos de red.



En entrevista con el GIT de Tecnologías de la Información y las Telecomunicaciones manifiestan que el arreglo del aire acondicionado, debido a su antigüedad, rondaría la suma de los $50 millones de pesos. En razón a lo anterior, se adelantó el proceso de mínima cuantía No. VJ-VPRE-MC-014-2019, cuyo objeto es *"Adquisición e instalación de un sistema de ventilación para el centro de cómputo principal de la Agencia Nacional de Infraestructura – ANI"*, por valor de $12.6 millones, suscribiéndose el contrato VPRE 509-2019 con fecha 12 de agosto de 2019.

Lo anterior es prenda de garantía para la solución de las situaciones expuestas con anterioridad, exceptuando la problemática evidenciada de organización del cableado estructurado, orden y aseo, que se hará dentro de las recomendaciones al final de este subcapítulo.

6.1.2. Centros de datos pisos sexto, séptimo y octavo

En visita de inspección a los centros de datos de estos pisos, se evidencia desorden en el cableado estructurado en los racks y objetos que no deben estar en estos cuartos, tal y como se puede comprobar en las siguientes imágenes:

Piso 6

Piso 7

Piso 7

Piso 8

Los demás aspectos como los accesos restringidos, los equipos portátiles de extinción de incendio que se encuentran cargados y vencen en marzo de 2020, no presentan inconvenientes.

Como conclusión de este subcapítulo se recomienda programar y adelantar jornadas de identificación y peinado del cableado estructurado de los centros de cómputo de los diferentes pisos,

evitando así un mal funcionamiento de los equipos clientes de la organización, disminuir la amenaza de desconexión de máquinas accidentalmente y facilitar la identificación de fallas en las comunicaciones que eleva el tiempo de solución para daños relacionados con los puntos de red.

De igual manera, se recomienda mantener aseados y despejados los corredores de transito de los centros de cómputo; no solamente porque el polvo puede afectar los equipos, sino porque también, puede ocasionar accidentes u obstaculizar la libre circulación del aire, ocasionando recalentamiento en los equipos.

6.2. Revisión de políticas, planes y gestión documental

En el marco de la auditoría se revisaron los documentos que imparten los lineamientos para el Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones y que repercuten en la gestión de la Entidad y en el aseguramiento del apoyo y de las buenas prácticas en materia de tecnología en los demás procesos, específicamente la Política de Seguridad y Privacidad de la Información, el Plan Estratégico de Tecnologías de la Información – PETI.

6.2.1. Política de Seguridad y Privacidad de la Información

Se cuenta con la política codificada en el Sistema de Gestión de Calidad bajo el código GICO-PT-001 versión 2 con fecha de actualización 25 de mayo de 2019. Esta política se encuentra publicada y es socializada vía página web de la Entidad, bajo el link https://www.ani.gov.co/sites/default/files/sig/gico-p-001_politica_de_seguridad_y_privacidad_de_informacion_v2.pdf.

Esta política fue aprobada en el Comité Institucional de Gestión y Desempeño el día 28 de mayo de 2019, como consta en el acta No. 58 del Comité.

La política se encuentra alineada con lo dispuesto en la Estrategia de Gobierno en Línea según lo establecido en el Decreto 1078 de 2015 e incluye los parámetros establecidos en la Guía para la elaboración de la política general de seguridad y privacidad de la información del MINTIC de fecha 11 de mayo de 2016.

