ANi
Agencia Nacional de Infraestructura

PROSPERIDAD PARA TODOS

AGENCIA NACIONAL DE INFRAESTRUCTURA
Memorando No. 2014-102-002064-3
Fecha: 06/03/2014 11:07:03->102
FUN: ALEJANDRO FORERO GUZ-103
Anexos:Informe

ANi
Agencia Nacional de Infraestructura

Bogotá D.C.

PARA: **ING. ALEJANDRO FORERO GUZMAN.**
Gerente de Sistemas de Información y Tecnología

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

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

Apreciado ingeniero:

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

Cordialmente,

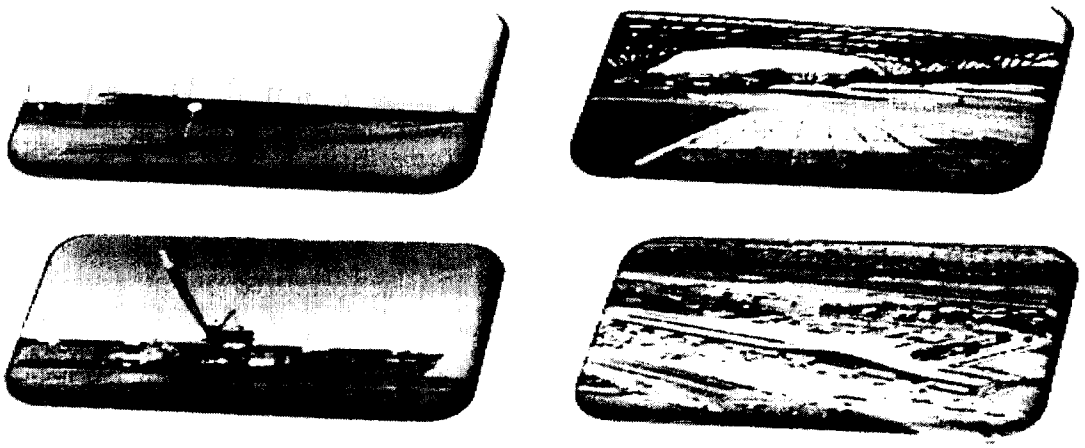
DIEGO ORLANDO BUSTOS FORERO
Jefe de Oficina de Control Interno

Cc Dr. Camilo Mendoza Rozo – Vicepresidente de Planeación, Riesgos y Entorno
Proyectó: Juan Diego Toro - Contratista Oficina de Control Interno.
Nro. Borrador:
GADF-F-010

Agencia Nacional de Infraestructura

INFORME DE AUDITORIA

Ministerio de Transporte



INFORME DE AUDITORÍA A LA SEGURIDAD DE LA INFORMACIÓN
PEI 124

2014

TABLA DE CONTENIDO

I. INTRODUCCIÓN.

Sabido es por los directivos de la entidad que la Oficina de Control Interno se constituye en uno de los instrumentos de alto nivel gerencial que busca asegurar el cumplimiento de los objetivos institucionales a través del engranaje del control como parte del ciclo de una administración exitosa. No en vano, la propia Constitución Política de Colombia lo trata como un principalísimo instrumento gerencial en sus artículos 209 y 269, junto con el control posterior, o de segundo grado, a cargo de las Contralorías, al decir de la H. Corte Constitucional en su sentencia C 1192 del 13 de septiembre de 2000.

El Control Interno, en este orden de ideas, es fundamentalmente axiológico y finalista, pues propende por asegurar que la gestión institucional de todos los órganos del Estado, se oriente hacia la realización de los fines que constituyen su objetivo y, que esta se realice con estricta sujeción a los principios constitucionales que guían el ejercicio de la función pública.

Ahora bien, en desarrollo del citado mandato constitucional, el artículo 9º. de la Ley 87 de 1993, definió la naturaleza de la Oficina de Control Interno, para todas las entidades y organismos de las ramas del poder público, en sus diferentes niveles (art. 5º), así:

"(...) es uno de los componentes del Sistema de Control Interno, de nivel gerencial o directivo, encargada de evaluar la eficiencia, eficacia y economía de los demás controles y de asesorar a la dirección en la continuidad del proceso administrativo, la revaluación de los planes establecidos y en la introducción de los correctivos necesarios para el cumplimiento de las metas u objetivos previstos (...)"

