Bogotá D.C

PARA: **DR. LUIS FERNANDO MEJÍA GÓMEZ**
Presidente (E)

DR. FERNANDO IREGUI MEJÍA
Vicepresidente de Planeación, Riesgos y Entorno

DRA. GINA ASTRID SALAZAR LANDÍNEZ
Vicepresidente Administrativa y Financiera

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 de la Entidad (PEI 124)

Respetados doctores:

En cumplimiento al Plan de Evaluación Independiente aprobado por el Comité de Coordinación del Sistema de Control Interno de la Agencia Nacional de Infraestructura, para la vigencia 2018, la Oficina de Control Interno realizó auditoría a los componentes de hardware, software y seguridad de la información de la Entidad (PEI 124).

Los aspectos evaluados y los resultados de la auditoría se presentan en el informe adjunto, así como las no conformidades y recomendaciones, con el fin de coadyuvar al mejoramiento continuo de la gestión del proceso y contribuir al logro de los objetivos que la ANI espera obtener con el mismo.

Adicionalmente, a partir de las validaciones realizadas se genera la siguiente advertencia, con el fin que la Vicepresidencia de Planeación, Riesgos y Entorno y la Vicepresidencia Administrativa y Financiera tomen medidas inmediatas respecto a lo siguiente:

> Se evidenció incremento en la probabilidad de materialización de los riesgos del proceso: GIC-1 Seguridad de la información comprometida, GIC-5 Pérdida de disponibilidad de los servicios tecnológicos (internet y comunicaciones) y GIC-6 Interrupción de la operación de negocio por problemas, fallas o daño parcial o total de los equipos críticos de la infraestructura tecnológica, lo anterior en virtud del posible acceso de personal no

autorizado al centro de datos del piso 2, ocasionado por la permanencia de la puerta de acceso abierta por problemas de temperatura y la cercanía con las ventanillas de recibo de correspondencia, lo cual propicia un escenario para la materialización de riesgos por daños accidentales o premeditados en los equipos.

De acuerdo con lo previsto en el literal g art. 4º, los literales h, j y k del artículo 12 y el artículo 14 de la Ley 87 de 1993, se envía copia de este informe a las dependencias involucradas, con el fin de que se formule el plan de mejoramiento correspondiente a las no conformidades contenidas en el documento adjunto, en consideración a la necesaria documentación de respuesta a través de la adopción de medidas preventivas o correctivas procedentes para lo cual el término recomendado es de treinta (30) días calendario contados a partir de la radicación.

Cordial saludo,

GLORIA MARGOTH CABRERA RUBIO
Jefe Oficina de Control Interno

C.C. Ing. Jorge Bernardo Gómez Rodríguez – Gerente Equipo de Sistemas de Información y Tecnología
Dra. Nelsy Jenith Maldonado Ballen – Coordinadora Grupo Interno de Trabajo Administrativo y Financiero

Anexo: Informe 20 folios

Proyectó: Juan Diego Toro Bautista – Contratista Oficina de Control Interno
Borrador No. 2018-102-0011334

Agencia Nacional de Infraestructura

INFORME DE AUDITORÍA

Ministerio de Transporte

EVALUACIÓN INTEGRAL DE HARDWARE, SOFTWARE Y SEGURIDAD DE LA INFORMACIÓN
PEI 124

2018

Contenido

1. OBJETIVOS 3
2. ALCANCE 3
3. METODOLOGÍA 4
4. MARCO LEGAL 6
5. VERIFICACIÓN DE ANTECEDENTES 6
6. DESARROLLO DEL INFORME 7
6.1. Verificación muestral del inventario de hardware 7
6.2. Verificación muestral del inventario de software y del cumplimiento de las políticas de instalación de software no autorizado 8
6.3. Infraestructura de los centros de datos 10
6.3.1. Centro de datos piso 2 10
6.3.2. Centro de datos piso 6 14
6.3.3. Centro de datos piso 7 17
6.3.4. Centro de datos piso 8 20
6.4. Revisión del mapa de riesgos 24
6.5. Revisión de políticas y procedimientos 29
6.6. Revisión de activos de información: tangibles 31
6.7. Revisión de activos de información: intangibles 32
6.8. Seguimiento a los compromisos de las auditorías vigencias anteriores y al Plan de Mejoramiento por Procesos PMP (Por sus siglas en español) 34
7. CALIFICACIÓN DE LA AUDITORÍA Y CONCEPTO DEL AUDITOR 35
8. ADVERTENCIAS, NO CONFORMIDADES Y RECOMENDACIONES: 36
8.1. Fortalezas 36
8.2. Funciones de advertencia 36
8.3. No conformidades 37
8.4. Recomendaciones 38

1. OBJETIVOS

- Conocer la situación exacta tanto del hardware en cuanto a: inventario de máquinas, medidas de control y seguridad, planes de mantenimiento, garantías y asignación de responsabilidades, así como del software de la Agencia, en aspectos claves como licenciamiento y perfiles de los usuarios.

- Realizar seguimiento y evaluar la utilización y aprovechamiento de los equipos de cómputo y de sus periféricos, de las instalaciones, mobiliario y equipos de comunicaciones, dedicados al apoyo tecnológico de la entidad, al igual que a la gestión informática de la Agencia Nacional de Infraestructura con respecto a la administración de los Softwares dedicados al apoyo tecnológico de la Entidad.

- Contribuir desde el ejercicio auditor en el aseguramiento de una mayor y mejor utilización de los recursos informáticos, con garantías de integridad, confidencialidad y disponibilidad de la información, mediante la recomendación de alternativas de seguridad y controles.
- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de los funcionarios que utilizan los activos computacionales de la Agencia y de los sistemas de procesamiento de información.

- Revisar los aspectos relevantes del ejercicio de los riesgos asociados al proceso de gestión de la información y comunicaciones, identificando las diversas vulnerabilidades susceptibles de afectar los activos de información que tiene la Entidad.

- Verificar el cumplimiento normativo (ANSI/TIA/EIA/IEEE/NFPA/RETIE/NTC) y de buenas prácticas (COBIT e ISO) en lo que a seguridad informatica compete.

- Conocer los avances en la superación de las no conformidades, detectadas en las auditorías practicadas a los componentes de hardware, software y seguridad de la información, en las vigencias anteriores.

- Determinar oportunidades de mejora y recomendaciones.

2. ALCANCE.

Auditoría realizada en las instalaciones de la Agencia Nacional de Infraestructura, a los componentes de hardware, software, a los centros de datos ubicados en los pisos segundo, sexto, séptimo y octavo, a la seguridad informática interna y perimetral y mediante una muestra aleatoria a los siguientes aspectos en particular:

- Soportes del inventario de los equipos de cómputo dedicados al apoyo tecnológico de la Agencia Nacional de Infraestructura.

- Software sistema operativo y herramientas de ofimática en los equipos asignados en la institución.
- Verificación de instalación de software no autorizado en los equipos asignados por la institución.
- Gestión administrativa y de control del componente de hardware y software.
- Seguridad y protección de los usuarios, de la información, de los archivos y en general de todos y cada uno de los centros de cómputo.
- Gestión administrativa e informática de los centros de cómputo.
- Protección y respaldo de los archivos e información.
- Protección, custodia y niveles de acceso a la información.
- Políticas, planes y procedimientos que soportan el proceso de gestión de la información y comunicaciones.

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 a las normas de auditoría, para lo cual se hizo necesario efectuar una planeación y ejecución de trabajo, donde se tuvieron en cuenta los siguientes aspectos:

- ***Solicitud de información al proceso de gestión de la información y comunicaciones:*** El día 10 de abril de 2018, mediante comunicación con número de radicado 2018-102-005714-3 adjunto a los papeles de trabajo, se solicitó la información correspondiente al inventario de activos de información en materia de hardware, discriminados por pisos incluidos los centros de cómputo; en la misma comunicación se solicitaron documentos, tales como: lista de software estándar, relación de proyectos 2018 y 2019, mapa de riesgos del proceso, listado de amenazas y vulnerabilidades de los activos de información, plan de continuidad del negocio (BIA), soportes de los respaldos y las restauraciones y formato de acuerdos de niveles de servicio.