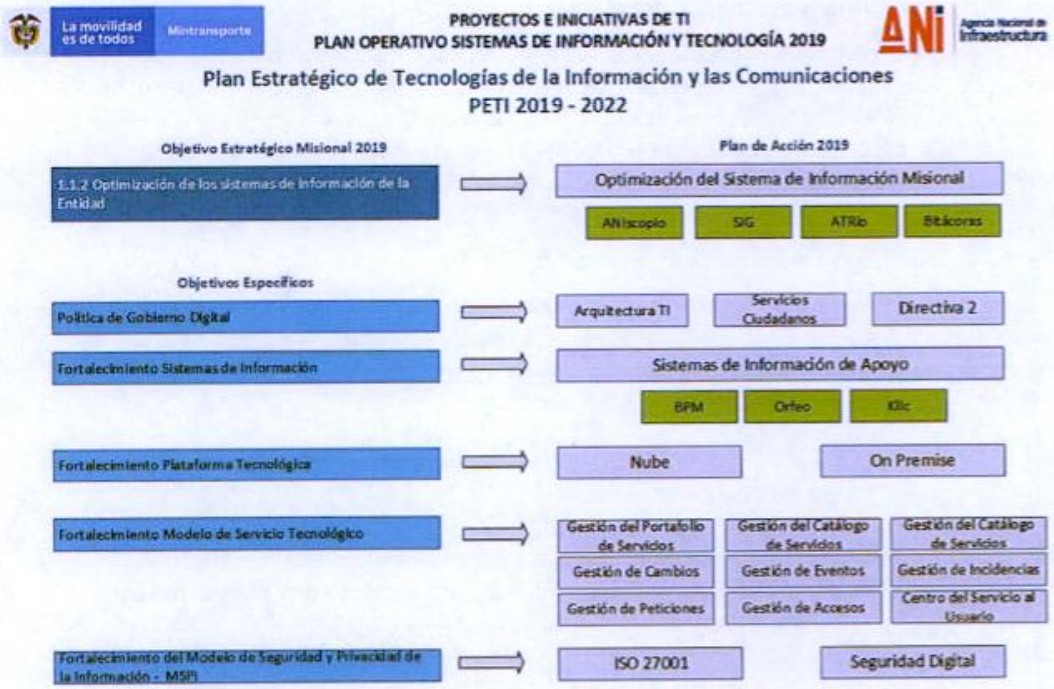
6.2.2. Plan Estratégico de Tecnologías de la Información

La Entidad dispone del Plan que dispone lo estratégico en temas de TI para el periodo 2019-2022. El Plan, en su versión No. 2, se encuentra publicado en la página web y fue revisado y actualizado el 30 de mayo de 2019.

El plan estratégico de tecnologías de la información "PETI", se formuló considerando los lineamientos emitidos por la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las

Comunicaciones (MinTIC), buscando la alineación de los procesos de la Agencia con la tecnología con el fin de generar valor tanto al interior como hacia el exterior de la Entidad.

El planteamiento de la Estrategia TI, está orientado a la protección y conservación del activo informático y toda la infraestructura tecnológica; alineada con el plan de desarrollo vigente, la planeación estratégica del sector y de la Agencia, con el propósito de optimizar los recursos y visionar las necesidades actuales conforme a la demanda de protección y salvaguarda de la información.



Para el 30 de mayo de 2019 el mapa de ruta trazado estratégicamente para el año 2019, contempla las siguientes metas y reportaba los siguientes estados de avance:

PROYECTOS E INICIATIVAS DE TI
PLAN OPERATIVO SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA 2019

	Metas	Estado
1	Generación del reporte de seguimiento al avance de los proyectos carreteros	Terminado
2	Formulación PETI 2019-2022	En Proceso
3	Formulación plan de tratamiento de riesgos de seguridad de la información	Terminado
4	Formulación plan de gestión de seguridad de la información	Terminado
5	Ajuste al servicio de interoperabilidad con MinTransporte	Terminado
6	Generación del reporte de PINES	Por Hacer
7	Revisión del funcionamiento técnico de los módulos de ANISCOPIO	En Progreso
8	Revisión al portal de información geográfica	En Progreso
9	Conformación del equipo de profesionales y técnicos para el fortalecimiento del sistema de información misional de la Agencia	En Progreso
10	PSPI - Gestionar la aprobación de la política general de seguridad y privacidad de la información	En Prueba
11	PSPI - Gestionar la aprobación de los documentos que integren el sistema de calidad relacionados con el modelo de seguridad y privacidad de la información	En Progreso
12	PSPI - Realizar la matriz de valoración de riesgos de seguridad de la información del proceso GICO	En Progreso
13	PTRS - Definición de controles para el tratamiento de los riesgos de seguridad de la información del proceso GICO	Por Hacer
14	PTRS - Implementación de controles para el tratamiento de los riesgos de seguridad de la información de GICO	Por Hacer