Así las cosas, es preponderante el rol que tanto la Constitución Política y la Ley asignan a la oficina de control interno, dada la importancia sin precedentes que en la nueva visión del control que plasmó el Constituyente de 1991, juega el control interno para la modernización de la administración pública y el mejoramiento de la capacidad de gestión de sus instituciones, todo lo cual, connota un énfasis particular en el control estratégico de gestión, y un serio compromiso con el monitoreo de los resultados de la acción institucional, para el cabal cumplimiento de sus fines y objetivos, de acuerdo a los principios constitucionales rectores del ejercicio de la función pública.

Dicho énfasis se encuentra contemplado en abundante normatividad, jurisprudencia y doctrina, dentro de cuyos contenidos queremos destacar la Ley 87 de 1993 que en su articulado describe la funcionalidad y características del Jefe de la Oficina de Control Interno, robustecida por la Ley 1474 de 2011 que determina la designación del Jefe de dicha Oficina por parte del Presidente de la República con el fin de viabilizar autonomía e independencia en la valoración del control, así como el Decreto 1537 de 2001 que reglamenta parcialmente la aludida Ley 87 de 1993 donde se precisa el rol que deben desempeñar las oficinas de control interno dentro de las organizaciones públicas, enmarcado en cinco tópicos: valoración de riesgos, acompañamiento y asesoría, evaluación y seguimiento, fomento de la cultura de control y relación con entes externos.

En concordancia con lo señalado en las Resoluciones 297 del 24/05/2013 y 852 del 11/12//2012, referentes al manejo de las comunicaciones oficiales en la Agencia Nacional de Infraestructura, en esta oportunidad, nos vamos a adentrar en el terreno de la seguridad informática y sus componentes: infraestructura, hardware y software que abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de las instalaciones que los albergan.

Por su parte la seguridad lógica se refiere a la seguridad en el uso de softwares, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios de la información.

II. 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, asi 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.

III. ALCANCE.

Auditoría realizada dentro de las instalaciones de la Agencia Nacional de Infraestructura, a los centros de cómputo ubicados en los pisos segundo, sexto y séptimo, 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

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

- ***Visita preliminar:*** Se realizó una entrevista el día 11 de diciembre de 2013 a las 11:30 a.m. en compañía del funcionario del área ing. Javier Zúñiga, como parte de la planificación de la auditoria y con el objeto de observar cómo está estructurada la infraestructura informática, su distribución, características, medidas de seguridad visibles a priori y limitantes para la realización de la auditoría, entre otros.

- ***Ejecución de la auditoría:*** El día 23 de diciembre de 2013, mediante lista de chequeo adjunta a los papeles de trabajo, se efectúo la inspección a las instalaciones en compañía del ing. Javier Zúñiga.

- ***Solicitud de documentación soporte:*** Mediante correo de fecha 23 de enero de 2014, se solicitó la documentación que permite respaldar las respuestas a los requerimientos del proceso auditor.

V. 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

VI. 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 y el Plan de Mejoramiento por Procesos, 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.

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.

VII. 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

Capítulo 1
Infraestructura Centros de Cómputo

Como consecuencia de la visita preliminar se comprobó la existencia de 3 centros de cómputo: uno principal ubicado en el segundo piso y dos auxiliares en los pisos 6 y 7. Dado que los tres 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 tres centros debían cumplir con la normatividad técnica y las buenas prácticas. Lo anterior condujo a que en la auditoria se evaluaran los tres 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 PROTECCION Y CONSERVACION 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**	0			0	No se cuenta con el formato, ni se lleva control alguno
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 cuenta con el formato, ni se lleva control alguno

I. SEGURIDAD EN LA PROTECCION Y CONSERVACION DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(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	Se hace con regularidad, pero no se lleva control ni datos de frecuencia
13	Planilla de control de limpieza del centro de cómputo	0			0	No se cuenta con el formato, ni se lleva control alguno
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	Nunca se ha realizado un estudio para este fin
	Puerta de acceso					
17	Mecanismo de apertura			2	2	
18	Configuración para prevenir el acceso de personal no autorizado	0			0	Se hizo prueba de apertura con el carnet de un personal ajeno y permitió el ingreso
19	Cortafuego (Material para impedir la propagación del fuego)			2	2	
20	Ventana de inspección			2	2	
21	Apertura en sentido de salida			2	2	
22	Planilla de control de acceso	0			0	No se cuenta con el formato, ni se lleva