  Esta información fue allegada a esta auditoría el lunes 16 de abril de 2018, cumpliendo con la fecha estipulada en el comunicado y atendiendo en completitud el requerimiento.

- ***Apertura de la auditoría:*** El día 17 de abril 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.

- ***Ejecución de la auditoría:*** Bajo la modalidad de muestreo, tomando el 10% del universo para ser analizado, se inspeccionaron 60 equipos de cómputo personales, de diferentes dependencias, asimismo, se revisaron los aspectos principales de los centros de datos de los pisos 2,6,7 y 8. Esta actividad fue llevada a cabo los días 17 y 18 de abril de 2018, como estaba estipulado en el acta de apertura. Estas visitas fueron adelantadas en compañía del personal designado por la gerencia de tecnología.

- ***Entrevista:*** El día 19 de abril de 2018, mediante listas de chequeo incorporadas a este informe, se efectuó entrevista en el Grupo de Sistemas de Información y Tecnología sobre los riesgos, las políticas y procedimientos y aspectos relevantes de los bienes tangibles e intangibles.

- ***Socialización de resultados y cierre de la auditoría:*** El día 23 de abril de 2018, se socializaron, al responsable del proceso de Sistemas de Información y Tecnología, 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.

  De acuerdo con los manuales de funciones actuales de la Entidad se evidenciaron funciones relacionadas con el proceso administrativo y financiero, razón por la cual se socializaron los resultados y se brindó la oportunidad de soportar las eventuales no conformidades surgidas en consecuencia del ejercicio de control. Esta actividad se soporta mediante acta de fecha 24 de abril de 2018, 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.

Los parámetros de calificación, definidos para determinar el porcentaje de cumplimiento, son los mismos aplicados en las auditorías anteriores:

CUMPLIMIENTO		
NO CUMPLE	**CUMPLE CON RECOMENDACIONES**	**CUMPLE**
0-60%	61% - 80%	81% - 100%

4. MARCO LEGAL

A continuación, se describe el marco legal e institucional:

- 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".*
- Constitución Política de Colombia Artículos 1, 2, 23,103,209 y 270
- Norma ANSI/TIA 942 Telecommunications Infraestructure Standard
- Reglamento Técnico de Instalaciones Eléctricas, RETIE*
- Código Eléctrico Colombiano, Norma NTC 2050
- Normas ANSI/TIA/EIA 568-B, 569-A, 606-A Commercial Building Telecommunications Cabling Standard, Pathways and Spaces
- Norma ANS/J-STD 607-A, Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications
- Normas NFPA 101 Life Safety Code, NFPA 2001 Standard on Clean Agent Fire Extinguishing Systems, NFPA 72 National Fire Alarm Code, NFPA 75 Standard for the Protection of Electronic Computer Data Processing Equipment, NFPA 76 Standard for the Protection of Telecommunications Facilities.
- Decreto 648 de 2017 Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.
- Directiva Presidencial 002 del 12 de febrero de 2002.
- Artículos 1, 2, 61, 103, 209 y 270 de la Constitución Política de Colombia.

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.

Mientras que, en lo relacionado con el Plan de Mejoramiento por Procesos, se evidenciaron 2 no conformidades numeradas así: 189-2015 y 190-205, las cuales serán tratadas en el capítulo 6 del presente informe.

6. DESARROLLO DEL INFORME

Concordante 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. Verificación muestral del inventario de hardware.
2. Verificación muestral del inventario de software y del cumplimiento de las políticas de instalación de software no autorizado.
3. Infraestructura de los centros de datos.
4. Revisión del mapa de riesgos del proceso de Gestión de la Información y las Comunicaciones.
5. Revisión de políticas y procedimientos.
6. Revisión activos de información: tangibles.
7. Revisión activos de información: intangibles.
8. Revisión de los compromisos de las auditorías anteriores para los componentes de hardware, software y seguridad de la información. Seguimiento al Plan de Mejoramiento de Procesos PMP.

6.1. *Verificación muestral del inventario de hardware*

Del total de 658 equipos con que cuenta la Entidad se seleccionó una muestra del 10% (60 equipos), dividida en los 4 pisos de la Entidad. A estos equipos se les cotejó que los números seriales físicos correspondieran con los consignados en el inventario suministrado por el proceso y además que el funcionario responsable del equipo figurara y coincidiera en el mismo registro.

Las listas de chequeo se encuentran incluidas en los papeles de trabajo de la auditoría y son susceptibles de ser consultadas sin restricción alguna.

El siguiente cuadro resume los resultados obtenidos a partir de la práctica de la lista de chequeo en cada piso:

	ASPECTOS AUDITADOS				TOTAL AUDITADO
	a. El equipo de cómputo referenciado corresponde con el funcionario asignado		b. Los números de serie corresponden a los consignados en el Inventario		
	cumple	no cumple	cumple	no cumple	
2° PISO	15	0	13	2	15
6° PISO	15	0	14	1	15
7° PISO	15	0	15	0	15
8° PISO	15	0	15	0	15
TOTALES	**60**	**0**	**57**	**3**	**60**
PORCENTAJE	100%	0%	95%	5%	

CUMPLIMIENTO	**98%**
	CUMPLE

De acuerdo con los criterios evaluados y con la tabla de calificación descrita en el Capítulo 3 del presente informe, el porcentaje del 98% cumple. Sin embargo, esta auditoría considera como oportunidad de mejora, la implementación de un control adicional a los existentes, a través de la verificación periódica y aleatoria al inventario, máxime cuando se trata de un catálogo cuyo control es compartido con la Vicepresidencia Administrativa y Financiera.

Adicionalmente se recomienda que se incorporen al inventario los cambios de periféricos, (monitores, teclados y/o mouse), de manera inmediata, dado que es allí, donde se evidencian los incumplimientos.

Una última recomendación se brinda en el sentido de reglamentar a las dependencias o sensibilizar al nivel directivo y asesor, dado que bien sea por traslado o retiro de sus servidores se reasignan equipos sin que tenga conocimiento de estas decisiones el área de sistemas o el área administrativa para la modificación inmediata del inventario.

6.2. *Verificación muestral del inventario de software y del cumplimiento de las políticas de instalación de software no autorizado.*

De los 658 equipos con que cuenta la Entidad, se tomó una muestra de 60 equipos (10%), en los cuales se verificó el software instalado, teniendo como línea base el listado del software licenciado y la relación de software que por defecto (estándar) debe contener cada equipo de cómputo de la Entidad.

A estos equipos se les cotejó si tenían: licenciado el sistema operativo, licenciado el aplicativo office, instalado el software antivirus y si reportaba software no autorizado.

Las listas de chequeo se encuentran incluidas en los papeles de trabajo de la auditoría y son susceptibles de ser consultadas sin restricción alguna.

El siguiente cuadro resume los resultados obtenidos a partir de la práctica de la lista de chequeo en cada piso:

	ASPECTOS AUDITADOS								TOTAL AUDITADO
	a. El equipo de cómputo referenciado evidencia el sistema operativo licenciado		b. El equipo de cómputo referenciado evidencia la suite Office licenciada		c. El equipo de cómputo referenciado evidencia el funcionamiento del antivirus		d. El equipo de cómputo referenciado evidencia la instalación de software no autorizado		
	cumple	no cumple	cumple	no cumple	cumple	no cumple	cumple	no cumple	
2° PISO	15	0	15	0	15	0	3	12	15
6° PISO	15	0	15	0	15	0	6	9	15
7° PISO	15	0	15	0	15	0	6	9	15
8° PISO	15	0	15	0	15	0	3	12	15
TOTALES	**60**	**0**	**60**	**0**	**60**	**0**	**18**	**42**	**60**
PORCENTAJE	100%	0%	100%	0%	100%	0%	30%	70%	

CUMPLIMIENTO	**83%**
	CUMPLE

De acuerdo con los criterios evaluados y a la tabla de calificación descrita en el capítulo 3 del presente informe, el porcentaje del 83% cumple. Sin embargo, esta auditoría recomienda, como oportunidad de mejora y teniendo en cuenta que más de la mitad (55%) corresponde a complementos (no necesitan permiso para instalarse), para gestionar archivos PDF, para visualizar archivos de un formato en particular y reproductores de música, entre otros, adelantar una brigada de revisión y eliminación de software no autorizado.

