Agencia Nacional de Infraestructura

GOBIERNO DE COLOMBIA

Para contestar cite:
Radicado ANI No.: **20181020172563**
Fecha: **29-10-2018**

MEMORANDO

Bogotá D.C.

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

DR. FERNANDO AUGUSTO RAMÍREZ LAGUADO
Vicepresidente de Planeación, Riesgo y Entorno (E)

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

ASUNTO: Informe de evaluación y seguimiento a la implementación del sistema de gestión de la seguridad de la información bajo Norma ISO 27001 (PEI 183)

Respetados doctores:

En cumplimiento al Plan de Evaluación Independiente aprobado por el Comité de Coordinación del Sistema de Control Interno de la Agencia Nacional de Infraestructura, para la vigencia 2018, la Oficina de Control Interno realizó auditoría a la implementación del sistema de gestión de la seguridad de la información bajo Norma ISO 27001 (PEI 183).

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

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

Cordial saludo,

GLORIA MARGOTH CABRERA RUBIO
Jefe Oficina de Control interno

Anexos: Informe 22 folios

cc: Carlos Andrés Montoya Arteaga – VPRE
Oscar Fernando Ramos Benavides - VPRE

Proyectó: Juan Diego Toro Bautista – Contratista OCI
VoBo: GLORIA MARGOTH CABRERA RUBIO (JEFE)
Nro Rad Padre:
Nro Borrador: 20181020043985
GADF-F-010

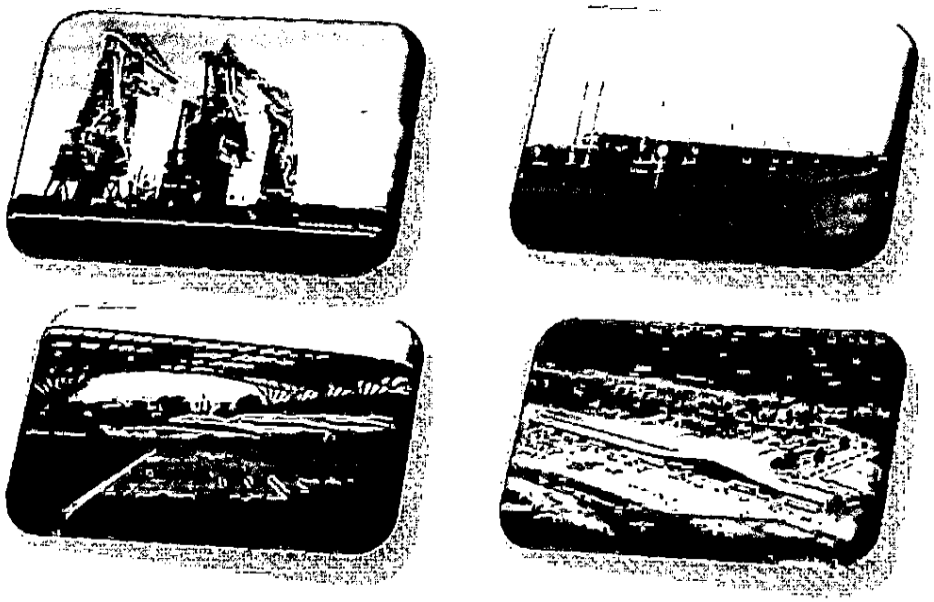
ANI
Agencia Nacional de Infraestructura

GOBIERNO DE COLOMBIA

INFORME DE EVALUACIÓN Y SEGUIMIENTO A LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO NORMA ISO 27001:2013

PEI 183

Ministerio de Transporte



2018

Información y Tecnología sobre los requisitos y controles implementados bajo la norma ISO 27001:2013, en las instalaciones de la Oficina de Control Interno.

- ***Socialización de resultados y cierre de la auditoría:*** El día 23 de octubre de 2018, se socializaron, al responsable del proceso de Sistemas de Información y Tecnología, los resultados de la auditoria y se brindó el espacio para las aclaraciones y o allegar soportes para conjurar las eventuales situaciones evidenciadas en el ejercicio auditor. La anterior actividad se encuentra soportada mediante acta que reposa en los papeles de trabajo.

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

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 ISO- IEC 27001:2013
- Procedimiento EVCI-P-002 Versión 006 del 16 de julio de 2018
- Política de Seguridad y Privacidad de la información GICO-PT-001 Versión 001 del 28/08/2015
- Plan de Tratamiento de riesgos de seguridad y privacidad de la información publicado bajo el link: https://www.ani.gov.co/sites/default/files/u410/plan_de_tratamiento_de_riesgos_de_seguridad_y_privacidad_de_la_informacion_ani.docx
- Decreto 648 de 2017 Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.
- Decreto 612 de 2018 Por medio del cual se fijan directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del Estado.