I. SEGURIDAD EN LA PROTECCION Y CONSERVACION DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
						control alguno
23	Avisos de señalización y prohibiciones	0			0	No se evidenciaron
	Sistemas de detección de humo					
24	Equipos extintores		1		1	Sistema fm200, se encuentra vencido
25	Red de sensores			2	2	
26	Red de regaderas			2	2	
27	Planillas de control de mantenimiento	0			0	No se cuenta con el formato, ni se lleva control alguno
	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	0			0	No se cuenta con el formato, ni se lleva control alguno
31	Mobiliario (Racks)			2	2	
	CENTRO DE COMPUTO PRINCIPAL (SEGUNDO PISO)	0	2	40	42	
	CUMPLIMIENTO				67,74%	Cumple con recomendaciones

Lista de chequeo centros de cómputo secundario (6 y 7 piso)

I. SEGURIDAD EN LA PROTECCION Y CONSERVACION 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	0			0	No se cuenta con el formato, ni se lleva control alguno
4	Control de la estática e imantación (Polo a tierra)			2	2	
5	Sistema de Refrigeración			2	2	Ventilación natural
6	Control de temperatura y humedad			2	2	
7	Planilla de toma de dato permanente para control	0			0	No se cuenta con el formato, ni se lleva control alguno
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	Se hace con regularidad, pero no se lleva control ni datos de frecuencia
13	Planilla de control de limpieza del centro de cómputo	0			0	No se cuenta con el formato, ni se lleva control alguno
14	Sumideros o sifones para evacuación de aguas			2	2	

I. SEGURIDAD EN LA PROTECCION Y CONSERVACION DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(2)		
15	Iluminación permanente y de respaldo			2	2	
16	Estudios de concentración de partículas	0			0	Nunca se ha realizado un estudio para este fin
	Puerta de acceso					
17	Mecanismo de apertura			2	2	
18	Configuración para prevenir el acceso de personal no autorizado	0			0	Se hizo prueba de apertura con el carnet de un personal ajeno y permitió el ingreso
19	Cortafuego (Material para impedir la propagación del fuego)		1		1	A pesar de ser en vidrio su resistencia no es tan elevada como la metálica
20	Ventana de inspección	0			0	No cuenta con esta disposición
21	Apertura en sentido de salida	0			0	No cuenta con esta disposición
22	Planilla de control de acceso	0			0	No se cuenta con el formato, ni se lleva control alguno
23	Avisos de señalización y prohibiciones	0			0	No se evidenciaron
	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	0			0	No se cuenta con el formato, ni se lleva control alguno

I. SEGURIDAD EN LA PROTECCION Y CONSERVACION DE LOCALES, INSTALACIONES, MOBILIARIO Y EQUIPOS						
		cumplimiento			puntaje	
ITEM	DESCRIPTOR	no cumple	parcial	total		Observaciones
		(0)	(1)	(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	0			0	No se cuenta con el formato, ni se lleva control alguno
31	Mobiliario (Racks)			2	2	
	CENTRO DE COMPUTO SECUNDARIO (SEXTO y SEPTIMO PISOS)	0	2	36	38	
	CUMPLIMIENTO				61,29%	Cumple con recomendaciones

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 ítem VIII, 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 2012 publicado en la página web con 5 riesgos identificados (Numerales 55 al 59) con sus respectivas acciones de mitigación.

Con relación al mapa de riesgos vigencia 2013, el ingeniero Javier Zúñiga en la entrevista de auditoría, manifiesta su participación en la elaboración de este mapa en cabeza de la Gerencia de Sistemas de Información y Tecnología, y que se encuentra pendiente su aprobación, socialización al interior del área y su publicación.

Por lo anterior, al ser un documento pendiente de aprobación, no pudo ser evaluado y la auditoría se limitó al mapa de riesgos con vigencia 2012. Aclarado esto, el seguimiento a este mapa arrojo algunas recomendaciones que serán materia de los ítems posteriores.

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		1		1	
3	Contempla planes de contingencia			2	2	
4	Incorporado al plan general de riesgos			2	2	
5	Planillas de socialización al interior del área	0			0	No se evidenciaron
6	Se encuentra publicado en cumplimiento del plazo fijado		1		1	
		0	2	6	8	
	CUMPLIMIENTO				66,67%	Cumple con recomendaciones

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 en físico, ninguno en medio digital; todos los documentos se encuentran próximos a su publicación en la intranet.

