Agencia Nacional de Infraestructura

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

Para contestar cite:

AGENCIA NACIONAL DE INFRAESTRUCTURA
Memorando No. 2017-102-007866-3
Fecha: 01/08/2017 17:09:43->102
FUN: JAIME ABRAHAM GARCIA-103
Anexos:Informe 10 folios

Bogotá D.C

PARA: **JAIME GARCÍA MÉNDEZ**
Vicepresidente de Planeación, Riesgos y Entorno

MARÍA CLARA GARRIDO GARRIDO
Vicepresidente Administrativa y Financiera

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

ASUNTO: Informe de evaluación integral, con énfasis en riesgos, a los compromisos de las auditorías de hardware, software y seguridad de la información, de las vigencias anteriores (PEI 124).

Respetados vicepresidentes:

Comedidamente me permito remitir para su consideración la evaluación integral (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
Evaluación integral, con énfasis en riesgos, a los compromisos de las auditorías de HW,SW y Seguridad (PEI 124)	1**	5*	0*

*Estas no conformidades, recomendaciones y observaciones se denotan en el capítulo 8 del informe que se anexa a la presente comunicación.
**La no conformidad se abre al proceso de Gestión del Talento Humano, y es quien debe generar el plan de mejoramiento.

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.

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

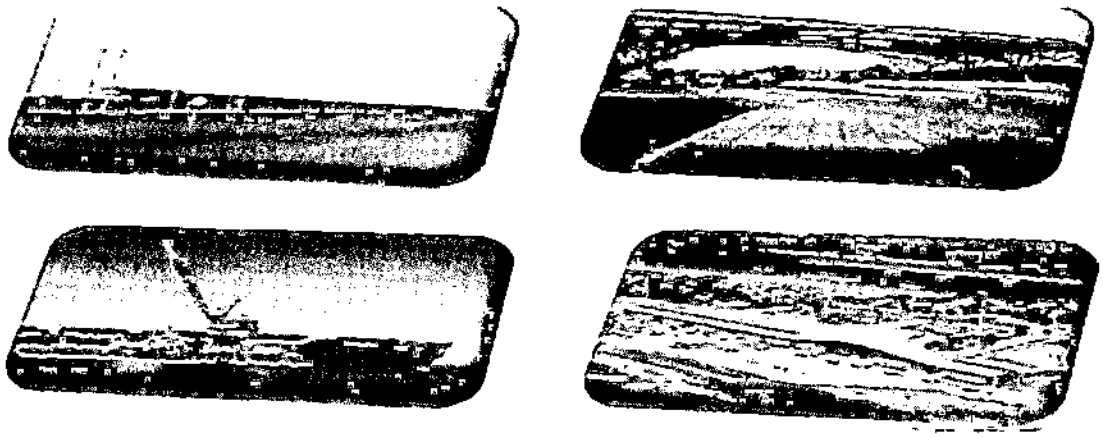
c.c. **JORGE BERNARDO GÓMEZ RODRÍGUEZ** – Gerente de Sistemas
IVONNE DE LA CARIDAD PRADA MEDINA – Gerente de Talento Humano

Anexo: Informe 10 Folios
Proyectó: Juan Diego Toro – Contratista Oficina de Control Interno
Nro Borrador: 2017-102-001303-4

Agencia Nacional de Infraestructura

INFORME DE AUDITORÍA

Ministerio de Transporte



EVALUACIÓN INTEGRAL, CON ÉNFASIS EN RIESGOS, A LOS COMPROMISOS DE LAS AUDITORÍAS DE HARDWARE, SOFTWARE Y SEGURIDAD, DE LAS VIGENCIAS ANTERIORES
PEI 124

2017

Contenido

1. OBJETIVOS

- 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.
- Comprobar el ejercicio de levantamiento de los riesgos asociados al proceso de gestión de la información y comunicaciones.
- Evaluar el avance de la implementación del Sistema de Gestión de Seguridad de la Información SGSI (por sus siglas en español), conforme a los requisitos de la norma ISO/IEC 27001:2013.
- Determinar oportunidades de mejora y recomendaciones.