Es importante rescatar que el área de sistemas ha implementado mecanismos que impiden la instalación de software sensible; sin embargo, en internet se encuentra software que no necesita una solicitud de permisos para instalarse, tal como los complementos. Es en este sentido se considera pertinente que el área de sistemas realice una verificación y limpieza e implemente revisiones periódicas y aleatorias, respecto a la instalación de este tipo de aplicativos.

6.3. *Infraestructura de los 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). Dado que los cuatro centros, cumplen guardadas las proporciones en envergadura y capacidad, con la función de suministrar los servicios de cómputo y seguridad de la información a la Agencia, se determinó que los cuatro centros debían cumplir con la normatividad técnica y las buenas prácticas. Lo anterior condujo a que en la auditoría se evaluaran la totalidad de los centros de cómputo bajo los mismos parámetros.

Los parámetros evaluados fueron:

- Especificaciones técnicas de acuerdo con la normatividad:
  - Estructura falsa
  - Ductería
  - Infraestructura eléctrica
  - Sistema de detección de incendios
  - Cableado estructurado (Categoría e identificación)
- Sistema de control de temperatura
- Sistema de respaldo eléctrico (UPS)
- Mobiliario
- Limpieza
- Iluminación
- Control de accesos
- Señalización

6.3.1. Centro de datos piso 2

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
1	Pisos Falsos			2	2	Ajustar baldosas (foto 1)
2	Techos Falsos			2	2	
3	Planilla de control de limpieza de la estructura falsa			2	2	
4	Control de la estática e imantación (Polo a tierra)			2	2	

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS

		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
5	Sistema de Refrigeración		1		1	Cuenta con ventilación, pero no enfriamiento. El equipo de refrigeración se encuentra dañado. (foto 2)
6	Control de temperatura y humedad		1		1	Cuenta con ventilación, pero no enfriamiento. El equipo de refrigeración se encuentra dañado.
7	Planilla de toma de dato permanente para control	0			0	No se está llevando
8	Cableado estructurado		1		1	Desorganizado y sin identificación. (foto 3)
9	Cableado eléctrico			2	2	
10	Ampliaciones eléctricas			2	2	
11	Protección frente a riesgo de corto circuito			2	2	
12	Limpieza del centro de cómputo		1		1	Hay objetos en el piso (foto 4)
13	Planilla de control de limpieza del centro de cómputo		1		1	Desactualizadas
14	Sumideros o sifones para evacuación de aguas			2	2	
15	Iluminación permanente y de respaldo			2	2	
	Puerta de acceso					
16	Mecanismo de apertura	0			0	La puerta permanece abierta (foto 5)
17	Configuración para prevenir el acceso de personal no autorizado			2	2	
18	Cortafuego (Material para impedir la propagación del fuego)			2	2	
19	Ventana de inspección			2	2	

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS

		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
20	Apertura en sentido de salida			2	2	
21	Planilla de control de acceso			2	2	
22	Avisos de señalización y prohibiciones			2	2	
	Sistemas de detección de humo					
23	Equipos extintores			2	2	
24	Red de sensores			2	2	
25	Red de regaderas			2	2	
26	Planillas de control de mantenimiento		1		1	Pendiente mantenimiento desde 2016. Actualmente en proceso de contratación
	Sistemas de respaldo de energía					
27	Acometida regulada, supresores de picos			2	2	
28	Unit Power Supply (UPS)			2	2	
29	Planillas de control de mantenimiento		1		1	Pendiente mantenimiento desde 2016. Actualmente en proceso de contratación
30	Mobiliario (Racks)			2	2	
	CENTRO DE CÓMPUTO PRINCIPAL (SEGUNDO PISO)	0	7	42	49	81.66%
	CUMPLIMIENTO					Cumple

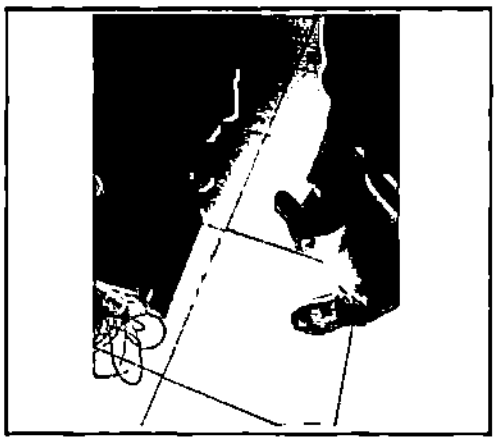


Foto 1

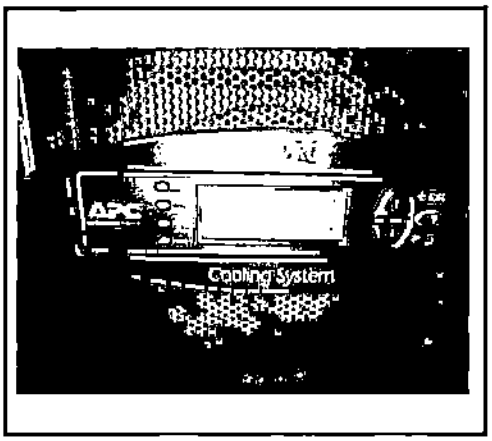


Foto 2

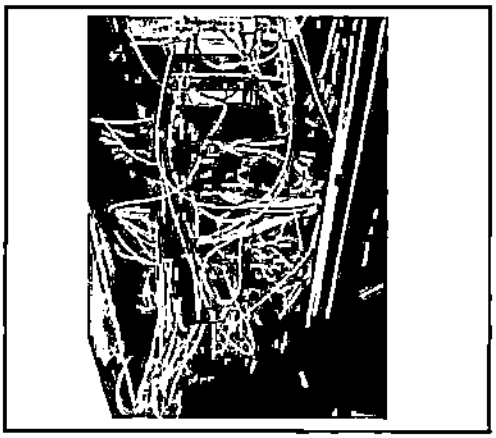


Foto 3

Foto 4

Foto 5

6.3.2. Centro de datos piso 6

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
1	Pisos Falsos			2	2	
2	Techos Falsos			2	2	
3	Planilla de control de limpieza de la estructura falsa			2	2	
4	Control de la estática e imantación (Polo a tierra)			2	2	
5	Sistema de Refrigeración			2	2	Ventilación natural (foto 6)
6	Control de temperatura y humedad					N/A
7	Planilla de toma de dato permanente para control					N/A
8	Cableado estructurado			2	2	(foto 7)
9	Cableado eléctrico			2	2	
10	Ampliaciones eléctricas			2	2	
11	Protección frente a riesgo de corto circuito			2	2	
12	Limpieza del centro de cómputo		1		1	Hay objetos en el piso (fotos 8 y 9)
13	Planilla de control de limpieza del centro de cómputo		1		1	Desactualizadas
14	Sumideros o sifones para evacuación de aguas			2	2	
15	Iluminación permanente y de respaldo			2	2	
	Puerta de acceso					
16	Mecanismo de apertura			2	2	
17	Configuración para prevenir el acceso de personal no autorizado			2	2	

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS

		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
18	Cortafuego (Material para impedir la propagación del fuego)	0			0	La puerta es en vidrio (foto 10)
19	Ventana de inspección			2	2	
20	Apertura en sentido de salida	0			0	Abre en sentido opuesto
21	Planilla de control de acceso			2	2	
22	Avisos de señalización y prohibiciones			2	2	
	Sistemas de detección de humo					
23	Equipos extintores			2	2	
24	Red de sensores			2	2	(foto 11)
25	Red de regaderas	0			0	(foto 12)
26	Planillas de control de mantenimiento		1		1	Pendiente mantenimiento desde 2016. Actualmente en proceso de contratación
	Sistemas de respaldo de energía					
27	Acometida regulada, supresores de picos			2	2	
28	Unit Power Supply (UPS)			2	2	
29	Planillas de control de mantenimiento		1		1	Pendiente mantenimiento desde 2016. Actualmente en proceso de contratación
30	Mobiliario (Racks)			2	2	
	CENTRO DE CÓMPUTO PRINCIPAL (SEXTO PISO)	0	4	42	46	76.66%
	CUMPLIMIENTO					Cumple con recomendaciones