Consecuente con la obligación de efectuar revisiones periódicas al PETI, el GIT de Tecnologías de la Información y las Telecomunicaciones realizó una actualización con fecha 12 de julio de 2019, incluyendo lo siguiente: Cambio a G.I.T Tecnologías de la Información y las Telecomunicaciones, Diagnóstico Interoperabilidad y Diagnóstico Autenticación Electrónica. De igual manera, en la actualidad los indicadores de las metas del Plan presentan los siguientes avances:

PROYECTOS E INICIATIVAS DE TI
PLAN OPERATIVO G.I.T. TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES 2019

	Metas	Recurso	Apoyo	Cúando	Estado
1	Generación del reporte de seguimiento al avance de los proyectos carreteros	Miguel Gonzalez		Mayo	Terminado
2	Formulación PETI 2019-2022	Luis Fernando Morales		Mayo	Terminado
3	Formulación plan de tratamiento de riesgos de seguridad de la información	Oscar Ramos		Enero	Terminado
4	Formulación plan de gestión de seguridad de la información	Oscar Ramos		Enero	Terminado
5	Ajuste al servicio de interoperabilidad con MinTransporte	Miguel Gonzalez		Julio	Terminado
6	Generación del reporte de PINES	Miguel Gonzalez		Diciembre	Por Hacer
7	Revisión del funcionamiento técnico de los módulos de ANISCOPIO	Miguel Gonzalez		Septiembre	En Progreso
8	Revisión al portal de información geográfica	Daniel Bula		Mayo	Terminado
9	Conformación del equipo de profesionales y técnicos para el fortalecimiento del sistema de información misional de la Agencia	Bibiana Alvarez		Junio	Terminado
10	PSPI - Gestionar la aprobación de la política general de seguridad y privacidad de la informacion	Andrés Boada		Mayo	Terminado
11	PSPI - Gestionar la aprobación de los documentos que integren el sistema de calidad relacionados con el modelo de seguridad y privacidad de la informacion	Guillermo Cadena		Diciembre	En Progreso
12	PSPI - Realizar la matriz de valoración de riesgos de seguridad de la información del proceso GICO	Oscar Ramos		Mayo	Terminado
13	PTRS - Definicion de controles para el tratamiento de los riesgos de seguridad de la información del proceso GICO	Guillermo Cadena		Diciembre	Por Hacer
14	PTRS - implementacion de controles para el tratamiento de los riesgos de seguridad de la información de GICO	Guillermo Cadena		Diciembre	Por Hacer

Es importante mencionar que estas modificaciones ya fueron socializadas al Vicepresidente de Planeación, Riesgos y Entorno y esta pendiente su publicación en la página web de la Entidad.

Como conclusión de este subcapítulo, se establece que el documento revisado cumple con la normatividad vigente, está actualizado, se encuentra alineado con la necesidad de la Entidad en materia de TI y está publicado como compromiso de socialización a través de la página web de la Entidad.

6.2.3. Gestión documental

Actualmente el GIT de Tecnologías de la Información y las Telecomunicaciones cuenta con la caracterización del proceso GICO-C-001 Gestión de la Información y las Comunicaciones en su versión 6 de fecha 26 de noviembre de 2018 cuyo objetivo es *"Brindar el apoyo tecnológico necesario para soportar el direccionamiento estratégico y operativo de la Entidad, a través de la formulación, ejecución y apropiación de proyectos de tecnología informática; y la gestión y mantenimiento de los servicios tecnológicos ofrecidos dentro del Catálogo de TI, así como la gestión de la seguridad de la información de acuerdo a la normatividad vigente y al marco de referencia adoptado por la Entidad"*.