5. VERIFICACIÓN DE ANTECEDENTES.

En lo pertinente al Plan de Mejoramiento Institucional y al Plan de Mejoramiento por Procesos, se precisa que no se evidenciaron hallazgos, no conformidades o recomendaciones relacionadas con la implementación del Sistema de Gestión de Seguridad de la Información bajo la Norma ISO 27001:2013.

Ahora bien, en la revisión de auditorías relacionadas con aspectos de seguridad de la información, específicamente, la evaluación integral de hardware, software y seguridad de la información PEI 124, adelantada por la Oficina de Control Interno en el mes de abril de 2018, se evidenciaron dos no conformidades 42-2018 y 43-2018 que impactan los controles contenidos en el Anexo A de la Norma ISO 27001:2013.

Por lo anterior, en este ejercicio auditor se evaluarán las acciones adoptadas para estas dos no conformidades y la efectividad en la corrección de la causa raíz que les dio origen.

6. TÉRMINOS Y DEFINICIONES.

A lo largo de este informe se evidenciarán términos técnicos, razón por la cual es importante, antes de entrar al siguiente capítulo, brindar la definición de cada uno de ellos:

SGSI: Sigla para nombrar el Sistema de Gestión de Seguridad de la Información

Gestión: Grupo de acciones necesarias para transformar determinados insumos en productos en un periodo determinado y dentro del marco de una política, programa o proyecto.

Información: Unidad básica de conocimiento. Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.

Seguridad de la Información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la Agencia.

Amenaza: Cualquier agente capaz de aprovechar las fallas de un sistema de seguridad de información para causar daños a los activos de información.

Vulnerabilidad: Punto en el cual un recurso es susceptible de ataque.

Riesgo: Probabilidad de que las amenazas exploten los puntos débiles causando perdida o daño a los activos e impactando los objetivos de la organización.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

PHVA: Como ocurre con todas las normas ISO, la 27001 es un sistema basado en el enfoque del ciclo de mejora continua o de Deming. Dicho ciclo consiste, en Planificar-Hacer-Verificar y Actuar.

7. DESARROLLO DEL INFORME.

La Norma 27001:2013 ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI).

La adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) es una decisión estratégica para una organización. El establecimiento e implementación del SGSI está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales.

Concordante con los apartes anteriores y la metodología aplicada en la auditoría, se elaboró una lista de chequeo, que contemplara todos los temas relevantes para medir el porcentaje de cumplimiento de los requisitos y controles contenidos en la norma ISO 27001:2013.

Los subcapítulos que conforman la auditoría se enuncian a continuación:

1. Verificación del cumplimiento de los objetivos de control y controles de referencia.
2. Verificación del cumplimiento de requisitos.
3. Verificación del proceso de valoración de riesgos de la seguridad de la información.
4. Revisión de los compromisos de la auditoría de seguridad de la información PEI 124 de abril de 2018.

7.1. Verificación del cumplimiento de los objetivos de control y controles de referencia

La Norma ISO 27001:2013 establece 113 puntos de control. Para esta auditoría se evaluaron 53 controles, bajo 7 objetivos de control y que incorporan los dos grandes temas: Las Políticas de seguridad de la información y los controles operacionales.

Consecuente con lo descrito previamente en el alcance de la presente auditoría, se evaluaron los controles del anexo A de la Norma de los siguientes numerales:

- 5. Políticas de seguridad
- 8. Gestión de activos
- 9. Control de acceso
- 11. Seguridad física y del entorno
- 12. Seguridad de las operaciones
- 13. Seguridad de las comunicaciones
- 14. Adquisición, desarrollo y mantenimiento de sistemas

A través de la siguiente lista de chequeo, se evaluaron estos controles:

Norma	Sección	Puntos a evaluar	Cumple	No cumple	N/A	Observaciones
5	POLÍTICAS DE SEGURIDAD					
5.1.	**Orientación de la dirección para la gestión de la seguridad de la información**					
5.1.1.	Conjunto de políticas para la seguridad de la información	1. ¿La Entidad tiene políticas de seguridad de la información?	2			Versión 001 de 2015
		2. ¿Las políticas de seguridad de la información son aprobadas por la administración?		0		No por la alta dirección
		3. ¿Las políticas de seguridad de la información han sido publicadas y comunicadas adecuadamente a los empleados?	2			Publicada y socializada
5.1.2.	Revisión de las políticas para la seguridad de la información	1. ¿Están las políticas de seguridad de la información sujetas a revisión?	2			Versión 002 para aprobación
		2. ¿Regularmente se hacen revisiones de las políticas de seguridad de la información? Especifique la periodicidad en la casilla observaciones.	2			Se está revisando una vez al año
		3. ¿Las políticas de seguridad de la información son revisadas cuando las circunstancias lo amerita?	2			Cambios en normatividad y entorno
8	GESTIÓN DE ACTIVOS					
8.1.	**Responsabilidad por los activos**					
8.1.1.	Inventario de activos	1. ¿Existe un inventario de todos los activos asociados a las instalaciones de procesamiento de información?	2			
		2. ¿El inventario de activos de información contiene información precisa y	2			