2. ALCANCE.

Auditoria 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.
- 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 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:

- ***Apertura de la auditoría:*** El dia 15 de mayo de 2017, mediante correo adjunto a los papeles de trabajo, se dio apertura al ejercicio auditor, informando el alcance y las fechas de las actividades principales.

- ***Solicitud de información al proceso de gestión de la información y comunicaciones:*** El día 15 de mayo de 2017, mediante correo 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 el mismo correo se solicitó el inventario de activos de información en materia de datos e información, de usuarios y del recurso humano que apoya el proceso; lo anterior bajo la administración y custodia del equipo de sistemas de información y tecnología.

  Esta información fue allegada a esta auditoría el día martes 23 de mayo de 2017, un día después de lo acordado.

- ***Solicitud de información al proceso de gestión administrativa y financiera (activos fijos):*** El día 15 de mayo de 2017, mediante correo adjunto a los papeles de trabajo, se solicitó la información correspondiente a los contratos de mantenimiento de la infraestructura tecnológica y las pólizas vigentes con las coberturas para corriente débil.

  Esta información fue allegada a esta auditoría, de forma anticipada, el día 18 de mayo de 2017.

- ***Solicitud de información al proceso de gestión del talento humano:*** El día 15 de mayo de 2017, mediante correo adjunto a los papeles de trabajo, se solicitó la información correspondiente al recurso humano que conforma la entidad, discriminando su tipo de contratación.

  Esta información no fue allegada a esta auditoría.

- ***Entrevista:*** El día 24 de mayo de 2017, mediante lista de chequeo incorporada a este informe, se efectuó entrevista a los funcionarios Oscar Fernando Ramos Benavides, Gerardo Enrique Reyes Guarnizo y Javier Alonso Zúñiga Gómez, integrantes del equipo de sistemas de información y tecnología.

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 y Sistema de Gestión de Seguridad de la Información:

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

Como metodología de análisis y gestión de riesgos de los Sistemas de Información:

MAGERIT Versión 2

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, Software y seguridad de la información. Es así, que por primera vez en esta vigencia se incorporó el énfasis en los riesgos identificados en el proceso de gestión de la información y las comunicaciones.

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 5 no conformidades.

Por lo anterior, este informe de auditoría y las recomendaciones en él descritas, se consolidan como las oportunidades de mejora, 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. Revisión del mapa de riesgos del proceso de Gestión de la Información y las Comunicaciones.
2. Seguimiento a la implementación del Sistema de Seguridad de la Información bajo la norma ISO/IEC 27001:2013.
3. 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. *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. Por esta razón, este ejercicio auditor evaluó los controles existentes, las acciones requeridas para reducir el riesgo y los indicadores propuestos.

En este capitulo 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.

[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.

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)	60%
GIC-2	Desarrollar y documentar planes de continuidad de negocio y recuperación ante presencia de desastres	80%
	Establecer la estrategia de redundancia de instalaciones o equipos para asegurar la continuidad del negocio	80%
	Adquirir equipos tecnológicos que apoyen la infraestructura como contingencia ante situaciones de interrupción	80%
GIC-3	Mantener un control estricto para la gestión de asignación de accesos y privilegios a los usuarios creados	70%
	Mantener un control de revisión de los accesos concedidos a los usuarios por parte de los propietarios de la información	70%
	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	80%
GIC-4	Mantener un control estricto para la gestión de asignación de accesos y privilegios a los usuarios creados	80%
	Toma de respaldos de información para restauración en caso necesario	100%
	Asegurar un único repositorio de información para garantizar la integridad de la información	80%

SIGLA	ACCIONES DE MITIGACIÓN DEL RIESGO	AVANCE
GIC-5	Mantener vigente las actividades y/o contrato para realizar los mantenimientos tanto preventivo como correctivo a los equipos de cómputo críticos	80%
	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%
GIC-6	Mantener vigente de las actividades y/o contrato para realizar los mantenimientos tanto preventivo como correctivo a los equipos de cómputo críticos.	80%
	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		**80%**

Fue menester de este ejercicio auditor, realizar una identificación de los riesgos basado 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
	Acceso a datos sensibles o privados	GIC-4

SEGURIDAD	RIESGOS	CORRELACIÓN CON EL MAPA DE RIESGOS
	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 a 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; su cobertura, controles, y acciones de mitigación están alineadas con el desarrollo e implementación del SGSI, con la normatividad vigente y en aras de una eventual certificación de la norma ISO/IEC 27001.