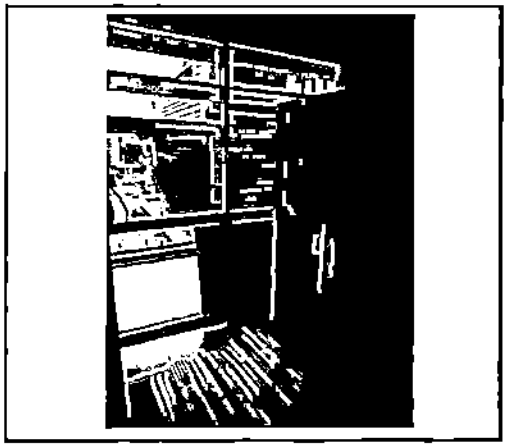


Foto 6

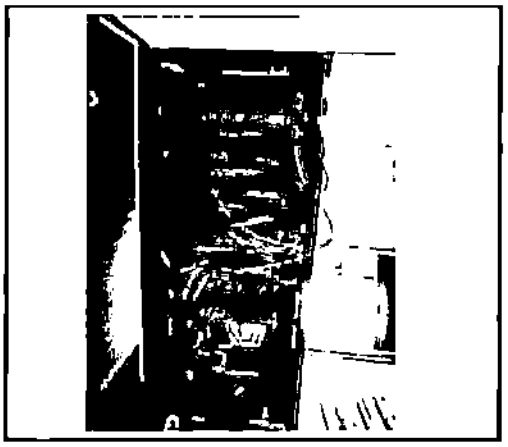
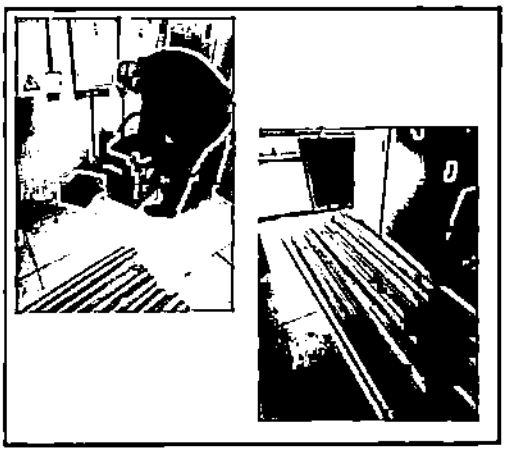


Foto 7



Fotos 8 y 9

Foto 10

Foto 11

Foto 12

6.3.3. Centro de datos piso 7

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
1	Pisos Falsos			2	2	
2	Techos Falsos			2	2	Se evidencia un panel suelto. (fotos 13 y 14)
3	Planilla de control de limpieza de la estructura falsa			2	2	
4	Control de la estática e imantación (Polo a tierra)			2	2	
5	Sistema de Refrigeración	0			0	No se evidencia ningún mecanismo de enfriamiento
6	Control de temperatura y humedad	0			0	No se evidencia
7	Planilla de toma de dato permanente para control	0			0	No se evidencia
8	Cableado estructurado			2	2	
9	Cableado eléctrico			2	2	
10	Ampliaciones eléctricas			2	2	
11	Protección frente a riesgo de corto circuito			2	2	
12	Limpieza del centro de cómputo		1		1	Hay objetos en el piso (foto 15)
13	Planilla de control de limpieza del centro de cómputo		1		1	Desactualizadas
14	Sumideros o sifones para evacuación de aguas			2	2	
15	Iluminación permanente y de respaldo			2	2	
	Puerta de acceso					
16	Mecanismo de apertura			2	2	
17	Configuración para prevenir el acceso de personal no autorizado			2	2	

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
18	Cortafuego (Material para impedir la propagación del fuego)	0			0	La puerta es en vidrio (foto 16)
19	Ventana de inspección			2	2	
20	Apertura en sentido de salida	0			0	Abre en sentido opuesto
21	Planilla de control de acceso			2	2	
22	Avisos de señalización y prohibiciones			2	2	
	Sistemas de detección de humo					
23	Equipos extintores			2	2	
24	Red de sensores			2	2	
25	Red de regaderas	0			0	(foto 17)
26	Planillas de control de mantenimiento		1		1	Pendiente mantenimiento desde 2016. Actualmente en proceso de contratación
	Sistemas de respaldo de energía					
27	Acometida regulada, supresores de picos			2	2	
28	Unit Power Supply (UPS)			2	2	
29	Planillas de control de mantenimiento		1		1	Pendiente mantenimiento desde 2016. Actualmente en proceso de contratación
30	Mobiliario (Racks)			2	2	
	CENTRO DE CÓMPUTO PRINCIPAL (SÉPTIMO PISO)	0	4	40	44	73.33%
	CUMPLIMIENTO					Cumple con recomendaciones