Norma	Sección	Puntos a evaluar	Cumple	No cumple	N/A	Observaciones
		actualizada?				
8.1.2.	Propiedad de los activos	¿Tienen los activos de la información un responsable definido que sea consciente de sus responsabilidades?	2			Propietario del activo
8.1.3.	Uso aceptable de los activos	1. ¿Existe una política de uso aceptable para cada clase o tipo de activos de información?	2			GICO-I-018 de 2015
		2. ¿Están los usuarios conscientes de esta política antes de su uso?	2			Envío de E-Cards
8.1.4.	Devolución de activos	¿Existe algún proceso para asegurar que los empleados y los contratistas hagan devolución de los activos de información de propiedad de la Entidad a la terminación de su contrato laboral?	2			Formato de ingreso y retiro GADF-F-014
8.2.	**Clasificación de la información**					
8.2.1.	Clasificación de la información	1. ¿Existe una política que rige la clasificación de la información?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
		2. ¿Existe un proceso por el cual toda la información se pueda clasificar de manera adecuada?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
8.2.2.	Etiquetado de la información	¿Existe un proceso o procedimiento que garantice el etiquetado y la correcta manipulación de los activos de información?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación

Norma	Sección	Puntos a evaluar	Cumple	No cumple	N/A	Observaciones
8.2.3.	Manejo de activos	1. ¿Existe un procedimiento para el manejo de cada clasificación de los activos de información?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
		2. ¿Están los usuarios de los activos de información al tanto de este procedimiento?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
8.3.	**Manejo de medios**					
8.3.1.	Gestión de medios removibles	1. ¿Existe una política que rige el uso de medios removibles?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
		2. ¿Existe algún proceso que diga cómo utilizar adecuadamente los medios removibles?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
		3. ¿Existen políticas de procesos o comunicados a los empleados que informe el uso adecuado de los medios removibles?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
8.3.2.	Disposición de los medios	¿Existe algún procedimiento formal que rija como se deben eliminar los medios removibles?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
8.3.3.	Transferencia de medios físicos	1. ¿Existe alguna política documentada y detallada que defina la forma cómo se debe transportar los medios removibles?		0		No existe en la versión 2015. Tampoco está Incluida en v002
		2. ¿Están protegidos los medios físicos contra el acceso no autorizado, mal uso o perdida durante su transporte?		0		No existe en la versión 2015. Tampoco está Incluida en v002
9	**CONTROL DE ACCESO**					
9.1.	**Requisitos de negocio para el control de accesos**					

Norma	Sección	Puntos a evaluar	Cumple	No cumple	N/A	Observaciones
	equipos	equipos?				
11.2.5.	Retiro de activos	1. ¿Existe un proceso de control de la salida de activos fuera de la Entidad?	2			
		2. ¿Se aplica este proceso?	2			
		3. ¿se realizan controles en sitio?	2			
11.2.6.	Seguridad de equipos y activos fuera de las instalaciones	1. ¿Existe una política de seguridad de activos fuera de la Entidad?	2			
		2. ¿Estas políticas son del conocimiento de todos?	2			
11.2.7.	Disposición segura o reutilización de equipos	1. ¿Existe una política que mencione que los activos de información pueden ser reutilizados o retirados en forma segura?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
		2 ¿Cuándo datos o información es borrada de dispositivos de almacenamiento es debidamente comprobado antes de su reutilización o eliminación?	2			
11.2.8.	Equipos de usuario desatendido	1. ¿La Entidad tiene una política en torno a cómo el equipo desatendido se debe proteger?	2			GICO-I-0018 de 2015
		2. ¿Existen controles técnicos para garantizar que un equipo se ha dejado inadvertidamente desatendido?	2			
11.2.9.	Política de escritorio limpio y pantalla limpia	¿Existe una política de puesto de trabajo despejado y bloqueo de pantalla?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación

