Agencia Nacional de Infraestructura

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

AGENCIA NACIONAL DE INFRAESTRUCTURA
Memorando No. 2016-102-012443-3
Fecha: 07/10/2016 11:39:29->102
FUN: JORGE BERNARDO GOMEZ-103
Anexos:Informe 14 folios

Bogotá D.C

PARA: **JORGE BERNARDO GÓMEZ RODRÍGUEZ**
Gerente de Sistemas y Tecnología

DE: **DIEGO ORLANDO BUSTOS FORERO**
Jefe Oficina de Control Interno

ASUNTO: Informe de auditoría a la seguridad de la información (PEI 124).

Respetado Ing. Jorge:

Comedidamente me permito remitir para su consideración la evaluación efectuada a la seguridad de la información de la entidad (PEI 124), dando cumplimiento al Plan de Evaluación Independiente que viene desarrollando la Oficina de Control Interno.

A continuación se anexa un cuadro, concluyendo lo evidenciado en la evaluación realizada:

Proyecto / Objeto de la auditoría	No Conformidades	Recomendaciones	Observaciones
Auditoría a la seguridad de la información (PEI 124)	1*	7*	0*

*Estas no conformidades, recomendaciones y observaciones se denotan en el capítulo 7 del informe que se anexa a la presente comunicación.

Con fundamento en lo anterior, nos dirigimos a esa dependencia, en los términos del literal g., artículo 4; los literales h, j, y k del artículo 12 y el artículo 14 de la Ley 87 de 1993, y de los Decretos 4165/11 y 1745/11, solicitando atentamente se sirva enviar el plan de mejora sobre el contenido de las no conformidades contenidas en el documento adjunto en consideración a la necesaria documentación de respuesta a través de la adopción de las medidas correctivas o preventivas procedentes o de la oportuna aclaración de las circunstancias de hecho a que haya lugar.

Agencia Nacional de Infraestructura

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

Para contestar cite:
Radicado ANI No.: *RAD_S*
RAD_S
Fecha: *F_RAD_S*

En atención al carácter probatorio del informe proferido y del cumplimiento periódico de seguimiento al contenido de lo comunicado mediante el presente, el término recomendado para la emisión de respuesta es de treinta (30) días contados a partir de la radicación (Art. 14 CPACA).

Con un muy cordial saludo,

DIEGO ORLANDO BUSTOS FORERO
Jefe Oficina de Control Interno

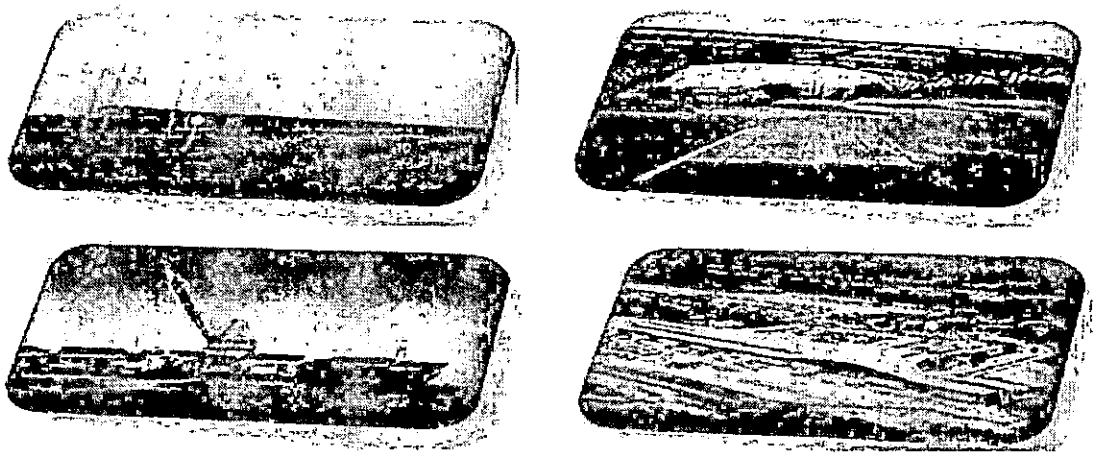
c.c. **JAIME GARCÍA MÉNDEZ** - Vicepresidente de Planeación, Riesgos y Entorno

Anexo: Informe 14 Folios
Proyectó: Juan Diego Toro – Contratista Oficina de Control Interno
Nro Borrador: 2016-102-0023688

Agencia Nacional de Infraestructura

INFORME DE AUDITORÍA

Ministerio de Transporte



INFORME DE AUDITORÍA A LA SEGURIDAD DE LA INFORMACIÓN
PEI 124

2016

TABLA DE CONTENIDO

1. OBJETIVOS

- Conocer la situación exacta de los activos de información de la Agencia, en cuanto a, protección, control y medidas de seguridad.
- Asegurar una mayor integridad, confidencialidad y disponibilidad de la información mediante la recomendación de seguridades y controles.
- Identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en la auditoría de seguridad informática a las instalaciones, redes y servidores
- Evaluar la utilización y aprovechamiento de los equipos de cómputo, de sus periféricos, de las intalaciones, mobiliario y equipos de comunicaciones, asi como del uso de sus recursos técnicos y materiales para el procesamiento de la información.
- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de sus usuarios.
- 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.