Este proceso incluye dos procedimientos:

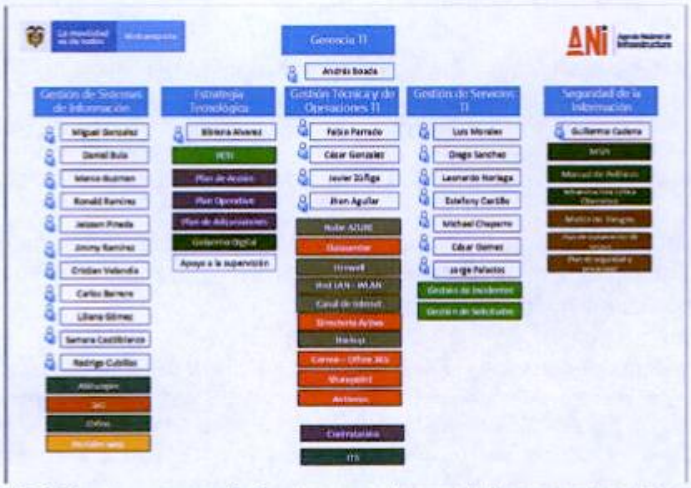
- GICO-P-001 Identificación de necesidades y soluciones tecnológicas V3 del 6 julio 2018
- GICO-P-006 Gestión de cambios en tecnología de información V1 del 6 julio 2018

En auditorías anteriores se ha recomendado la actualización de la gestión documental de tal manera que incluya las diferentes actividades y la alineación con las políticas modernas de gobierno digital.

En la entrevista de auditoría se aportó el memorando No. 2019-607-010381-3 del 19 de julio de 2019 cuyo asunto es: "Solicitud cambio de nombre del proceso GESTIÓN DE LA INFORMACIÓN Y COMUNICACIONES (GICO)" y cuyo cuerpo manifiesta lo siguiente:

> *"Por medio del presente, solicito en mi condición de líder del proceso GESTIÓN DE LA INFORMACIÓN Y COMUNICACIONES (GICO) poner en consideración del próximo comité MIPG el cambio del nombre de dicho proceso por el de GESTIÓN TECNOLÓGICA (GTEC). Dicha solicitud se justifica en virtud de la Resolución 821 del 10 de Junio del 2019, la cual modificó la Resolución No 2042 de 2018 "Por medio de la cual se modifica se establecen los Grupos Internos de trabajo en las diferentes dependencias de la escritura orgánica de la Agencia Nacional de Infraestructura, se definen sus fundones y las de sus Coordinadores", modificada por la Resolución No 567 de 2019, en el sentido de crear en la Vicepresidencia de Planeación, Riesgos y Entorno, un nuevo grupo interno de trabajo, denominado: Grupo Interno de Trabajo de tecnologías de la Información y las Telecomunicaciones.*
>
> *Por lo anterior, se está actualizando la caracterización, el objeto y el alcance del proceso, así como una revisión documental general en la que se incluye procedimientos, formatos, instructivos, políticas y manuales."* (Subrayado fuera de texto)

En razón a lo anterior, el GIT se encuentra trabajando en la construcción de la caracterización del proceso, cuyo objetivo propuesto es el siguiente: *"Liderar la transformación digital de la Agencia a través del uso de la tecnología y la innovación brindando los servicios TI que permita el cumplimiento de los objetivos de la entidad y el relacionamiento con los ciudadanos."*. De la misma forma, el GIT esta definiendo sus procedimientos con base en el siguiente esquema:



Contemplado la definición de un procedimiento por cada uno de los paquetes claves del GIT alineados a la política de Gobierno Digital:

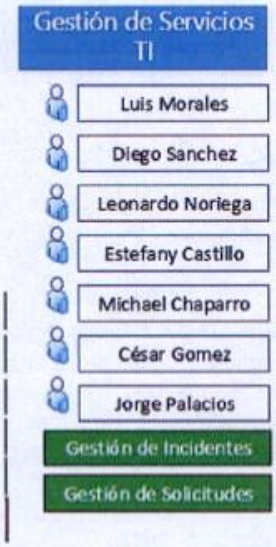
- Gestión de Sistemas de Información
- Estrategia Tecnológica
- Gestión Técnica y de Operaciones TI
- Gestión de Servicios TI
- Seguridad de la Información

Como conclusión de este subcapítulo, se evidencia el compromiso del GIT en la tarea de alinear el proceso con las disposiciones vigentes por el Ministerio de las TIC´s en su Política de Gobierno Digital.