Norma	Sección	Puntos a evaluar	Cumple	No cumple	N/A	Observaciones
12	SEGURIDAD DE LAS OPERACIONES					
12.2.	Protección contra códigos maliciosos					
12.2.1.	Controles contra códigos maliciosos	1. ¿Tiene controles para detectar código malicioso?	2			
		2. ¿Tiene controles para evitar la propagación de códigos maliciosos?	2			
		3. ¿La Entidad tiene controles y la capacidad de recuperar de una infección de un código malicioso?	2			
12.3.	Copias de respaldo					
12.3.1.	Respaldo de la información	1. ¿Existe una política de copia de seguridad programada?	2			GICO-I-0020 de 2015
		2. ¿Cumple la política de copia de seguridad de la organización con los marcos legales pertinentes?	2			
		3. ¿Son las copias de seguridad hechas de acuerdo con las políticas?	2			
		4. ¿Se probaron las copias de seguridad?		0		No hay pruebas documentadas
13	SEGURIDAD DE LAS COMUNICACIONES					
13.1.	Gestión de la seguridad de las redes					
13.1.1.	Controles de redes	¿Existe un proceso de administración de red en la Entidad?	2			
13.1.2.	Seguridad de los servicios de red	1. ¿La Entidad implementa un enfoque de gestión del riesgo que identifique todos los servicios de red y los acuerdos de servicio?		0		Se ha presentado dos veces el proceso y no ha pasado a licitación
		2. ¿Está la seguridad exigida en los acuerdos y contratos con proveedores de servicios?	2			

Norma	Sección	Puntos a evaluar	Cumple	No cumple	N/A	Observaciones
		3. ¿Las políticas de seguridad en redes están reglamentadas?	2			
13.1.3.	Separación en las redes	¿La topología de red cumple con la segregación de las redes para las diferentes tareas?	2			Segregación por VLAN por pisos, servidores y servicios.
13.2.	**Transferencia de información**					
13.2.1.	Políticas y procedimientos de transferencia de información	1. ¿Las políticas organizacionales rigen cómo se debe transferir la información?		0		No existe en la versión 2015. Tampoco está Incluida en v002
		2. ¿Están disponibles los procedimientos de cómo se deben transferir los datos a todos los empleados?		0		No existe en la versión 2015. Tampoco está Incluida en v002
		3. ¿Están los controles técnicos pertinentes para prevenir las formas no autorizadas de la transferencia de datos?		0		No existe en la versión 2015. Tampoco está Incluida en v002
13.2.2.	Acuerdos sobre transferencia de información	¿Hacen contratos con terceros y acuerdos dentro de los detalles de la Entidad, los requisitos para obtener información en el negocio de las transferencias?		0		No existe en la versión 2015. Tampoco está Incluida en v002
13.2.3.	Mensajería electrónica	¿Las políticas de seguridad cubren el uso de transferencia de información durante el uso de sistemas de mensajería electrónica?		0		No existe en la versión 2015. Incluida en v002, pendiente de aprobación
13.2.4.	Acuerdos de confidencialidad o de no divulgación	1. ¿Los funcionarios y contratistas firman acuerdos de confidencialidad o de no divulgación?	2			
		2. ¿Son estos acuerdos sujetos a revisión	2			

Norma	Sección	Puntos a evaluar	Cumple	No cumple	N/A	Observaciones
		periódica?				
		3. ¿Se mantienen registros de los acuerdos?	2			
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					
14.2.	Seguridad en los procesos de desarrollo y de soporte					
14.2.1.	Política de desarrollo seguro	1. ¿La Entidad desarrolla software o tecnologías en sistemas?			X	La Entidad tiene tercerizado el desarrollo
		2. ¿Si es así, hay políticas que ordenan la implementación y evaluación de controles de seguridad?			X	La Entidad tiene tercerizado el desarrollo
14.2.6.	Ambiente de desarrollo seguro	1. ¿Se ha establecido un entorno de desarrollo seguro?	2			Ambientes de desarrollo, pruebas y producción en AZURE
		2. ¿Todos los proyectos utilizan el entorno de desarrollo seguro adecuadamente durante el ciclo de desarrollo del sistema?	2			
14.2.8.	Pruebas de seguridad de sistemas	¿Cuándo los sistemas o aplicaciones son desarrollados, la seguridad es probada como parte de los procesos de desarrollo?		0		No se hacen pruebas y las pruebas que realiza el tercero de caja negra, blanca y seguridad no se documentan
14.2.9.	Prueba de aceptación de sistemas	¿Existe un proceso establecido para aceptar nuevos sistemas, aplicaciones o mejoras en la etapa de producción?	2			

La lista de chequeo se encuentra incluida en los papeles de trabajo de la auditoría y es susceptible de consulta sin reserva alguna.