2. ALCANCE.

Auditoría realizada dentro de las instalaciones de la Agencia Nacional de Infraestructura, a los centros de cómputo ubicados en los pisos segundo, sexto, séptimo y octavo, a la seguridad informática interna y perimetral. Esta auditoria abarca los componentes de hardware, software e infraestructura con limitantes a:

- La 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.
- La gestión administrativa e informática de los centros de cómputo
- La protección y respaldo de los archivos e información
- La protección, custodia y niveles de acceso a la información

3. METODOLOGÍA.

La metodología empleada por la Oficina de Control Interno, es la usualmente aceptada para la elaboración de este tipo de informes de acuerdo a las normas nacionales e internacionales de auditoria, para lo cual se hizo necesario efectuar una planeación y ejecución de trabajo, donde se tuvieron en cuenta los siguientes aspectos:

- ***Ejecución de la auditoría:*** El día 29 de septiembre de 2016, mediante lista de chequeo adjunta a los papeles de trabajo, se efectuó la inspección a las instalaciones en compañía de los funcionarios Luis Fernando Morales experto de la Gerencia de Sistemas y Julián Hernández de la mesa de ayuda.

- ***Entrevista:*** El día 29 de septiembre de 2016, mediante listas de chequeo adjuntas a los papeles de trabajo, se efectuó entrevista al funcionario Luis Fernando Morales experto de la gerencia de sistemas, para soportar los siguientes temas y que complementan el ejercicio de inspección descrito en el párrafo anterior: **(i) Seguridad en los accesos a las áreas de sistemas, (ii) Seguridad en la información institucional, bases de datos, sistemas operativos y demás software institucional, (iii) Seguridad en los sistemas computacionales y dispositivos periféricos, comunicaciones, redes, sistemas mayores y pc´s, y (iv) Protección contra piratería informática, accesos no autorizados y virus informático.**

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.

En materia de buenas prácticas:

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

5. VERIFICACIÓN DE ANTECEDENTES

El Plan de Acción de la Oficina de Control Interno en años anteriores, incluía dentro de sus auditorías las correspondientes a los componentes de Hardware y Software y su alcance se limitaba a inventariar y reportar el estado de sus equipos, periféricos y aplicativos, pero no contemplaba el componente primordial y es el relacionado con la seguridad de la información.

Es así, que por primera vez en 2013 se incluyó la auditoría a este componente, definiendo en su alcance la seguridad no solo física, sino también la lógica. La claridad de esta amalgama se traduce en la salvaguarda de los bienes tangibles de los sistemas de cómputo de la Agencia, tales como el hardware, periféricos y equipos asociados, las instalaciones eléctricas, las instalaciones de comunicación y de datos, las construcciones, el mobiliario y equipo de oficina, así como la protección a los accesos a los centros de cómputo. En sí, es todo lo relacionado con la seguridad, la prevención de riesgos y protección de los recursos físicos informáticos de la Agencia. Entre tanto, los bienes intangibles de los centros de cómputo, tales como software (aplicaciones, sistemas operativos y lenguajes), así como lo relacionado con los métodos y procedimientos de operación, las políticas informáticas, los niveles de acceso a los sistemas y programas institucionales y el uso robusto de contraseñas, también se incorporaron en el alcance de esta auditoría.

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 y por ende tampoco a lo que se refiere el alcance definido en el párrafo precedente.

Mientras que, en lo relacionado con el Plan de Mejoramiento por Procesos, se evidenciaron 4 no conformidades numeradas así: 76-2014, 188-2015, 189-2015 y 190-2015.

Por lo anterior, este informe de auditoría y las recomendaciones en él descritas, se consolidan como la piedra angular, para afrontar eventuales situaciones de riesgo que comprometan la integridad, confiabilidad y disponibilidad de la información que involucra a la Agencia y sus funcionarios.