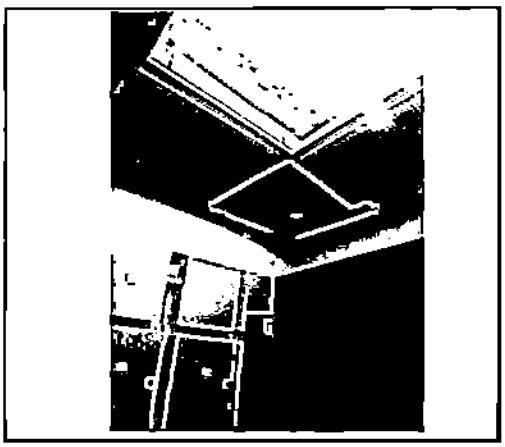


Foto 13

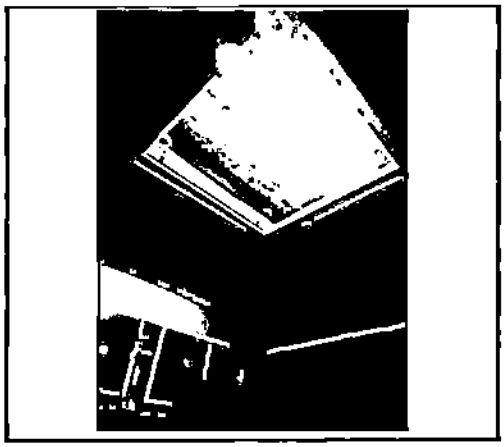


Foto 14

Foto 15

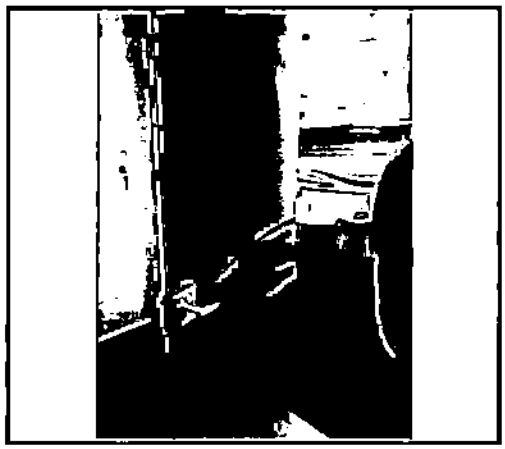


Foto 16

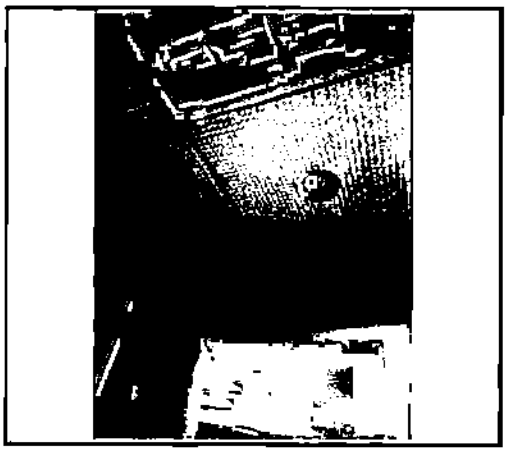


Foto 17

6.3.4. Centro de datos piso 8

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
1	Pisos Falsos			2	2	
2	Techos Falsos			2	2	
3	Planilla de control de limpieza de la estructura falsa			2	2	
4	Control de la estática e imantación (Polo a tierra)			2	2	
5	Sistema de Refrigeración			2	2	
6	Control de temperatura y humedad			2	2	
7	Planilla de toma de dato permanente para control	0			0	No se evidencia
8	Cableado estructurado			2	2	(Foto 18)
9	Cableado eléctrico			2	2	
10	Ampliaciones eléctricas			2	2	
11	Protección frente a riesgo de corto circuito			2	2	
12	Limpieza del centro de cómputo		1		1	Hay objetos (cajas con equipos obsoletos) en el piso que obstaculizan la ventilación. (fotos 19 y 20)
13	Planilla de control de limpieza del centro de cómputo		1		1	Desactualizadas
14	Sumideros o sifones para evacuación de aguas			2	2	
15	Iluminación permanente y de respaldo			2	2	
	Puerta de acceso					
16	Mecanismo de apertura			2	2	
17	Configuración para prevenir el acceso de personal no autorizado			2	2	

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS

		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
18	Cortafuego (Material para impedir la propagación del fuego)			2	2	
19	Ventana de inspección			2	2	
20	Apertura en sentido de salida			2	2	
21	Planilla de control de acceso			2	2	
22	Avisos de señalización y prohibiciones			2	2	
	Sistemas de detección de humo					
23	Equipos extintores			2	2	
24	Red de sensores			2	2	
25	Red de regaderas			2	2	
26	Planillas de control de mantenimiento		1		1	Pendiente mantenimiento desde 2016. Actualmente en proceso de contratación
	Sistemas de respaldo de energía					
27	Acometida regulada, supresores de picos			2	2	
28	Unit Power Supply (UPS)			2	2	
29	Planillas de control de mantenimiento		1		1	Pendiente mantenimiento desde 2016. Actualmente en proceso de contratación
30	Mobiliario (Racks)			2	2	
	CENTRO DE CÓMPUTO PRINCIPAL (OCTAVO PISO)	0	4	50	54	90.00%
	CUMPLIMIENTO					Cumple

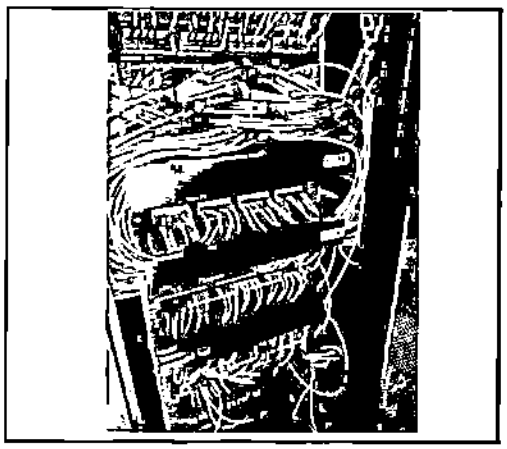


Foto 18

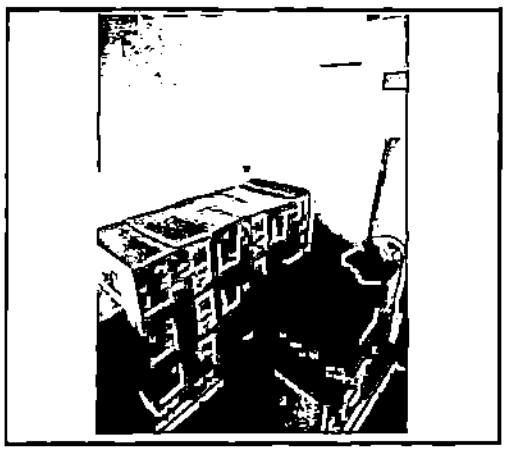


Foto 19

Foto 20

CUMPLIMIENTO CONSOLIDADO						
		ESCALA DE CUMPLIMIENTO				
ÍTEM	DESCRIPTOR	NO CUMPLE	CUMPLE CON RECOMENDACIONES	CUMPLE	PUNTAJE	OBSERVACIONES
		0% - 60%	61% - 80%	81% - 100%		
I	Infraestructura centro de datos principal (PISO 2)			2	2	81,66%
I	Infraestructura centro de datos (PISO 6)		1		1	76,66%
I	Infraestructura centro de datos (PISO 7)		1		1	73,33%
I	Infraestructura centro de datos (PISO 8)			2	2	90,00%
TOTALES					6	CUMPLE CON RECOMENDACIONES
CUMPLIMIENTO CONSOLIDADO					75,00%	

Situaciones evidenciadas

De la revisión efectuada, podemos identificar la existencia de algunas falencias que deben ser subsanadas, con el objeto de mejorar la gestión en cuanto a la construcción de un esquema de seguridad informática, más robusto y confiable, donde los diferentes componentes que la constituyan eviten que se presenten las siguientes situaciones o que se eleven los niveles de riesgo:

- **Función de Advertencia**, por incremento en la probabilidad de materialización de los riesgos del proceso: GIC-1 Seguridad de la información comprometida, GIC-5 Pérdida de disponibilidad de los servicios tecnológicos (internet y comunicaciones) y GIC-6 Interrupción de la operación de negocio por problemas, fallas o daño parcial o total de los equipos críticos de la infraestructura tecnológica, lo anterior en virtud del posible acceso de personal no autorizado al centro de datos del piso 2, ocasionado por la permanencia de la puerta de acceso abierta por problemas de temperatura y la cercanía con las ventanillas de recibo de correspondencia, lo cual propicia un escenario para la materialización de riesgos relacionados con daños accidentales o premeditados en los equipos.

- Se evidencian piezas de la infraestructura de pisos y techos falsos faltantes o desajustadas. Lo anterior puede ocasionar accidentes a los servidores que laboran en estas áreas.

- Objetos en el piso de los centros de datos, que obstaculizan el tránsito de los pasillos internos, elevan la temperatura interna de los cuartos y dados los materiales inflamables (plástico y cartón) de estos objetos, incrementa los riesgos de incendio.

- Mecanismos de registro de las actividades; se pudo observar en la evaluación la ausencia de planillas u otro mecanismo de control, para actividades de lectura y registro de temperatura, limpieza de los centros de datos, custodia y manejo de las llaves de los racks, que requieren, por su nivel de riesgo, un seguimiento permanente que incluya los datos tomados de la actividad y la firma del responsable de ejecutarlo y de supervisarlo.

- Las puertas de acceso a los centros de datos de los pisos 6 y 7 en vidrio, no cumplen con las características técnicas de material (cortafuego) y de sentido de apertura. El incumplimiento de estas especificaciones incrementa el riesgo de propagación de incendio y la exposición del cuarto de datos a agentes exógenos.

- Desorden en el cableado estructurado, como se pudo evidenciar en el centro de datos del piso 2 presenta un desorden en la disposición e identificación de los cables de red, lo cual puede originar perdida de referencia del punto físico por dificultad en la identificación o desconexión accidental u premeditada de un usuario activo.

- Sistemas de detección y control de incendios, en los centros de datos de los pisos 6 y 7 no se evidencian los splinters (regaderas) para extinción de incendios. La ausencia de estas medidas de control y mitigación incrementa el impacto de riesgo en caso de incendio.

- Sistemas de refrigeración y control de temperatura, en el centro de datos de séptimo piso no se cuenta con una fuente de aire, ni natural ni artificial, razón por la cual, la sensación térmica es alta y aumenta el riesgo de mal funcionamiento de los equipos por sobrecalentamiento.