La siguiente tabla resume el cumplimiento de cada uno de los objetivos de control evaluados y el porcentaje y calificación final del subcapítulo:

RESUMEN						
OBJETIVO DE CONTROL	DESCRIPTOR	CUMPLIMIENTO			PUNTAJE	OBSERVACIONES
		NO CUMPLE	CUMPLE CON RECOMEN.	CUMPLE		
		0-60%	61%-80%	81%-100%		
5.	POLÍTICAS DE SEGURIDAD			2	2	83,33%
8.	GESTIÓN DE ACTIVOS	0			0	35,29%
9.	CONTROL DE ACCESO		1		1	73,68%
11.	SEGURIDAD FÍSICA Y DEL ENTORNO			2	2	88,46%
12.	SEGURIDAD DE LAS OPERACIONES			2	2	85,71%
13.	SEGURIDAD DE LAS COMUNICACIONES	0			0	53,85%
14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		1		1	75,00%
		0	2	6	8	
CUMPLIMIENTO					70,76%	CUMPLE CON RECOMENDACIONES

De acuerdo con los criterios evaluados y con la tabla de clasificación descrita en el Capítulo3 del presente informe, el porcentaje del 70,76% **CUMPLE CON RECOMENDACIONES.**

La carta guía para la implementación del SGSI es la Política de Seguridad de Información; esta política es un documento de alto nivel que denota el compromiso de la alta gerencia con la seguridad de la información y contiene la definición desde el punto de vista de la estrategia de la Entidad.

La política debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos y tratamiento de riesgos. Debe estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera.

Si bien se evidenció una política de seguridad y privacidad de la información versión 001 del 28 de agosto de 2015, publicada en la página web de la Entidad bajo el link https://www.ani.gov.co/sites/default/files/u233/gico-pt-001_politica_de_seguridad_y_privacidad_de_informacion_v1_0.pdf,esta política no se alinea completamente con lo dispuesto por la Norma ISO 27001:2013, ni se encuentra avalada por la alta dirección de la Entidad.

Pese a lo anterior, la Gerencia de Sistemas ha venido desarrollando desde el año 2016 una política que integre lo necesario para acompañar el proceso de implementación del Sistema de Gestión de Seguridad de la Información bajo la Norma ISO 27001:2013, pero a la fecha no ha sido avalada por la alta dirección de la Entidad y aunque se evidencian vacíos en el cumplimiento de algunos controles, es un versión que contempla la gran mayoría de los lineamientos dispuestos en la Norma ISO 27001 y supera con amplitud lo contenido en la versión 001 publicada desde 2015.

Como bien se declaró párrafos atrás, esta política denota el compromiso de la alta dirección con la adopción de un derrotero que acompañe el cumplimiento de los requisitos y controles contenidos bajo la Norma ISO 27001:2013 y su falta de aprobación, compromete el requisito 5.1. Liderazgo y compromiso de la Norma, al haber transcurrido 3 años desde la primera versión de un documento que debe ser revisado y actualizado permanentemente con los cambios emanados por las políticas de Gobierno Digital y demás cambios normativos.

Si bien se evidencia una Política de Seguridad V001 publicada, esta no contempla los lineamientos para el cumplimiento de la totalidad de los requisitos y controles requeridos por la Norma para la implementación del Sistema de Gestión de Seguridad de la Información, incumpliendo el literal c) del requisito 5.2 Política, y el literal a) del requisito 5.3. Roles, responsabilidades y autoridades en la Organización.

Lo anterior aunado al hecho de que se evidenciaron en el borrador de la política versión 002, pendiente de revisión y aprobación por la alta dirección, la incorporación del cumplimiento de controles ausentes en la versión 001, también se extrañaron controles, tales como, transferencia de medios físicos, derechos de acceso y transferencia de información. Esta evidencia repercute también en la baja calificación obtenida en el cumplimiento de los controles 8. Gestión de activos y 13. Seguridad de las comunicaciones.

7.2. Verificación del cumplimiento de requisitos

La Norma ISO 27001:2013 establece 10 requisitos de los cuales 7 (del 4 al 10) permiten establecer, implementar, mantener y mejorar continuamente un SGSI dentro del contexto de una organización. Para esta auditoría se evaluaron 5 requisitos, consecuente con la etapa del ciclo PHVA en el que se encuentra la implementación del SGSI. Los requisitos establecidos en la Norma ISO 27001:2013 son genéricos y están previstos para ser aplicables a todas las organizaciones independientemente de su tipo, tamaño o naturaleza.

Consecuente con lo descrito previamente en el alcance de la presente auditoría, se evaluaron los requisitos:

- 5. Liderazgo
- 6. Planificación
- 7. Soporte
- 8. Operación
- 9. Evaluación de desempeño

A través de la siguiente lista de chequeo, se evaluaron estos requisitos:

Requisito	Descripción	Deber	Cumple	Parcial	No cumple	Observaciones OCI
5.	Liderazgo					
5.1.	Liderazgo y compromiso	La alta dirección debe demostrar liderazgo y compromiso con respecto al SGSI		1		La Entidad contrató personal idóneo, el cual, ha adelantado las acciones de cumplimiento, sin embargo, a la fecha estas acciones no han sido aprobadas por la alta dirección.
5.2.	Política	La alta dirección debe establecer una política de seguridad de la información		1		Esta desactualizada, incompleta y avalada por la gerencia de sistemas del 2015
5.3.	Roles, responsabilidades y autoridades en la organización	La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen		1		No cumple con la totalidad de requisitos y controles dispuestos por la norma
6.	Planificación					
6.1.	Acciones para tratar riesgos y oportunidades					
6.1.1.	Generalidades	Al planificar el SGSI, la organización debe considerar el conocimiento de la organización y su contexto y comprender las	2			Se evidencian los documentos de comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI

Requisito	Descripción	Deber	Cumple	Parcial	No cumple	Observaciones OCI
		necesidades y expectativas de las partes interesadas y determinar los riesgos y oportunidades que es necesario tratar				
6.1.2.	Valoración de riesgos de la seguridad de la información	La organización debe definir y aplicar un proceso de valoración de riesgos de la seguridad de la información	2			Se evidencian los listados de activos de información, la identificación de las amenazas y vulnerabilidades, los riesgos y sus dueños y su valoración.
6.1.3.	Tratamiento de riesgos de la seguridad de la información	La organización debe definir y aplicar un proceso de tratamiento de riesgos		1		No están alineados con la totalidad de controles que aplican de la Norma ISO 27001
6.2.	Objetivos de seguridad de la información y planes para lograrlos	La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes	2			Se evidencian los objetivos de seguridad de la información y el diligenciamiento de la declaración de aplicabilidad
7.	Soporte					
7.1.	Recursos	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI	2			La gerencia de sistemas cuenta con los recursos necesarios para adelantar estas actividades.

Requisito	Descripción	Deber	Cumple	Parcial	No cumple	Observaciones OCI
7.2.	Competencia	La organización debe determinar la competencia necesaria de las personas que realizan las actividades propias del SGSI	2			Se evidenciaron los estudios previos, el objeto contractual y sus funciones y la experiencia del responsable de dirigir el proyecto de implementación del SGSI
7.3.	Toma de conciencia	Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de la política y su contribución a la eficacia del sistema	2			Se han adelantado campañas de sensibilización al interior del equipo de sistemas
7.4.	Comunicación	La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGSI		1		Se evidencia la matriz RACI, sin embargo, no se han formalizado, ni aplicado las directrices
7.5.	Información documentada	El SGSI debe incluir la información documentada requerida por esta norma		1		La mayoría de información se encuentra documentada en manuales, políticas, procedimientos, instructivos y formatos, sin embargo, no se evidencian documentos para la definición de perímetros de seguridad, pruebas de simulacros del servicio de

Requisito	Descripción	Deber	Cumple	Parcial	No cumple	Observaciones OCI
						suministro alterno de energía, Pruebas de recuperación de backups, entre otros
8.	Operación					
8.1.	Planificación y control operacional	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el requisito de planificación.		1		El SGSI no ha superado la etapa del Hacer del ciclo PHVA, a pesar de que se adelantan varias actividades que se encuentran implementadas y operando
8.2.	Valoración de riesgos de seguridad de la información	La organización debe llevar a cabo valoraciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos		1		El SGSI no ha superado la etapa del Hacer del ciclo PHVA, sin embargo, esta actividad se adelanta periódicamente en virtud de que se encuentra contenida en el mapa de riesgos de la Entidad.
8.3.	Tratamiento de riesgos de la seguridad de la información	La organización debe implementar el plan de tratamiento de riesgos de la información y debe conservar la		1		El SGSI no ha superado la etapa del Hacer del ciclo PHVA, sin embargo, esta actividad se adelanta periódicamente en

Requisito	Descripción	Deber	Cumple	Parcial	No cumple	Observaciones OCI
		información documentada de los resultados de este tratamiento.				virtud de que se encuentra contenida en el mapa de riesgos de la Entidad.
9.	Evaluación de desempeño					
9.1.	Seguimiento, medición, análisis y evaluación	La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del SGSI		1		El SGSI no ha superado la etapa del Hacer del ciclo PHVA, sin embargo, esta actividad se adelanta periódicamente en virtud de que se diligencian mensualmente los indicadores del proceso y ahí están inmersos los de las actividades relacionadas con la implementación de buenas prácticas de la Norma, entre otros.
9.2.	Auditoría interna				0	El SGSI no ha superado la etapa del Hacer del ciclo PHVA. No se evidencian auditorías por parte del Sistema de Gestión de Calidad en las etapas planeativas ni de hacer del ciclo PHVA.

La lista de chequeo se encuentra incluida en los papeles de trabajo de la auditoría y es susceptible de consulta sin reserva alguna.