6. DESARROLLO DEL INFORME

Concordante con los apartes anteriores y la metodología aplicada a 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. Infraestructura Centros de Cómputo
2. Mapa de Riesgos
3. Políticas y procedimientos
4. Bienes tangibles
5. Bienes intangibles
6. Seguimiento a las no conformidades de auditorías anteriores

Capítulo 1
Infraestructura Centros de Cómputo

Como consecuencia de la visita preliminar se comprobó la existencia de 4 centros de cómputo: 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 a 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

Lista de chequeo centro de cómputo principal 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	
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	

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)		
6	Control de temperatura y humedad			2	2	
7	Planilla de toma de dato permanente para control			2	2	
8	Cableado estructurado		1		1	Desorganizado y sin identificación.
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			2	2	
13	Planilla de control de limpieza del centro de cómputo	0			0	No se cuenta con planillas
14	Sumideros o sifones para evacuación de aguas			2	2	
15	Iluminación permanente y de respaldo			2	2	
16	Estudios de concentración de partículas	0			0	No se han practicado
	Puerta de acceso					
17	Mecanismo de apertura			2	2	
18	Configuración para prevenir el acceso de personal no autorizado	0			0	A la fecha no se ha configurado el sensor y permite el ingreso de personal no autorizado
19	Cortafuego (Material para impedir la propagación del fuego)			2	2	
20	Ventana de inspección	0			0	El data center no cuenta con ventana de inspección.
21	Apertura en sentido de salida			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)		
22	Planilla de control de acceso	0			0	No cuenta con planillas
23	Avisos de señalización y prohibiciones			2	2	
	Sistemas de detección de humo					
24	Equipos extintores		1		1	El equipo extintor de agente limpio FM 200 se evidencia en su manómetro el estado de recarga.
25	Red de sensores			2	2	
26	Red de regaderas			2	2	
27	Planillas de control de mantenimiento			2	2	
	Sistemas de respaldo de energía					
28	Acometida regulada, supresores de picos			2	2	
29	Unit Power Supply (UPS)			2	2	
30	Planillas de control de mantenimiento			2	2	
31	Mobiliario (Racks)			2	2	
	CENTRO DE CÓMPUTO PRINCIPAL (SEGUNDO PISO)	0	2	48	50	80.65%
	CUMPLIMIENTO					Cumple

Lista de chequeo centro de cómputo secundario (6 piso)

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	Natural. Razón para practicar el estudio de concentración de partículas.
6	Control de temperatura y humedad			2	2	
7	Planilla de toma de dato permanente para control			2	2	
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			2	2	
13	Planilla de control de limpieza del centro de cómputo	0			0	No se cuenta con planillas
14	Sumideros o sifones para evacuación de aguas			2	2	
15	Iluminación permanente y de respaldo			2	2	
16	Estudios de concentración de partículas	0			0	No se ha practicado
	Puerta de acceso					
17	Mecanismo de apertura			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	Configuración para prevenir el acceso de personal no autorizado	0			0	A la fecha no se ha configurado el sensor y permite el ingreso de personal no autorizado
19	Cortafuego (Material para impedir la propagación del fuego)	0			0	Puerta de vidrio
20	Ventana de inspección	0			0	No cuenta con ventana
21	Apertura en sentido de salida	0			0	Abre en sentido opuesto
22	Planilla de control de acceso	0			0	No se cuenta con planillas
23	Avisos de señalización y prohibiciones		1		1	Cuenta solo con la prohibición de ingreso.
	Sistemas de detección de humo					
24	Equipos extintores			2	2	
25	Red de sensores			2	2	
26	Red de regaderas	0			0	No cuenta con el sistema
27	Planillas de control de mantenimiento			2	2	
	Sistemas de respaldo de energía					
28	Acometida regulada, supresores de picos			2	2	
29	Unit Power Supply (UPS)			2	2	
30	Planillas de control de mantenimiento			2	2	
31	Mobiliario (Racks)			2	2	

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		Cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple (0)	parcial (1)	total (2)		Observaciones
	CENTRO DE CÓMPUTO SECUNDARIO SEXTO PISO	0	1	44	45	72.58%
	CUMPLIMIENTO					Cumple con recomendaciones

Lista de chequeo centro de cómputo secundario (7 piso)