6.3. Tratamiento de incidentes de seguridad

A partir del mes de mayo de 2019 el GIT de Tecnologías de la Información y las Telecomunicaciones viene adelantando el tratamiento a los incidentes de seguridad ocurridos en la Entidad. Esta buena práctica permite consolidar una base de conocimiento de seguridad. Es importante hacer claridad frente a la diferencia de los reportes de fallas de hardware o de software que son comunes y que su solución se realiza a través de la mesa de ayuda. Los incidentes de seguridad deben ser tratados por personal especializado.

El GIT ha incluido esta actividad dentro del nuevo esquema bajo la gestión de servicios de TI:



En ese contexto, el GIT evidencia los soportes de tres incidentes de seguridad:

- Incidente: Indisponibilidad Pagina Web.
  Fecha De Inicio: miércoles 8 de mayo 8:30am
  Se evidencia mensaje de error en el portal web el cual no permite ingreso al front end y back end.

- Incidente: Reporte Recepción de Correos Sospechosos en Cuentas Institucionales.
  Fecha De Inicio: lunes 5 de agosto 2019 – 2:02 pm
  Se recibe reporte de recepción de correos con dudosa procedencia o al menos no identificados.

- Incidente: Reporte intento de Phishing (suplantación de identidad) en Cuentas Institucionales.
  Fecha De Inicio: lunes 15 de julio 2019 – 9:08 am
  Se recibe reporte de intento de suplantación de identidad de usuario.

En el tratamiento de cada uno de estos incidentes el GIT definió el plan de acción, en los casos donde se necesitaba aplicó una solución temporal, al igual que controló el tiempo de afectación, si se reiteró el incidente y el nuevo plan de acción, la solución definitiva, el tiempo de afectación entre el suceso primigenio y la reiteración; y por último, el plan de mejoramiento incluyendo las acciones correctivas y preventivas.

Se recomienda continuar adelantando esta buena práctica y formalizar la información en un formato de reporte para unificar los tratamientos e ir consolidando la base de datos de conocimiento y tratamiento de incidentes de seguridad.

6.4. Revisión avance transición del protocolo IPv4 a IPv6[1]

El Manual de Gobierno Digital ha dispuesto dos herramientas que permiten medir y evaluar el avance en los indicadores de cumplimiento para los habilitadores transversales de Arquitectura y de Seguridad.

El habilitador transversal de Arquitectura busca que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI. El habilitador de Arquitectura soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar.

Este habilitador contiene seis (6) dominios del Marco de Referencia de Arquitectura Empresarial, específicamente el dominio de servicios tecnológicos. Este dominio permite gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en las instituciones.
Este dominio evalúa lo dispuesto en la Resolución No. 2710 del 3 de octubre de 2017 "Por la cual se establecen lineamientos para la adopción del protocolo IPv6" y en la Cartilla Guía de Transición del IPv4 a IPv6 del Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC versión 1.0.2. del 30 de mayo de 2019.

---

[1] El Protocolo de Internet (IP) es un elemento de direccionamiento de Internet que permite por medio de conmutación de paquetes la interacción de toda clase de dispositivos y aplicaciones conectados a la red, el protocolo confiere a cualquier dispositivo conectado un número que representa su dirección en la red mundial de internet.

Actualmente el protocolo de Internet que se está utilizando es la versión número 4 (IPv4), con direcciones de 32 bits de longitud, lo que equivale a un total de: 4.294.967.296 de direcciones IP.

Que el 10 de junio de 2014, la entidad responsable del Registro de Direcciones de Internet para América Latina y el Caribe, (LACNIC por sus siglas en inglés) la cual depende de la Autoridad Mundial para la Asignación de Números de Internet (IANA por sus siglas en inglés); anunció el agotamiento del stock de direcciones IPv4 y expresó su preocupación por la demora de los gobiernos y proveedores de servicio de internet – ISP en la adopción de la versión 6 del protocolo (IPv6) en la región.