La siguiente tabla resume el cumplimiento de cada uno de los requisitos evaluados y el porcentaje y calificación final del subcapítulo:

RESUMEN						
REQUISITO	DESCRIPTOR	CUMPLIMIENTO			PUNTAJE	OBSERVACIONES
		NO CUMPLE	CUMPLE CON RECOMEN.	CUMPLE		
		0-60%	61%-80%	81%-100%		
5.	LIDERAZGO	0			0	50,00%
6.	PLANIFICACIÓN			2	2	87,50%
7.	SOPORTE		1		1	80,00%
8.	OPERACIÓN	0			0	50,00%
9.	EVALUACIÓN DE DESEMPEÑO	0			0	25,00%
CUMPLIMIENTO					58,50%	NO CUMPLE

De acuerdo con los criterios evaluados y con la tabla de clasificación descrita en el Capítulo 3 del presente informe, el porcentaje del 58,50% **NO CUMPLE.**

Se incumple el requisito **5. Liderazgo** de la Norma, al no contar con una política de seguridad actualizada, que cumpla con la totalidad de controles descritos en la norma y no estar aprobada por la alta dirección de la Entidad.

Asimismo, se evidencia el incumplimiento de los requisitos **8. Operación** al no poder llevar a cabo actividades, tales como, seguimiento al tratamiento de los riesgos o el control operacional y **9. de Evaluación de desempeño** al no poder revisar internamente el SGSI, al no realizar auditorías internas del SGSI, aplicar indicadores y métricas y a partir de ello adoptar acciones correctivas y de mejora.

7.3. Verificación del proceso de valoración de riesgos de la seguridad de la información.

En la actualidad, las organizaciones se enfrentan a muchos riesgos e inseguridades procedentes de focos diversos. Esto quiere decir que los activos de información, uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades.

La seguridad de estos activos de información está en función de la correcta gestión de una serie de factores como: la capacidad, la elaboración de un plan de contingencia frente a los incidentes, el análisis de riesgos,

las competencias, el grado de involucración de la alta dirección, las inversiones en seguridad y el grado de implementación de controles.

Aunque existen muchos soportes documentales diferentes, como la información en papel o los soportes analógicos participantes, lo cierto es que, en la actualidad, la mayor parte de la información gestionada por una organización se sustenta en la información automatizada a través de las nuevas herramientas de las TIC's. Por este motivo la Norma ISO 27001 trata aspectos mayoritariamente del rango informático.

La Gerencia de Sistemas alineado con lo dispuesto en la Norma ha realizado el levantamiento de la información: listado de activos, listado de amenazas, listado de vulnerabilidades:

Listado de activos de información

							Valoración de activos (Seguridad de la Información)			
Código activo	Activo de Información	Tipo de activo	Descripción	UBICACIÓN	Proceso/Área	Propietario de Activo (Responsabilidad)	Integridad	Confidencialidad	Disponibilidad	Valor activo
A_GICO_1	CHASIS TIPO BLADE 16 CUCHILLAS	(HD) Hardware	Componente que permite la instalación de cuchillas (blade)	Rack	Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	2	2	2	6
A_GICO_2	RACK	(HD) Hardware	Gabinete para alojar y proteger físicamente los equipos allí instalados (Data center (4), Piso 6, Piso 7, Piso 8 (2)	Centro de Datos	Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	1	3	2	6
A_GICO_3	FIREWALL	(HD) Hardware	Dispositivo para controlar y permitir los accesos bien externos o internos hacia internet, LAN	Centro de Datos	Equipo de Sistemas de la Información y Tecnología	Gerente de Sistemas	3	3	3	9

							Valoración de activos (Seguridad de la Información)			
Código activo	Activo de Información	Tipo de activo	Descripción	UBICACIÓN	Proceso/Área	Propietario de Activo (Responsabilidad)	Integridad	Confidencialidad	Disponibilidad	Valor activo
			(seguridad perimetral, políticas y reglas de red)							
A_GICO_4	SISTEMA OPERATIVO IOS	(SW) Software	Sistema Opertivo de Firewall	Fortinet 600C	Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_5	SWICTH - Core_ANI 1 HA	(HD) Hardware	Core - Permiten la conectividad hacia LAN, Switch Core, Administrador de DHCP - VLANS	Rack - Centro de Datos	Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_6	SWICTH - Core_ANI 2 HA	(HD) Hardware	Respaldo	Rack - Centro de Datos	Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_7	SAN HITACHI	(HD) Hardware	Discos para almacenamiento de información de gran volúmen	Rack - Centro de Datos	Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_8	STORAGE MANAGER	(HD) Hardware	Interface de administración de la SAN (Arreglos de discos)	Rack - Centro de Datos	Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_9	SERVIDOR	(HD) Hardwar	Aloja el software	Rack - Centro	Equipo Sistem	Gerente de	3	3	3	9