I. SEGURIDAD EN LA PROTECCIÓN Y CONSERVACIÓN DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		Cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple (0)	parcial (1)	total (2)		Observaciones
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	0			0	
6	Control de temperatura y humedad	0			0	
7	Planilla de toma de dato permanente para control	0			0	
8	Cableado estructurado			2	2	
9	Cableado eléctrico			2	2	
10	Ampliaciones eléctricas			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)		
11	Protección frente a riesgo de corto circuito			2	2	
12	Limpieza del centro de cómputo			2	2	
13	Planilla de control de limpieza del centro de cómputo	0			0	No se cuenta con planillas
14	Sumideros o sifones para evacuación de aguas			2	2	
15	Iluminación permanente y de respaldo			2	2	
16	Estudios de concentración de partículas	0			0	No se han practicado
	Puerta de acceso					
17	Mecanismo de apertura			2	2	
18	Configuración para prevenir el acceso de personal no autorizado	0			0	A la fecha no se ha configurado el sensor y permite el ingreso de personal no autorizado
19	Cortafuego (Material para impedir la propagación del fuego)	0			0	Puerta de vidrio
20	Ventana de inspección	0			0	No cuenta con ventana
21	Apertura en sentido de salida	0			0	Abre en sentido opuesto
22	Planilla de control de acceso	0			0	No se cuenta con planillas
23	Avisos de señalización y prohibiciones		1		1	Cuenta solo con la prohibición de ingreso.
	Sistemas de detección de humo					
24	Equipos extintores			2	2	
25	Red de sensores			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)		
26	Red de regaderas	0			0	No cuenta con el sistema
27	Planillas de control de mantenimiento			2	2	
	Sistemas de respaldo de energía.					
28	Acometida regulada, supresores de picos			2	2	
29	Unit Power Supply (UPS)			2	2	
30	Planillas de control de mantenimiento			2	2	
31	Mobiliario (Racks)			2	2	
	CENTRO DE CÓMPUTO SECUNDARIO SÉPTIMO PISO	0	1	38	39	62.90%
	CUMPLIMIENTO					Cumple con recomendaciones

Lista de chequeo centro de cómputo secundario (8 piso x 2 cuartos: "a" y "b")

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	

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)		
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			2	2	
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	En el secundario se evidencia un socket de lámpara
13	Planilla de control de limpieza del centro de cómputo			2	2	
14	Sumideros o sifones para evacuación de aguas			2	2	
15	Iluminación permanente y de respaldo			2	2	
16	Estudios de concentración de partículas	0			0	No se han practicado
	Puerta de acceso					
17	Mecanismo de apertura			2	2	
18	Configuración para prevenir el acceso de personal no autorizado			2	2	
19	Cortafuego (Material para impedir la propagación del			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)		
	fuego)					
20	Ventana de inspección	0			0	No cuentan con ventana de inspección
21	Apertura en sentido de salida			2	2	
22	Planilla de control de acceso			2	2	
23	Avisos de señalización y prohibiciones			2	2	
	Sistemas de detección de humo					
24	Equipos extintores			2	2	
25	Red de sensores			2	2	
26	Red de regaderas			2	2	
27	Planillas de control de mantenimiento			2	2	
	Sistemas de respaldo de energía					
28	Acometida regulada, supresores de picos			2	2	
29	Unit Power Supply (UPS)			2	2	
30	Planillas de control de mantenimiento			2	2	
31	Mobiliario (Racks)			2	2	
	CENTRO DE CÓMPUTO SECUNDARIO OCTAVO PISO X 2	0	1	56	57	91.94%
	CUMPLIMIENTO					Cumple

Se observaron algunas fallas en aspectos de control, pero en términos generales, los centros de cómputo cuentan con una infraestructura adecuada, las situaciones encontradas y sus recomendaciones se apreciarán en el numeral 7, mientras que la calificación de este capítulo se participará en las conclusiones.

Capítulo 2
Mapa de riesgos del área

El proceso cuenta con el mapa de riesgos vigencia 2016 publicado en el sistema de gestión de calidad (http://54.165.63.184/ANI/index.php) con 4 riesgos identificados y con sus respectivas acciones de mitigación.

II. MAPA DE RIESGOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
1	El área cuenta con un mapa de riesgos			2	2	
2	Se encuentra actualizado			2	2	
3	Contempla planes de contingencia	0			0	No contempla el plan de emergencia y recuperación ante desastres
4	Incorporado al plan general de riesgos			2	2	
5	Planillas de socialización al interior del área			2	2	
6	Se encuentra publicado en cumplimiento del plazo fijado			2	2	
		0	0	10	10	83,33%
	CUMPLIMIENTO					Cumple

Capítulo 3
Políticas y procedimientos

Frente a este particular, se incluye en la auditoría la revisión de la documentación procedimental existente, tal como, las políticas, caracterizaciones y formatos que acompañan al área informática en su rol preponderante de apoyo misional. Los criterios de inspección se enmarcan en la accesibilidad a esta documentación, la oportunidad y si proporciona las características de seguridad que requiere, por su naturaleza, la Agencia.

Para claridad en el informe, se evaluaron los documentos de Políticas Informáticas, caracterización del proceso, procedimientos, formatos e instructivos publicados en la intranet.