Igualmente se puede concluir que el porcentaje de avance del 80% 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, por lo menos en lo que al proceso de Gestión de la información y las comunicaciones se refiere.

6.2. *Seguimiento a la implementación del Sistema de Seguridad de la Información bajo la norma ISO/IEC 27001:2013*

Para contextualizar al lector de este informe se transcribe la generalidad de la norma, que refleja la importancia de la adopción de esta normatividad para el futuro de la entidad:

> *"Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple."*

Mediante muestreo, se examinó el avance en la conformidad actual del Sistema de Gestión de Seguridad de la Información (SGSI) de la Agencia Nacional de Infraestructura ANI (por sus siglas en español) frente a los requisitos de la norma técnica internacional ISO/IEC 27001:2013 a manera de criterio de auditoría.

Como se manifiesta en el alcance de esta auditoría, no se examina la totalidad de numerales que presenta la norma, que son 130 requisitos, las limitantes de esta auditoría, explora los requisitos con apego a los componentes auditados en vigencias anteriores, para garantizar la superación de las no conformidades o recomendaciones de estas auditorías.

Frente a lo anterior, basado en una lista de chequeo de 33 preguntas, y una vez evaluados los documentos solicitados, así como los disponibles en el espacio colaborativo "sharepoint" de la Entidad, se presentan los siguientes resultados:

ÍTEM	PREGUNTAS	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE CON RECOMENDAC.	CUMPLE	
		(0)	(1)	(2)	
1	¿Cuál fue la metodología utilizada para la construcción del mapa de riesgos?			2	
2	¿Qué recursos se utilizaron en la elaboración del mapa de riesgos del proceso?			2	
3	¿Cuenta la entidad con un Sistema de Gestión de la Seguridad de la Información (SGSI)?			2	
4	¿Cuál es el porcentaje de avance del proyecto de implementación de SGSI (Controles propuestos vs. Controles implementados) - Informe de avance?			2	
5	¿Cuenta la entidad con una Política de Seguridad de la Información?			2	
6	Fecha de la última actualización			2	
7	¿Cuenta la entidad con un inventario de activos de información?			2	
8	Fecha de la última actualización			2	
9	¿Cuenta la entidad con un listado de las amenazas a que están expuestos los activos de información?			2	
10	¿Cuenta la entidad con un listado de las vulnerabilidades de los activos de información?			2	

ITEM	PREGUNTAS	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE CON RECOMENDAC.	CUMPLE	
		(0)	(1)	(2)	
11	¿Cuenta la entidad con un manual de buenas prácticas de control de seguridad de la información?			2	
12	¿Cuenta la entidad con planes de continuidad de negocio y recuperación ante presencia de amenazas (BIA)?			2	
13	¿Cuenta la entidad con una estrategia de redundancia de instalaciones o equipos para asegurar la continuidad del negocio?			2	
14	¿Cuenta la entidad con equipos tecnológicos que apoyen la infraestructura como contingencia ante situaciones de interrupción?			2	
15	¿Cuenta la entidad con una Política de control para la gestión de asignación de accesos y privilegios de los usuarios?			2	
16	¿Cuánta la entidad con el procedimiento de monitoreo y seguimiento a la asignación de accesos a los usuarios?			2	
17	¿Cuenta la entidad con una política de respaldo y restauración?			2	
18	¿Cuenta la entidad con soportes documentales de las pruebas de restauración?			2	
19	¿Cuenta la entidad con soportes documentales de sensibilización a los usuarios acerca de las responsabilidades de respaldo de información?			2	