6.4. *Revisión del mapa de riesgos*

El mapa de riesgos publicado en la página web de la entidad, bajo el enlace https://www.ani.gov.co/sites/default/files/u233/mapa_de_riesgos_ani_2017_final.pdf, en lo que al proceso de apoyo "Gestión de la información y las comunicaciones" respecta, identifica 6 riesgos a saber:

SIGLA	RIESGO	VALORACIÓN
GIC-1	Seguridad de la información comprometida.	ALTO
GIC-2	Interrupción de negocio por desastre natural.	ALTO
GIC-3	Fallas o pérdida de la integridad de la información (completitud y exactitud).	MODERADO
GIC-4	Perdida de confidencialidad de la información de la agencia.	MODERADO
GIC-5	Perdida de disponibilidad de los servicios tecnológicos (internet y comunicaciones).	MODERADO
GIC-6	Interrupción de la operación de negocio por problemas, fallas o daño parcial o total de los equipos críticos de la infraestructura tecnológica.	ALTO

Como se puede observar en la tabla anterior se distribuye: 50% en riesgos con valoración alta y 50% con valoración moderada, mostrando la criticidad del proceso y obedeciendo a la lógica por ser un proceso de apoyo. En desarrollo de la auditoría se evaluaron los controles existentes, las acciones requeridas para reducir el riesgo y los indicadores propuestos.

En este capítulo es importante mencionar que, la identificación de los riesgos para el proceso de sistemas es un ejercicio que supera los métodos tradicionales de identificación y valoración del riesgo, dado que para el éxito de este ejercicio, es de vital importancia la identificación del inventario de activos de información, y no solo hacemos referencia a los bienes tangibles como hardware y software, sino también la información y documentación y otros tantos activos intangibles de la Entidad; también, se identifican las vulnerabilidades[1] y las amenazas[2] de cada uno de esos activos.

Consecuente con el cronograma de implementación de las acciones que muestra la fecha final 30 de septiembre de 2017, se verificó el nivel de avance con los documentos soportes, encontrándose los siguientes resultados:

SIGLA	ACCIONES DE MITIGACIÓN DEL RIESGO	AVANCE
GIC-1	Mantener la implementación de buenas prácticas de control de seguridad de la información en beneficio de la mitigación de riesgos asociados y bajo esquema y lineamientos de la norma ISO/IEC 27001 y Gobierno en Linea (GEL)	80%

[1] Característica de un activo de información y que representa un riesgo para la seguridad de la información, un ejemplo de esto son las contraseñas débiles.
[2] Evento que puede afectar los activos de información y están relacionadas con el recurso humano, eventos naturales o fallas técnicas.

SIGLA	ACCIONES DE MITIGACIÓN DEL RIESGO	AVANCE
GIC-2	Desarrollar y documentar planes de continuidad de negocio y recuperación ante presencia de desastres	100%
	Establecer la estrategia de redundancia de instalaciones o equipos para asegurar la continuidad del negocio	100%
	Adquirir equipos tecnológicos que apoyen la infraestructura como contingencia ante situaciones de interrupción	100%
GIC-3	Mantener un control estricto para la gestión de asignación de accesos y privilegios a los usuarios creados	100%
	Mantener un control de revisión de los accesos concedidos a los usuarios por parte de los propietarios de la información	100%
	Sensibilización a los funcionarios de la entidad para que el almacenamiento de la información se realice en la(s) unidad(es)asignada(s) por el equipo de sistemas	100%
GIC-4	Mantener un control estricto para la gestión de asignación de accesos y privilegios a los usuarios creados	100%
	Toma de respaldos de información para restauración en caso necesario	100%
	Asegurar un único repositorio de información para garantizar la integridad de la información	100%
GIC-5	Mantener vigente las actividades y/o contrato para realizar los mantenimientos tanto preventivo como correctivo a los equipos de cómputo críticos	50%
	Asegurar la disponibilidad de los servicios tecnológicos mediante estrategias de contingencia	80%
	Realizar actividades de evaluación para mejoramiento de la plataforma tecnológica para aprovechamiento de la misma	80%

SIGLA	ACCIONES DE MITIGACIÓN DEL RIESGO	AVANCE
GIC-6	Mantener vigente de las actividades y/o contrato para realizar los mantenimientos tanto preventivo como correctivo a los equipos de cómputo críticos.	50%
	Asegurar la adquisición y mantenimiento de equipos críticos para respaldo ante cualquier necesidad de uso en situaciones de contingencia	80%
	Mantener respaldos de información en caso de falla, problema o daño de equipo tecnológico critico	100%
Avance general		**88,75%**
Cumplimiento		**Cumple**

Fue menester de este ejercicio auditor, realizar una identificación de los riesgos basados en la metodología MAGERIT versión 2, que permitiera a posteriori, efectuar recomendaciones u oportunidades de mejora al mapa de riesgos elaborado por el equipo de sistemas de información y tecnología.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

Con base en la información remitida por la gerencia de sistemas, de la identificación de amenazas y vulnerabilidades se obtuvieron los siguientes riesgos para cada tipo de seguridad (Confidencialidad, Disponibilidad e Integridad):

SEGURIDAD	RIESGOS	CORRELACIÓN CON EL MAPA DE RIESGOS
Integridad	Descarga y propagación de virus en la red	GIC-1
	Uso delictivo de datos	GIC-1
	Acceso no autorizado a servidores	GIC-1
	Acceso y manipulación a redes privadas	GIC-4
	Acceso y manipulación a información privada	GIC-4
	Alteración y destrucción de la información	GIC-1
	Alteración y destrucción de datos	GIC-1
	Alteración y destrucción de respaldos	GIC-1
	Exposición de datos de autenticación a usuarios no autorizados	GIC-1
	Robo de equipos	GIC-6
	Perdida de información por error de hardware	GIC-6
	Perdida de información por error de usuario	GIC-3
	Infiltración en información transmitida no cifrada	GIC-3
Disponibilidad	Perdida del equipo	GIC-1
	Acceso no autorizado a servidores	GIC-1
	Robo de información	GIC-1
	Alteración y destrucción de la información	GIC-1
	Alteración y destrucción de datos	GIC-1
	Alteración y destrucción de respaldos	GIC-1
	Robo de equipos	GIC-6
	Robo información	GIC-4
	Infiltración de virus	GIC-6
	Perdida de información por error de usuario	GIC-1
	Perdida de información por error de hardware	GIC-6
Confidencialidad	Intromisiones de otros usuarios al equipo	GIC-4
	Acceso por entidades externas a información sensible o privada	GIC-4
	Uso delictivo de datos	GIC-1
	Acceso no autorizado a servidores	GIC-1
	Acceso y manipulación a redes privadas	GIC-4
	Acceso y manipulación a información privada	GIC-4
	Robo de información	GIC-1
	Acceso por usuarios no autorizados	GIC-4

SEGURIDAD	RIESGOS	CORRELACIÓN CON EL MAPA DE RIESGOS
	Acceso a datos sensibles o privados	GIC-4
	Acceso a respaldos por usuarios no autorizados	GIC-4
	Divulgación de información de la organización	GIC-4
	Robo de equipos	GIC-6
	Robo de información	GIC-4
	Infiltración de virus	GIC-6
	Perdida de información por error de usuario	GIC-1

De acuerdo con la tabla anterior, la correlación es perfecta, es decir, de acuerdo a la metodología empleada por esta auditoría versus la identificación de riesgos elaborada por el equipo de sistemas de tecnología e información, no se evidencian riesgos adicionales.

En conclusión, el mapa de riesgos actual del proceso de Gestión de la Información y las Comunicaciones, contempla la totalidad de riesgos que debería contener; su cobertura, controles, y acciones de mitigación están alineadas con el desarrollo e implementación del SGSI, con la normatividad vigente y con los parámetros exigidos por la norma ISO/IEC 27001, en caso de una eventual certificación.

Igualmente se puede concluir que el porcentaje de avance del 88,75% en la implementación de las acciones de mitigación supera con holgura las expectativas a la fecha y muestra una buena gestión en el seguimiento del mapa de riesgos de la Entidad, en lo que al proceso de Gestión de la información y las comunicaciones se refiere.

6.5. *Revisión de políticas y procedimientos*

En el marco de la auditoría se revisaron los documentos que imparten los lineamientos para la Gerencia de Sistemas de Información y Tecnología y los 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.