III. POLÍTICAS Y PROCEDIMIENTOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
1	La Entidad cuenta con una Política de Seguridad			2	2	
2	Se encuentra actualizado			2	2	
3	Socializada y Publicada			2	2	
4	Política de cambio de claves			2	2	
5	Política de copias de respaldo			2	2	
6	Caracterización del proceso			2	2	
7	Actualizado			2	2	
8	Socializado y publicado			2	2	
9	Procedimientos			2	2	
10	Actualizados			2	2	
11	Socializados y Publicados			2	2	
		0	0	22	22	100.00%
	CUMPLIMIENTO					Cumple

Capítulo 4
Bienes tangibles

Reviste mayor importancia, en el componente de seguridad informática, el de los bienes tangibles. Determinar si se tiene el control de los equipos que componen el núcleo de procesamiento, almacenamiento y respaldo, es tarea primordial de esta auditoría.

Por tanto, se revisaron concienzudamente todos y cada uno de los equipos de cómputo, dispositivos periféricos, equipos de comunicación de voz y datos, equipos de respaldo, monitoreo, dispositivos de grabación PVR, topología del cableado y sistemas mayores, que se alojan en los tres centros de cómputo.

Los criterios de evaluación e inspección aplicados a los equipos descritos fueron: inventario, disposición, configuración, protección, plan de soporte, mantenimiento y garantía. Para llevar a cabo esta inspección se solicitó al ingeniero Javier Zúñiga los documentos pertinentes; copia de los cuales, se anexan a este informe.

Aunque en términos generales este aspecto se encuentra cubierto, y no presenta mayores observaciones, en el acápite de conclusiones y recomendaciones se participarán las propias como oportunidad de mejora.

IV. BIENES TANGIBLES						
		cumplimiento			puntaje	
ITEM	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	
2	Se cuenta con un plan de mantenimiento			2	2	
3	Se lleva control sobre los periodos de garantía			2	2	
4	Se cuenta con servidores espejo para contingencia		1		1	No es totalmente redundante
			1	6	7	87.50%
	CUMPLIMIENTO					Cumple

Capítulo 5
Bienes intangibles

Similar al capítulo anterior, los bienes intangibles se constituyen también, como uno de los componentes más importantes en materia de seguridad informática. Los aplicativos, herramientas informáticas, correo, sistemas de información y bases de datos constituyen el *target* de la evaluación.

Los criterios de evaluación e inspección aplicados al componente blando fueron: inventario, configuración, políticas administrativas, niveles de usuario, roles y responsabilidades, custodia de los medios de instalación, control de distribución, licenciamiento y políticas de claves de acceso, plan de soporte, mantenimiento y garantía.

Los aspectos evaluados para los bienes intangibles develaron algunas observaciones materia de los capítulos posteriores.

V. BIENES INTANGIBLES						
		cumplimiento			puntaje	
ITEM	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			2	2	
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		1		1	Se encuentran fuera del sistema de gestión de calidad
6	Documento de definición de roles y responsabilidades			2	2	

7	Políticas de claves de acceso			2	2	
		0	1	12	13	92.86%
	CUMPLIMIENTO					Cumple

Capítulo 6
Seguimiento a las no conformidades de auditorías anteriores

En la revisión de antecedentes se detectaron 4 no conformidades, que a la fecha permanecen abiertas.