ÍTEM	PREGUNTAS	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE CON RECOMENDAC.	CUMPLE	
		(0)	(1)	(2)	
20	¿Cuenta la entidad con un único repositorio de información que asegure la integridad?			2	
21	¿Cuenta la entidad con un contrato vigente para realizar los mantenimientos tanto correctivos como preventivos?			2	
22	¿Cuenta la entidad con una política de uso de contraseñas?			2	
23	¿Cuenta la entidad con un documento de acuerdos de niveles de servicio?			2	
24	¿Cuenta la entidad con los manuales de funciones y responsabilidades de los colaboradores de la gerencia de sistemas conforme la política de seguridad de la información?			2	
25	¿Cuenta la entidad con los acuerdos de confidencialidad de los colaboradores de la gerencia de sistemas y de externos que realicen contratos con información de la entidad?			2	
26	¿Se le ha capacitado a los colaboradores de la gerencia de sistemas en seguridad de la información?		1		Se recomienda sensibilizar el equipo de sistemas de cuál es su rol dentro de la implementación
27	¿Cuenta la entidad con un procedimiento para el etiquetado de los activos de información?		1		Se recomienda incluir activos intangibles

ÍTEM	PREGUNTAS	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE CON RECOMENDAC.	CUMPLE	
		(0)	(1)	(2)	
28	¿Cuenta la entidad con capacitaciones al interior de la entidad en el Plan Anual de Capacitaciones, en temas de seguridad de la información?			2	
29	¿Cuenta la entidad con un registro de casos de violación de la seguridad de la información?			2	
30	En caso afirmativo a la anterior pregunta ¿Qué acciones se tomaron?			2	
31	¿Cuenta la entidad con contratos vigentes para mantenimientos de: UPS, Control de temperatura y extinción de incendio?			2	
32	¿Cuenta la entidad con mecanismos que impidan el acceso a personal ajeno a los centros de cómputo?			2	
33	¿Cuenta la entidad con mecanismos que garanticen el control sobre la salida de equipos de cómputo de la entidad?			2	

TOTAL CUMPLIMIENTO	0	2	62	97%
				Cumple

En conclusión, para esta lista de chequeo el cumplimiento es del 97%, evidenciando que no solo se han superado las no conformidades detectadas en los ejercicios anteriores, sino que el camino recorrido en la búsqueda del cumplimiento de la normatividad es el correcto, y los avances obtenidos en esta materia aunado al equipo humano responsable de la implementación y la eventual certificación es el idóneo para esta labor.

Se recomienda socializar al interior del talento humano del equipo de sistemas de información y tecnología, sensibilizando a cada uno de los miembros la importancia, los beneficios, el proceso de implementación del Sistema de Gestión de Seguridad de la Información y su rol dentro de este proceso.

En cuanto al proceso de Gestión Administrativa y Financiera, especificamente al equipo de activos fijos, se recomienda investigar e incluir en el procedimiento GADF-P-007 la identificación de la información intangible de todos los procesos críticos de la entidad, tal como, la información de los procesos judiciales de la entidad, información de contratación, información de seguimiento de los proyectos por mencionar algunas.

Esto podría convertirse en el principal insumo para la generación de un futuro sistema de información, como se ha venido promoviendo desde la oficina de control interno, desde hace poco más de cuatro años, por supuesto con un trabajo mancomunado de toda la entidad y direccionado por el equipo de sistemas de información y tecnologia, para beneficio de la ciudadanía.

6.3. *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 5 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
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	SI / 100%	Cerrar
421	2014	8. Adquirir las guayas necesarias, para garantizar la seguridad de los equipos portátiles con que cuenta la entidad.	Gerencia de activos fijos	JDT	Marzo 2014	SI/ 100%	Cerrar

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 Se encuentra en proceso de contratación
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 Se encuentra en proceso de contratación

212	2016	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 se encuentra para recarga.	Gerencia de sistemas Activos fijos	JDT	**Septiembre de 2016**	**NO / 50%**	**Permanece abierta** **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, ya se superó la etapa de estudios previos y que por esta razón no se da el cierre de las ultimas 3 no conformidades.