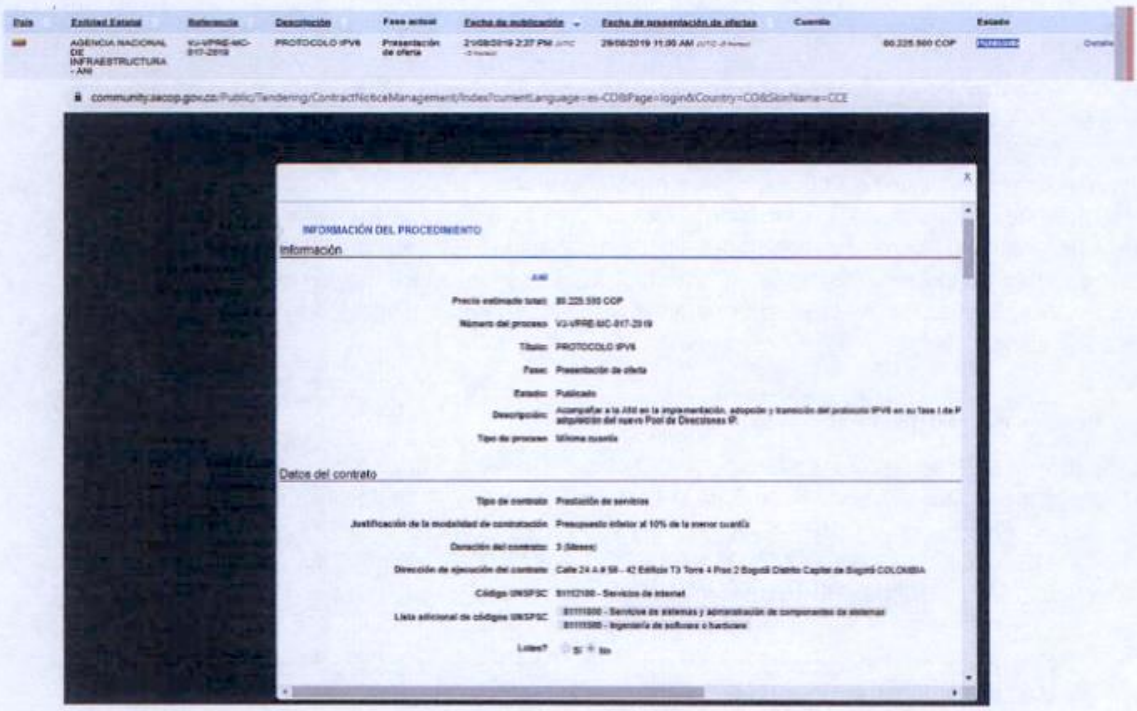
Que el agotamiento de las direcciones IPv4 conlleva a un estancamiento en el desarrollo de nuevos servicios, aplicaciones y tecnologías basadas en internet, dado que el número de dispositivos conectados a la red crece exponencialmente y no habría direcciones disponibles que soporten dicha demanda.

En razón a lo anterior, esta adopción se da en tres fases, la fase de planeación, la fase de implementación y la fase pruebas de funcionalidad. La adopción de este protocolo está reglamentado a través de la Resolución 2710 de 2017, con un plazo máximo de adopción para el 31 de diciembre de 2019.