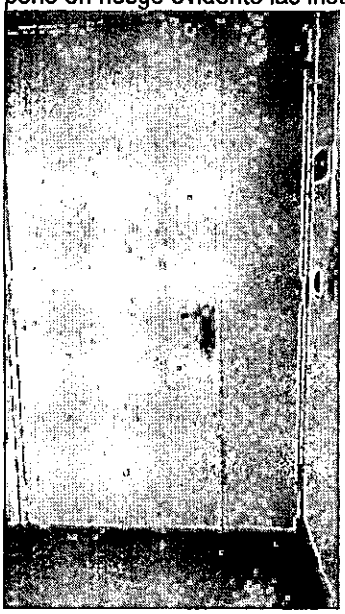
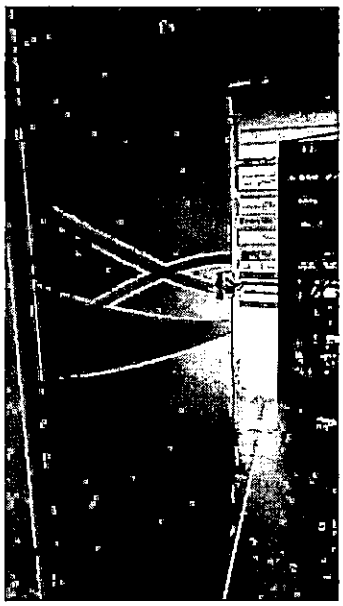
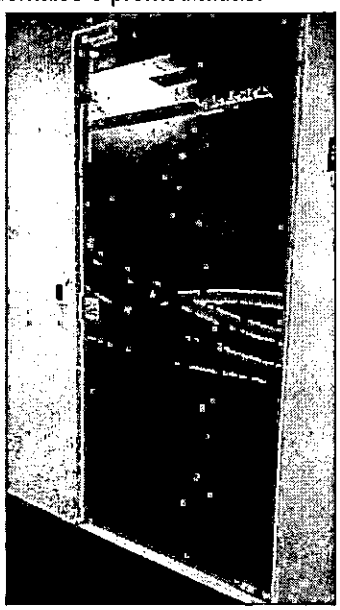
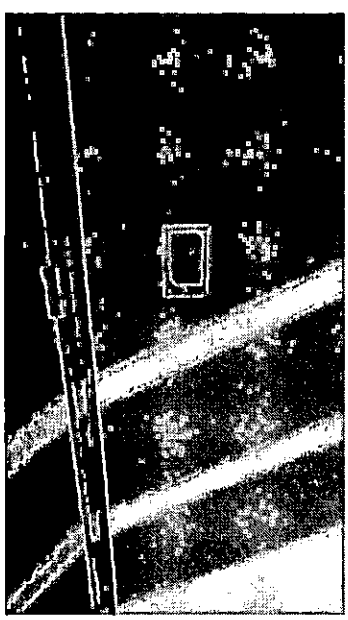
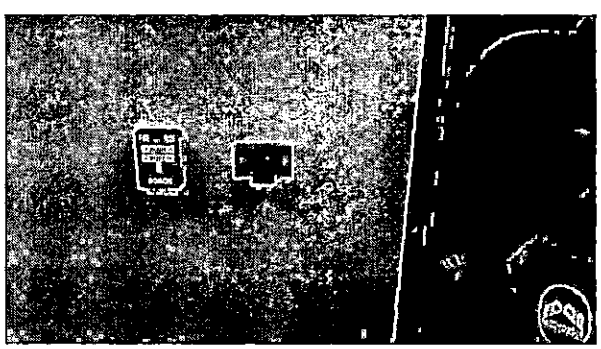
CODIGO	AÑO	DESCRIPCIÓN E IDENTIFICACIÓN NO CONFORMIDAD REAL O POTENCIAL.	CONCESIÓN / ÁREA (RESPONSABLE DE LA IMPLEMENTACIÓN)	AUDITOR.	FECHA AUDITORÍA (dd/mm/aa)	CUMPLE / %	ACCIÓN
76	2014	2. Configurar en el menor tiempo posible los sensores de apertura de las puertas de acceso a los centros de cómputo para impedir el ingreso de personas ajenas al área.	Gerencia de sistemas	JDT	Marzo 2014	NO	Permanece abierta
188	2015	4. Ubicar la señalización necesaria y recomendada en los centros de cómputo.	Gerencia de sistemas Activos fijos	JDT	Sept 2015	NO / 50%	Permanece abierta

189	2015	5 Dotar de mecanismos de riego de agua para eventualidades de incendio en los centros de cómputo de los pisos 6 y 7. Igualmente dotar de sendos equipos extintores los cuartos que conforman el centro de cómputo del piso octavo.	Gerencia de sistemas Activos fijos	JDT	Sept 2015	NO / 50%	Permanece abierta
190	2015	6. Dotar de un aire acondicionado portátil con control de temperatura el centro de cómputo del piso 7, similar al que se encuentra operando en el piso 8.	Gerencia de sistemas Activos fijos	JDT	Sept 2015	NO / 50%	Permanece abierta

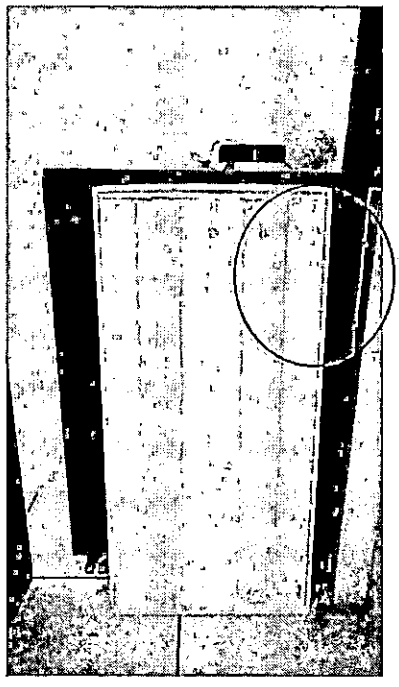
7. SITUACIONES ENCONTRADAS

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:

1. ***Acceso de personal no autorizado:*** Se evidenció que, a pesar de contar con el sensor de apertura de las puertas de ingreso al centro de cómputo principal y a los tres centros auxiliares, estos no se encuentran configurados para permitir el acceso únicamente del personal autorizado; situación que pone en riesgo evidente las instalaciones ante actuaciones accidentales o premeditadas.