La siguiente lista de chequeo muestra el estado de cumplimiento de estos documentos:

		cumplimiento				
ITEM	DESCRIPTOR	no cumple	parcial	total	puntaje	Observaciones
		0	1	2		
1	La Entidad cuenta con una Política Estratégica de Seguridad de la Información		1		1	El borrador del documento se encuentra en revisión por la alta gerencia
2	Se encuentra actualizada		1		1	
3	Socializada y Publicada		1		1	
4	La Entidad cuenta con un Manual de Políticas de la Información		1		1	El borrador del documento se encuentra en revisión por la alta gerencia
5	Se encuentra actualizado		1		1	
6	Socializado y Publicado		1		1	
7	La Entidad cuenta con un Manual de Buenas Prácticas de seguridad de la Información		1		1	El borrador del documento se encuentra en revisión por la alta gerencia
8	Se encuentra actualizado		1		1	
9	Socializado y Publicado		1		1	
10	La Entidad cuenta con una Política de Respaldo y restauración			2	2	
11	Se encuentra actualizada			2	2	
12	Socializada y Publicada			2	2	
13	La Entidad cuenta con un Documento de Acuerdos de Niveles de Servicio			2	2	
14	Se encuentra actualizado			2	2	
15	Socializado y Publicado			2	2	

	0	9	12	21	
CUMPLIMIENTO				70,00%	Cumple con recomendaciones

Se evidenció la gestión del área de sistemas en la elaboración de estas políticas, sin embargo, se recomienda implementar mecanismos más expeditos para involucrar a la alta gerencia en la aprobación de estas políticas que contribuyen a robustecer la gestión de la Entidad.

El Departamento Administrativo de la Función Pública – DAFP, acaba de expedir el Decreto 612 del 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, por medio del cual decreta en su ***Artículo 1***, que las entidades del Estado deberán integrar entre otros planes los siguientes: Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Seguridad de la Información, para lo cual según el ***Artículo 2 de Transición*** el plazo vence a más tardar el 31 de julio de 2018. Este tema fue objeto de revisión por parte del Comité Institucional de Gestión y Desempeño de la Entidad y las actividades para su cumplimiento serán coordinadas por el Grupo Interno de Trabajo de Planeación.

Es importante avanzar en la formalización de estas políticas a través de la intervención de la alta gerencia en su aprobación, dado que son los insumos primordiales para alinear los planes de acción de la Entidad con la planeación estratégica y marcarán el derrotero de la gestión venidera.

6.6. *Revisión de activos de información: tangibles*

Con base en el listado de activos de información remitidos a esta auditoría, se efectuó una revisión de los considerados físicos, incluyendo los activos que garanticen la mitigación de las amenazas, encontrando el siguiente comportamiento:

		cumplimiento			puntaje	
ÍTEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		0	1	2		
1	**Inventario físico de equipos del centro de cómputo (Equipos de cómputo, servidores, equipos de comunicación, equipos de respaldo, monitoreo y grabación), especificando, propiedad, estado y capacidad.**			2	2	

		cumplimiento			puntaje	
ÍTEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		0	1	2		
2	Se cuenta con un plan de mantenimiento		1		1	El último mantenimiento se practicó en 2016. Se encuentran en proceso de contratación los mantenimientos.
3	Se lleva control sobre los periodos de garantía			2	2	
4	Se cuenta con servidores espejo para contingencia			2	2	
5	La entidad cuenta con un plan de continuidad del negocio y recuperación BIA			2	2	
6	Se encuentra actualizado			2	2	
7	Socializado y Publicado			2	2	

	0	1	12	13	
CUMPLIMIENTO				92,86%	Cumple

Si bien es cierto, la Entidad cumple con un porcentaje superior y no ha sufrido la materialización de ninguno de los riesgos identificados, también lo es, que reviste principal importancia contar con planes de mantenimiento vigentes, con enfoques mayormente en lo preventivo y secundariamente en lo correctivo, con el fin de garantizar la no presencia de eventuales daños graves en la infraestructura tecnológica de la Entidad.

6.7. *Revisión de activos de información: intangibles*

Con base en el listado de activos de información remitidos a esta auditoría, se efectuó una revisión de los considerados lógicos, incluyendo los activos que garanticen la mitigación de las vulnerabilidades, encontrando el siguiente comportamiento:

		cumplimiento			puntaje	
ÍTEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		0	1	2		
1	Inventario físico del software instalado en los equipos del centro de cómputo (Licenciamiento, Motores de bases de datos, sistemas de información, aplicativos en general), especificando, propiedad y estado.			2	2	
2	Se cuenta con un plan de mantenimiento		1		1	El último mantenimiento se practicó en 2016. Se encuentran en proceso de contratación los mantenimientos.
3	Se lleva control sobre los periodos de garantía			2	2	
4	Grabación y custodia de las grabaciones del PVR			2	2	
5	Existen instructivos de configuración de los servidores			2	2	
5	La entidad cuenta con un plan de continuidad del negocio y recuperación BIA			2	2	
6	Se encuentra actualizado			2	2	
7	Socializado y Publicado			2	2	
6	La entidad cuenta con el listado de activos de información			2	2	
7	Se encuentra actualizado			2	2	
8	Socializado y Publicado			2	2	

	0	1	20	21
CUMPLIMIENTO				95,45% Cumple

Si bien es cierto, la Entidad cumple con un porcentaje superior y no ha sufrido la materialización de ninguno de los riesgos identificados, también lo es, que reviste principal importancia contar con planes de mantenimiento vigentes, con enfoques mayormente en lo preventivo y secundariamente en lo correctivo, con el fin de garantizar la no presencia de eventuales daños graves en la infraestructura tecnológica de la entidad.

6.8. *Seguimiento a los compromisos de las auditorías vigencias anteriores y al Plan de Mejoramiento por Procesos PMP (Por sus siglas en español)*

En la revisión de antecedentes se detectaron 2 no conformidades, el comportamiento de estas no conformidades se manifiestan a continuación:

CÓDIGO	AÑO	DESCRIPCIÓN E IDENTIFICACIÓN NO CONFORMIDAD REAL O POTENCIAL.	CONCESIÓN / ÁREA (RESPONSABLE DE LA IMPLEMENTACIÓN)	AUDITOR.	FECHA AUDITORÍA (dd/mm/aa)	CUMPLE / %	ACCIÓN
189	2015	Dotar de mecanismos de extinción de incendios en los centros de cómputo de los pisos 6 y 7.	Vicepresidencia de Planeación Riesgos y Entorno (Gerencia de Sistemas) – Vicepresidencia Administrativa y Financiera (Coordinación Administrativa y Financiera)	JDT	Sept 2015	NO / 50%	Esta no conformidad se reitera en esta auditoría, modificando su descripción y responsables Se encuentra en proceso de contratación

CÓDIGO	AÑO	DESCRIPCIÓN E IDENTIFICACIÓN NO CONFORMIDAD REAL O POTENCIAL.	CONCESIÓN / ÁREA (RESPONSABLE DE LA IMPLEMENTACIÓN)	AUDITOR.	FECHA AUDITORÍA (dd/mm/aa)	CUMPLE / %	ACCIÓN
190	2015	Dotar de un mecanismo de disipación de calor en el centro de cómputo del piso 7.	Vicepresidencia de Planeación Riesgos y Entorno (Gerencia de Sistemas) – Vicepresidencia Administrativa y Financiera (Coordinación Administrativa y Financiera)	JDT	Sept 2015	NO / 50%	Esta no conformidad se reitera en esta auditoría, modificando su descripción y responsables Se encuentra en proceso de contratación

Se concluye que, actualmente se está adelantando el proceso de contratación para la solución integral de las debilidades de infraestructura.