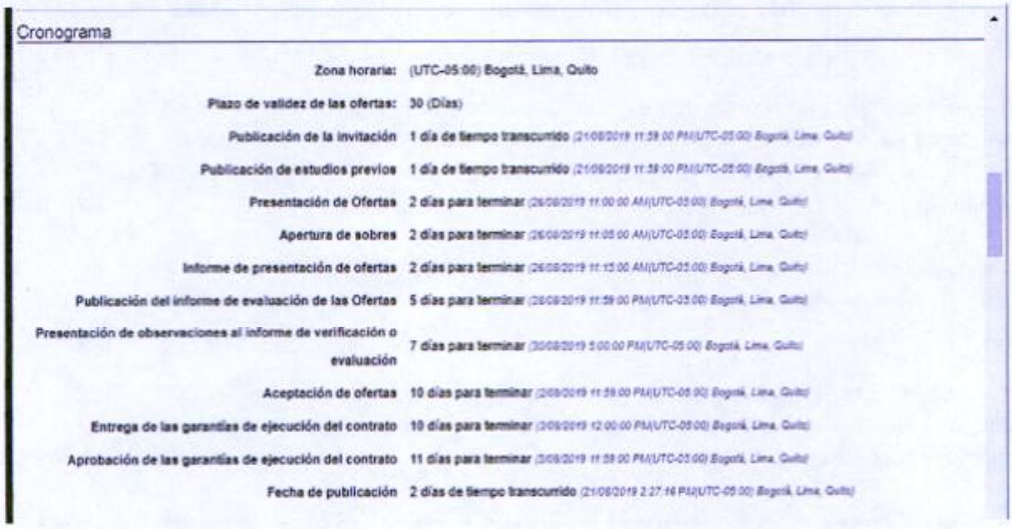
Esta adopción requiere de todo el compromiso de la alta dirección y la asignación de recursos para su transición. La Entidad ha realizado el Plan de Diagnóstico contenido en la fase de planeación, sin embargo, no cuenta con el plan detallado del proceso de transición, el plan de direccionamiento IPv6 y el plan de contingencias de para IPv6, para superar esta fase.

El GIT de Tecnologías de la Información y las Telecomunicaciones en entrevista, adjuntó los estudios previos y el anexo técnico para adelantar el proceso de contratación de mínima cuantía, pendiente de publicación en el SECOP II.

Para la fecha de elaboración de este informe se constató la publicación del proceso en el SECOP II, el cual se registra bajo el No. VJ-VPRE-MC-017-2019 publicado el día 21 de agosto de 2019. Como constancia se adjunta el reporte del SECOP II.



Consecuente con la modalidad de contratación y el cronograma publicado en el SECOP II, la ejecución del contrato debería empezar el 3 de septiembre de 2019.



Cronograma

Zona horaria:	(UTC-05:00) Bogotá, Lima, Quito
Plazo de validez de las ofertas:	30 (Días)
Publicación de la invitación	1 día de tiempo transcurrido (21/08/2019 11:59:00 PM(UTC-05:00) Bogotá, Lima, Quito)
Publicación de estudios previos	1 día de tiempo transcurrido (21/08/2019 11:59:00 PM(UTC-05:00) Bogotá, Lima, Quito)
Presentación de Ofertas	2 días para terminar (26/08/2019 11:00:00 AM(UTC-05:00) Bogotá, Lima, Quito)
Apertura de sobres	2 días para terminar (26/08/2019 11:05:00 AM(UTC-05:00) Bogotá, Lima, Quito)
Informe de presentación de ofertas	2 días para terminar (26/08/2019 11:15:00 AM(UTC-05:00) Bogotá, Lima, Quito)
Publicación del informe de evaluación de las Ofertas	5 días para terminar (28/08/2019 11:59:00 PM(UTC-05:00) Bogotá, Lima, Quito)
Presentación de observaciones al informe de verificación o evaluación	7 días para terminar (30/08/2019 5:00:00 PM(UTC-05:00) Bogotá, Lima, Quito)
Aceptación de ofertas	10 días para terminar (2/09/2019 11:59:00 PM(UTC-05:00) Bogotá, Lima, Quito)
Entrega de las garantías de ejecución del contrato	10 días para terminar (3/09/2019 12:00:00 PM(UTC-05:00) Bogotá, Lima, Quito)
Aprobación de las garantías de ejecución del contrato	11 días para terminar (3/09/2019 11:59:00 PM(UTC-05:00) Bogotá, Lima, Quito)
Fecha de publicación	2 días de tiempo transcurrido (21/08/2019 2:27:16 PM(UTC-05:00) Bogotá, Lima, Quito)

La Oficina de Control Interno hará un seguimiento en el mes de noviembre de 2019, con el fin de medir el avance en la implementación.