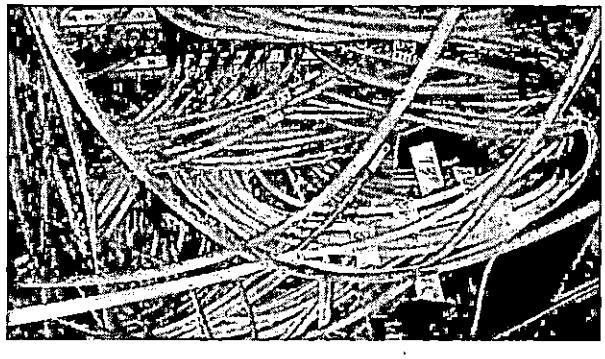






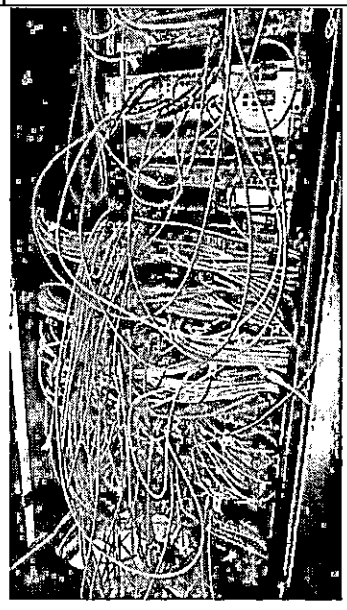
2. ***Objetos en el piso que obstaculizan el tránsito de los pasillos internos:*** En todos los centros de cómputo se encontraron objetos (tapas, escombros y lámparas) que pueden promover la accidentalidad de los funcionarios que laboran en estas áreas. Incluso se evidencia material inflamable como plástico y cartón.

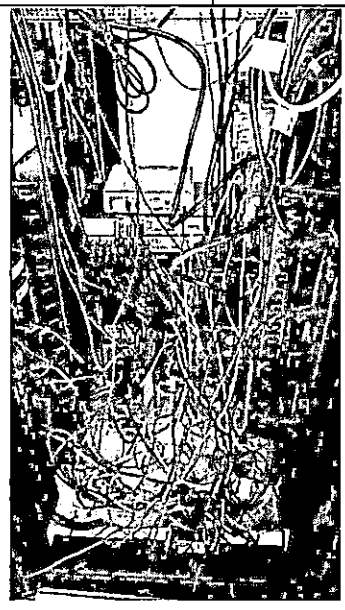


3. ***Mecanismos de Control (Planillas):*** Se pudo observar en la evaluación, la ausencia total de planillas u otro mecanismo de control, para actividades de control de temperatura, limpieza de los centros de cómputo, custodia y manejo de las llaves de los racks y de los cuartos del centro de cómputo del piso octavo, que requieren, por su nivel de riesgo, un seguimiento permanente que incluya los datos tomados de la actividad y la firma del responsable de control y supervisión.

4. ***Desorden en el cableado estructurado:*** Como se puede observar en las siguientes fotos, los rack's de los pisos 2 y 7 evidencian un gran desorden en la disposición y etiquetado de los cables de red, lo cual puede originar pérdida de referencia del punto físico por dificultad en la identificación o desconexión accidental de un usuario activo.







5. ***Sistemas de detección y control de incendio:*** En los centros de cómputo de los pisos 6 y 7 no se evidencia el sistema de regaderas para extinguir incendios. En el piso octavo en ninguno de los dos cuartos que constituyen el centro de cómputo se cuenta con equipo extintor solkaflam. La ausencia de estas medidas de control y mitigación incrementa el impacto del riesgo en caso de incendio.

6. ***Sistemas de refrigeración y control de temperatura:*** En el centro de cómputo del séptimo piso no se cuenta con una fuente de aire, ni natural ni artificial, razón por la cual se percibe una sensación térmica alta, aumentando el riesgo de mal funcionamiento de los equipos.