III. POLITICAS 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		1		1	Lo contenido en la Política General es muy débil, merece robustecerse
5	Política de copias de respaldo		1		1	Lo contenido en la Política General es muy débil, merece robustecerse
6	Caracterización del proceso			2	2	Revisión de los documentos en físico
7	Actualizado		1		1	Control en Intranet y pagina web
8	Socializado y publicado	0			0	Control en Intranet y pagina web
9	Procedimientos			2	2	Revisión de los documentos en físico
10	Actualizados		1		1	Control en Intranet y pagina web
11	Socializados y Publicados	0			0	Control en Intranet y pagina web
		0	**4**	**10**	**14**	
	CUMPLIMIENTO				**63,64%**	**Cumple con recomendaciones**

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 solicitaron 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.		1		1	No se evidencia la propiedad
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			2	2	
		0	2	4	7	
	CUMPLIMIENTO				87,50%	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.

A diferencia de los bienes tangibles, 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		1		1	No contempla todos los equipos
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	
6	Documento de definición de roles y responsabilidades			2	2	Contenido en la Política Informática
7	Políticas de claves de acceso		1		1	Contenido en la política informática
		0	2	10	12	
	CUMPLIMIENTO				85,71%	Cumple

VIII- 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 dos 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. ***Equipo de extinción de fuego vencido:*** Si bien es cierto, se cuenta con un sistema de extinción de incendio con tanques extintores fm-200 de agente limpio, una red de sensores y de riego con excelente cobertura, todo esto pierde efectividad si se encuentra vencida la carga de los tanques, como se evidenció en la evaluación.

3. ***Avisos de prohibiciones o restricciones***: Los centros de cómputo, en sus labores de apoyo misional, se constituyen en espacios cruciales para el funcionamiento normal de la Agencia, razón por la cual se inspeccionó la existencia de avisos de restricción de acceso para personal no autorizado, avisos de prohibición de consumo de alimentos y bebidas, avisos de mantener zonas despejadas, avisos de riesgo eléctrico, por mencionar los más importantes, que disuadan o prevengan, acciones eventuales bien o mal intencionadas.

4. ***Mecanismos de Control (Planillas):*** Se pudo observar en la evaluación, la ausencia total de planillas u otro mecanismo de control, para actividades (control de temperatura, limpieza, mantenimiento, accesos, revisión de equipos, estado de los extintores, custodia y manejo de las llaves de los racks, entre otros) 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.

XI. 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%		

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		1		1	67,74%
I	Infraestructura centro de cómputo secundario (piso 6)		1		1	61,29%
I	Infraestructura centro de cómputo secundario (piso 7)		1		1	61,29%
II	Mapa de riesgos		1		1	66,67%
III	Procedimientos y políticas		1		1	63,64%
IV	Bienes tangibles			2	2	87,50%
V	Bienes intangibles			2	2	85,71%
		0	5	4	9	
	CUMPLIMIENTO				64,29%	Cumple con 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, de acuerdo a la normatividad técnica plasmada en este informe.
4. Desagregar de los inventarios generales los bienes tangibles e intangibles que reposan en los centros de cómputo, lo que permite un mejor control y unas actuaciones mucho más eficaces. Adicionalmente, Incluir en los inventarios tanto de hardware como de software, la discriminación de la propiedad y su curva de funcionamiento.
5. Es imprescindible mantener un control permanente de la carga y estado en general de los extintores mediante la implementación de la planilla de control.

6. Si bien es cierto, la Política de Seguridad Informática contempla sendos capítulos se recomienda, robustecer la política de cambio de claves y backups. Estos dos temas son extremadamente importantes para el blindaje de la Agencia. Es necesario generar hacia los funcionarios una conciencia de obligatoriedad.
7. Socializar y publicar los procesos y procedimientos. Procurar que siempre reposen en la base de conocimiento digital de la Entidad, aun cuando nos encontremos inmersos en procesos de migración.

Para concluir el informe, es apropiado resaltar que a pesar de las observaciones (solo una es mayor, y es la que tiene que ver con la descarga del equipo de extinción de incendio), 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.

XII- PAPELES DE TRABAJO

Para el desarrollo de este informe se emplearon papeles de trabajo, los cuales se encuentran debidamente legajados y numerados en la carpeta PEI-124, estos constituyen parte integral del informe y reposan en la Oficina de Control Interno de la Agencia Nacional de Infraestructura.

Es conveniente precisar que el presente informe se constituye en una herramienta de trabajo que contribuya al mejoramiento continuo de la Seguridad Informática de la entidad, frente a las metas y políticas establecidas para lograr crear un mejor Estado y de esta forma prever graves riesgos.

Cordialmente,

DIEGO ORLANDO BUSTOS FORERO
Jefe de Oficina de Control Interno

Elaboró: Juan Diego Toro Bautista - Contratista Control Interno