Es importante mencionar que la Entidad, de acuerdo con el artículo 5 Contratación de la Resolución No 2710 del 3 de octubre de 2017, ha exigido el soporte IPv6 nativo en coexistencia con IPv4 en los procesos de selección, pliegos de condiciones, contratación de bienes y servicios relacionados con las TIC. Lo anterior pudo ser constatado en los estudios previos y el anexo técnico del proceso de renovación y modernización de la plataforma de seguridad perimetral (FIREWALL) (Adjunto a los papeles de trabajo).

6.5. Revisión mantenimientos infraestructura

En noviembre de 2018 se ejecutó el contrato VPRE 484 del 2018 de mantenimiento para la vigencia de 2018, que incluyó los equipos del Core de la LAN, para este año ya se aprobaron los estudios previos cuyo objeto es: "CONTRATAR EL SERVICIO DE MANTENIMIENTO PREVENTIVO, MANTENIMIENTO CORRECTIVO Y BOLSA DE REPUESTOS PARA LOS BIENES INFORMÁTICOS DE LA AGENCIA NACIONAL DE INFRAESTRUCTURA". (Documento adjunto a los papeles de trabajo).

Otros contratos próximos por suscribirse año 2019 de acuerdo con el Plan de Adquisiciones, relacionados con el mantenimiento correctivo y preventivo:

- Reemplazo de baterías de UPS
- Mantenimientos UPS
- Renovación antivirus
- Compra de dos servidores para aumentar en 60% la capacidad de proceso de la Entidad

7. CIERRE DE LA AUDITORÍA, CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

A partir de los resultados obtenidos en cada uno de los subcapítulos y a la no identificación de no conformidades se puede concluir que el proceso CUMPLE CON RECOMENDACIONES.

Se identificó una FORTALEZA, y es la evidencia de una gestión adecuada por parte de la Gerencia de Sistemas y de su equipo de trabajo, así como su contribución al fortalecimiento institucional; en consecuencia, se considera importante que continúe agregando valor en el apoyo a las áreas misionales de la Entidad.

Para concluir el informe, es apropiado resaltar que, en términos generales la Entidad cumple con la normatividad vigente, y el compromiso de la institución y en especial del área de sistemas han permitido contar con unos centros de cómputo robustos y con una confiabilidad alta en la información que allí se procesa y almacena. No obstante lo anterior, se presentan a continuación algunas recomendaciones para la mejora continua de la gestión.

7.2. Recomendaciones

1. Programar y adelantar jornadas de identificación y peinado del cableado estructurado de los centros de cómputo de los diferentes pisos, con el fin de: evitar un mal funcionamiento de los equipos clientes de la organización, disminuir la amenaza de desconexión de máquinas accidentalmente y facilitar la identificación de fallas en las comunicaciones que eleva el tiempo de solución para daños relacionados con los puntos de red.

2. Mantener aseados y despejados los corredores de transito de los centros de cómputo; no solamente porque el polvo puede afectar los equipos, sino que también, puede ocasionar accidentes u obstaculizar la libre circulación del aire ocasionando recalentamiento en los equipos.

3. Elaborar un formato de reporte de incidentes de seguridad que permita unificar los tratamientos e ir consolidando la base de datos de conocimiento.

4. Implementar puntos de control para los componentes de infraestructura que son de resorte de otras dependencias, como los vencimientos de los equipos de extinción de incendio portátil (extintores de Solkaflam), las coberturas y vencimientos de las pólizas de corriente débil, entre otros, minimizando el impacto que puede tener en el funcionamiento de la infraestructura un vencimiento.

Elaboró y realizó verificación:

Juan Diego Toro Bautista
Auditor Oficina de Control Interno

Apoyó la auditoría en transición IPv6:

Sergio Pulido Caycedo
Apoyo técnico asistencial OCI

Aprobó:

Gloria Margoth Cabrera Rubio
Jefe de Oficina de Control Interno