8. NO CONFORMIDADES, CONCLUSIONES Y RECOMENDACIONES:

Del estudio y revisión efectuada a la seguridad informática de la Agencia, y teniendo en cuenta, todos y cada uno de los componentes, objetos de este informe, se desprende la siguiente calificación:

RESULTADO FINAL						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	NO CUMPLE	CUMPLE CON RECOMENDAC	CUMPLE		Observaciones
		0-60%	61%-80%	81%-100%		
I	Infraestructura centro de cómputo principal			2	2	80,65%

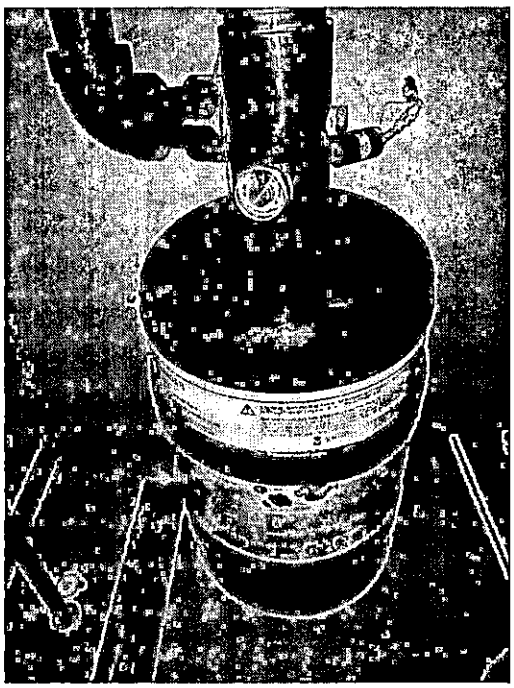
RESULTADO FINAL

		cumplimiento			puntaje	
ITEM	DESCRIPTOR	NO CUMPLE	CUMPLE CON RECOMENDAC	CUMPLE		Observaciones
		0-60%	61%-80%	81%-100%		
I	Infraestructura centro de cómputo secundario (piso 6)		1		1	72,58% ⇧
I	Infraestructura centro de cómputo secundario (piso 7)		1		1	62,90% ⇧
I	Infraestructura centro de cómputo secundario (piso 8)			2	2	91,94% ⇧
II	Mapa de riesgos			2	2	83.33% ⇩
III	Procedimientos y políticas			2	2	100% ⇨
IV	Bienes tangibles			2	2	87.50% ⇩
V	Bienes intangibles			2	2	92.86% ⇩
		0	2	12	14	
	CUMPLIMIENTO				87,50%	Cumple

El sentido de las flechas y los colores de este cuadro corresponden al comportamiento del ítem con respecto al ejercicio auditor del 2015, es decir, en cuanto al sentido puede denotar crecimiento, estabilidad o descenso del ítem.

8.1. No conformidades

Se evidenció en la visita de inspección al centro de cómputo principal del segundo piso que: el extintor de agente limpio fm200, de acuerdo al indicador de su manómetro (ver imágenes a renglón seguido), se encuentra para recarga y adicionalmente no se evidencia la hoja de vida. Lo anterior, en detrimento de la acción de mitigación del riesgo de incendio y contraviniendo lo dispuesto en la norma NTC 3808 de 2004 que expresa lo relacionado con: hoja de vida, cronograma de inspecciones, ubicación, señalización y fechas de vencimientos de recargas, entre otros, para los equipos extintores incluidos los de agente limpio.



8.2. Recomendaciones

Consecuente con la calificación, se sugiere adoptar las siguientes recomendaciones:

1. Crear y diligenciar juiciosamente las planillas de control para las actividades mencionadas, en especial para el control de ingreso de personal al centro de cómputo, control de temperatura y humedad.

2. Configurar en el menor tiempo posible los sensores de apertura de las puertas de acceso a los centros de cómputo para impedir el ingreso de personas ajenas al área.

3. En la medida de las posibilidades presupuestales, cambiar gradualmente las puertas de acceso a los centros de cómputo de los pisos 6 y 7 (actualmente en vidrio), de acuerdo a la normatividad técnica plasmada en este informe.

4. Destinar personal en jornadas no laborales para organizar (peinar) e identificar el cableado estructurado de los racks de los pisos mencionados.

5. Dotar de mecanismos de riego de agua para eventualidades de incendio en los centros de cómputo de los pisos 6 y 7.

6. Dotar de un aire acondicionado portátil con control de temperatura el centro de cómputo del piso 7, similar al que se encuentra operando en el piso 8.

7. Por último se recomienda mantener aseado 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.

Para concluir el informe, es apropiado resaltar que a pesar de las observaciones, 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.

Cordialmente,

DIEGO ORLANDO BUSTOS FORERO
Jefe de Oficina de Control Interno

Elaboró: Juan Diego Toro Bautista - Contratista Control Interno