7. CALIFICACIÓN DE LA AUDITORÍA Y CONCEPTO DEL AUDITOR

RESULTADO FINAL

ITEM	DESCRIPTOR	NO CUMPLE 0-60%	CUMPLE CON RESTR 61%-80%	CUMPLE 81%-100%	puntaje	Observaciones
6.1	Verificación muestral del inventario de hardware.			2	2	98,00%
6.2	Verificación muestral del inventario de software y del cumplimiento de las políticas de instalación de software no			2	2	83,00%
6.3	Infraestructura de los centros de datos.		1		1	75,00%
6.4	Revisión del mapa de riesgos del proceso de Gestión de la información y las Comunicaciones.			2	2	88,75%
6.5	Revisión de políticas y procedimientos.		1		1	70,00%
6.6	Revisión activos de información: tangibles.			2	2	92,86%
6.7	Revisión activos de información: intangibles.			2	2	95,45%
		0	2	10	12	
	CUMPLIMIENTO				85,71%	Cumple

Consecuente con la calificación final, el proceso **CUMPLE.** Sin embargo, es necesario atender y solucionar las situaciones descritas en el siguiente capítulo.

8. ADVERTENCIAS, NO CONFORMIDADES Y RECOMENDACIONES:

8.1. *Fortalezas*

A partir de la revisión integral de los componentes auditados se identificaron las siguientes fortalezas en el proceso:

1. Respecto a la capacidad de recuperación, ante la ocurrencia de incidentes catastróficos, la Entidad cuenta con una avanzada infraestructura tecnológica que incluye respaldos aplicables y personal altamente calificado que permite asegurar esa recuperación.

2. El proceso de Gestión de Tecnología ha adelantado los procesos para la contratación de los mantenimientos de los equipos de cómputo e impresoras, equipos del core de la LAN que incluye el cableado estructurado, a las Unit Power Supply (UPS) y aire acondicionado, infraestructura para control y extinción de incendios, firewall y sistemas de respaldo. Estos procesos se estarán ejecutando en el transcurso de los próximos cuatro meses.

   Es importante mencionar que para el año 2017, el área de tecnología adelantó los procesos de contratación ya que disponía de los recursos, sin embargo, estos procesos fueron suspendidos por concepto del Grupo Interno de Trabajo Contratación adscrito a la Vicepresidencia Jurídica.

3. El proceso de Gestión de Tecnología ha sometido a consideración del nivel directivo, las políticas de seguridad de la información, como parte del Plan Estratégico de Tecnologías de la Información PETI y del panorama que se avecina para las Entidades del Estado en materia normativa.

4. Se evidenció 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.

8.2. *Funciones de advertencia*

Se evidenció incremento en la probabilidad de materialización de los riesgos del proceso: GIC-1 Seguridad de la información comprometida, GIC-5 Pérdida de disponibilidad de los servicios tecnológicos (internet y comunicaciones) y GIC-6 Interrupción de la operación de negocio por problemas, fallas o daño parcial o total de los equipos críticos de la

infraestructura tecnológica, lo anterior en virtud del posible acceso de personal no autorizado al centro de datos del piso 2, ocasionado por la permanencia de la puerta de acceso abierta por problemas de temperatura y la cercanía con las ventanillas de recibo de correspondencia, lo cual propicia un escenario para la materialización de riesgos por daños accidentales o premeditados en los equipos.

8.3. *No conformidades*

El presente ejercicio presenta cinco (5) no conformidades, que obedecen a irregularidades en la infraestructura tecnológica de la Entidad, cuya responsabilidad está definida en los manuales de funciones de manera compartida, para el Grupo Interno de Trabajo Administrativo y Financiero de la Vicepresidencia Administrativa y Financiera y el Equipo de Sistemas de Información y Tecnología de la Vicepresidencia de Planeación, Riesgos y Entorno. En consecuencia, los planes de mejoramiento deben ser formulados y ejecutados de manera compartida conforme las unidades de medida propuestas.

1. Las puertas de acceso a los centros de datos de los pisos 6 y 7 no cumplen con las especificaciones técnicas descritas en las normas NFPA 101 Life Safety Code, NFPA 2001 Standard on Clean Agent Fire Extinguishing Systems, NFPA 72 National Fire Alarm Code, NFPA 75 Standard for the Protection of Electronic Computer Data Processing Equipment, NFPA 76 Standard for the Protection of Telecommunications Facilities. El incumplimiento de estas especificaciones incrementa el riesgo de propagación de incendio y la exposición del cuarto de datos a agentes exógenos.

2. Los centros de datos de los pisos 6 y 7 no cuentan con un sistema de extinción de incendio por tubería y splinters (regaderas), entretanto, en los pisos 2 y 8, se cuenta con este sistema, pero extingue el incendio con agua y no con agente limpio o Solkaflam. Lo anterior no cumple con las especificaciones técnicas descritas en las normas NFPA 101 Life Safety Code, NFPA 2001 Standard on Clean Agent Fire Extinguishing Systems, NFPA 72 National Fire Alarm Code, NFPA 75 Standard for the Protection of Electronic Computer Data Processing Equipment, NFPA 76 Standard for the Protection of Telecommunications Facilities. El incumplimiento de estas especificaciones incrementa el riesgo de incendio y de pérdidas de bienes tangibles e intangibles.

3. El centro de datos del piso 2 presenta un daño en el sistema de refrigeración, permitiendo la elevación de la temperatura y el incremento en el riesgo de daño de los equipos core de la LAN. Lo anterior se originó por la carencia de mantenimiento preventivo en los equipos de refrigeración y de respaldo de energía. El mal funcionamiento de este equipo ha obligado a la Administración de la Entidad a dejar la puerta abierta, perdiendo el control de acceso por parte de terceros a un área restringida por la sensibilidad de lo que contiene.

4. Actualmente la Entidad no cuenta con mantenimientos contratados ni planes de mantenimiento vigentes para la infraestructura tecnológica para los equipos de cómputo

(excluyendo los equipos nuevos que fueron adquiridos con dos mantenimientos al año por tres años), equipos del core de la LAN, equipos de respaldo de refrigeración y energía, entre otros, aumentando el riesgo de daño.

5. La Entidad carece de un sistema de refrigeración en el centro de datos del piso 7 y adicionalmente, este cuarto no cuenta con fuentes de ventilación natural. Lo anterior se refleja en una alta sensación térmica que aumenta el riesgo de daño o mal funcionamiento en los equipos de red.

8.4. *Recomendaciones*

1. Realizar con alguna periodicidad, controles aleatorios al inventario, máxime cuando se trata de un catálogo cuyo control es compartido con la Vicepresidencia Administrativa y Financiera.

2. Incorporar al inventario los cambios de periféricos, (monitores, teclados y/o mouse), de manera inmediata, dado que es allí, donde se evidencian los incumplimientos.

3. Reglamentar a las dependencias o sensibilizar al nivel directivo y asesor, dado que bien sea por traslado o retiro de sus funcionarios se reasignan equipos a otros funcionarios sin informar de estas decisiones al área de sistemas o al área administrativa para la modificación inmediata del inventario.

4. Adelantar una brigada de revisión y eliminación de software no autorizado e implementar mecanismos que impidan la instalación de complementos, tales como, gestores de archivos en formato PDF, visores y reproductores de música P2P y streaming, entre otros.

5. Adelantar una brigada de limpieza en los centros de datos, retirando los objetos que obstaculizan y que generan riesgo de incendio. Asimismo, ajustando las piezas del piso falso del centro de datos del piso 2 y de techo falso del centro de datos del piso 7. Se recomienda realizar de manera perentoria esta jornada y en el futuro institucionalizar estas limpiezas con una corta periodicidad.

6. Crear y diligenciar oportunamente las planillas de control para las actividades mencionadas, verbigracia, control de temperatura y limpieza de los centros de datos.

7. Contratar la intervención de personal calificado para la organización (peinado) e identificación del cableado de red.

8. Robustecer la participación en la definición de los planes de contingencia, formulando mecanismos alternos y más expeditos para la solución de las eventuales irregularidades que se puedan presentar en los centros de datos, evitando recurrir a controles improvisados que conducen a la materialización de riesgos o situaciones extremas.

9. Adelantar campañas de sensibilización para la identificación de la información intangible de todos los procesos críticos de la Entidad, tales como, la información de los procesos judiciales, información de contratación, información de seguimiento de los proyectos, entre otros.

Elaboró

Ing. Juan Diego Toro Bautista
Auditor Oficina de Control Interno

Aprobó

Gloria Margoth Cabrera Rubio
Jefe de la Oficina de Control Interno