7. CONCLUSIONES

1. El mapa de riesgos actual del proceso de Gestión de la Información y las Comunicaciones, contempla la totalidad de riesgos que debería; su cobertura, controles, y acciones de mitigación están alineadas con el desarrollo e implementación del SGSI, con la normatividad vigente y en aras de una eventual certificación de la norma ISO/IEC 27001.

2. El porcentaje de avance del 80% 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, por lo menos en lo que al proceso de Gestión de la información y las comunicaciones se refiere.

3. El cumplimiento para la lista de chequeo de los criterios básicos y asociados a los componentes auditados en ejercicios anteriores es del 97%, evidenciando que no solo se han superado las no conformidades detectadas en los ejercicios anteriores, sino que el camino recorrido en la búsqueda del cumplimiento de la normatividad es el correcto, y los avances obtenidos en esta materia aunado al equipo humano responsable de la implementación y la eventual certificación es el idóneo para esta labor.

4. Se tiene un compromiso decidido de la alta dirección hacia la seguridad de la información actualmente expresada en infraestructura tecnológica y en las bases del sistema de gestión de seguridad de la información, así como de riesgos.

5. Se cuenta con un talento humano altamente calificado y muy comprometido con las labores de gestión de seguridad.

6. Se cuenta con una infraestructura sólida, redundante, tolerante a fallos y pertinente a los propósitos y objetivos institucionales.

7. La infraestructura de seguridad es consistente con el nivel de riesgo al que puede estar expuesta la entidad por su misma naturaleza.

8. El nivel de estandarización de recursos y herramienta facilita la gestión de servicios, reduce riesgos de incompatibilidad y mejora la integración de información sobre eventos de seguridad y comportamiento de la plataforma.

9. Por último, actualmente se está adelantando el proceso de contratación para la solución integral de las debilidades de infraestructura, ya se superó la etapa de estudios previos.

8. NO CONFORMIDADES Y RECOMENDACIONES:

8.1. *No conformidades*

El presente ejercicio presenta una no conformidad para el proceso de Gestión de Talento humano por el incumplimiento en el envío de la información solicitada mediante correo de 15 de mayo de 2017, adjunto a los papeles de trabajo.

8.2. *Recomendaciones*

1. Socializar al interior del talento humano del equipo de sistemas de información y tecnología, sensibilizando a cada uno de los miembros la importancia, los beneficios, el proceso de implementación del Sistema de Gestión de Seguridad de la Información y su rol dentro de este proceso.

2. En cuanto al proceso de Gestión Administrativa y Financiera, específicamente al equipo de activos fijos, se recomienda investigar e incluir en el procedimiento GADF-P-007 la identificación de la información intangible de todos los procesos críticos de la entidad, tal como, la información de los procesos judiciales de la entidad, información de contratación, información de seguimiento de los proyectos por mencionar algunas.

   Esto podría convertirse en el principal insumo para la generación de un futuro sistema de información, como se ha venido promoviendo desde la oficina de control interno, desde hace poco más de cuatro años, por supuesto con un trabajo mancomunado de toda la entidad y direccionado por el equipo de sistemas de información y tecnología, para beneficio de la ciudadanía.

3. Se recomienda al líder del equipo de sistemas de información y tecnología para ejercicios futuros, tener en cuenta las fechas informadas para la entrega de la información, dado que, cualquier retraso entorpece las demás actividades programadas.

4. En cuando a la capacidad de recuperación ante la ocurrencia de incidentes catastróficos, la entidad cuenta con una avanzada infraestructura tecnológica que incluye respaldos aplicables, pero es necesario fortalecer los procesos (y personal relacionado) que permitan asegurar esa recuperación.

5. Por último, se recomienda en el momento que se considere oportuno y previo a la auditoria de certificación bajo la norma ISO/IEC 27001:2013, solicitar a este despacho una preauditoría que incluya la verificación de los 130 criterios o el alcance particular que se determine, como lo manifestado en la entrevista, específicamente para el proceso de contratación de la entidad.

Cordialmente,

DIEGO ORLANDO BUSTOS FORERO
Jefe de Oficina de Control Interno

Elaboró: Juan Diego Toro Bautista - Contratista Control Interno
Apoyó: Sergio Pulido Caycedo – Contratista Control Interno