							Valoración de activos (Seguridad de la Información)			
Código activo	Activo de Información	Tipo de activo	Descripción	UBICACIÓN	Proceso/Área	Propietario de Activo (Responsabilidad)	Integridad	Confidencialidad	Disponibilidad	Valor activo
	HITACHI	e	para realizar las actividades de respaldo de información	de Datos	as de Información y Tecnología	Sistemas				
A_GICO_10	WINDOWS SERVER 2012 R2 ESTANDAR	(SW) Software	Sistema operativo	Servidor	Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_11	BACKUP EXCEL	(SW) Software	Administrador de software para programación de las actividades de toma de respaldo de información		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_12	LIBRERÍA ORACLE	(SW) Software	Permite la transferencia de la información de respaldo a los medios de almacenamiento externos (cinta)		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_13	SWITCH SAN	(HD) Hardware	Reciben la conectividad desde la SAN hacia los servidores		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_1	SWITCH BROCAD	(HD) Hardwar	Interconector entre la		Equipo Sistem	Gerente de	3	3	3	9

							Valoración de activos (Seguridad de la Información)			
Código activo	Activo de Información	Tipo de activo	Descripción	UBICACIÓN	Proceso/Área	Propietario de Activo (Responsabilidad)	Integridad	Confidencialidad	Disponibilidad	Valor activo
4	E	e	SAN y los servidores		as de Información y Tecnología	Sistemas				
A_GICO_15	CONTROLADORA INALAMBRICA	(HD) Hardware	Controladora Wireless Piso 2, 4 AP, Piso 6 - 3 AP, Piso 7 - 3 AP		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_16	ROUTER DE UNE	(RED) Redes y Comunicaciones	Canal de Internet HA de 256 MB y troncal SIP 60 lineas		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_17	AIRE DE PRESICION	(HD) Hardware	Enfriador de aire para el datacenter refrigerado por agua 100 T		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_18	SIIF	(SW) Software	Sistema de información financiero		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_19	SERVIDOR DL 380	(HD) Hardware	Servidor para alojar máquinas virtuales		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_20	SERVIDOR ML 310	(HD) Hardware	Servidor para aplicación		Equipo Sistemas de	Gerente de Sistema	3	3	3	9

							Valoración de activos (Seguridad de la Información)			
Código activo	Activo de Información	Tipo de activo	Descripción	UBICACIÓN	Proceso/Área	Propietario de Activo (Responsabilidad)	Integridad	Confidencialidad	Disponibilidad	Valor activo
			de ORFEO		Información y Tecnología	s				
A_GI CO_21	PC SERVIDOR HP dc 5700	(HD) Hardware	FTP Control Interno - Repositorio de información		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GI CO_22	VIRANI 1 (Servidor Físico)	(HD) Hardware	Hyper-V		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GI CO_23	VIRANI 2 (Servidor Físico)	(HD) Hardware	Hyper-V		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GI CO_24	VIRANI 3 (Servidor Físico)	(HD) Hardware	Hyper-V		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GI CO_25	VIRANI 4 (Servidor Físico)	(HD) Hardware	Hyper-V		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GI CO_26	VIRANI 6 (Servidor Físico)	(HD) Hardware	Hyper-V		Equipo Sistemas de Inform	Gerente de Sistemas	3	3	3	9

							Valoración de activos (Seguridad de la Información)			
Código activo	Activo de Información	Tipo de activo	Descripción	UBICACIÓN	Proceso/Área	Propietario de Activo (Responsabilidad)	Integridad	Confidencialidad	Disponibilidad	Valor activo
					ación y Tecnología					
A_GICO_27	VIRANI7(Servidor Físico)	(HD) Hardware	Hyper-V		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_28	HYPERV1 (Servidor Físico)	(HD) Hardware	Hyper-V		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_29	ANIAZ-SGI-AP01 (Servidor Virtual)	(HD) Hardware	Nuevo SGI		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_30	SVCDANI01	(HD) Hardware	Domain Controller - IIS		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_31	DC-ANI-AZURE	(SVC) Servicio Contratado	Controlador Dominio Nuevo		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_32	SHP-ANI-AZURE	(SVC) Servicio Contratado	Sharepoint Tableros de Control		Equipo Sistemas de Información y	Gerente de Sistemas	3	3	3	9

							Valoración de activos (Seguridad de la Información)			
Código activo	Activo de Información	Tipo de activo	Descripción	UBICACIÓN	Proceso/Área	Propietario de Activo (Responsabilidad)	Integridad	Confidencialidad	Disponibilidad	Valor activo
					Tecnología					
A_GICO_33	SQLBI-ANI-AZURE	(SVC) Servicio Contratado	SQLServer , instancia de trableros de control, Instancia nuevo SIG		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_34	ANIAZ-SGI-AP01	(SVC) Servicio Contratado	APLICACION SGI		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_35	ANIAZ-UNI-AP02	(SVC) Servicio Contratado	APLICACION UNIANI		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_36	SVCDANI6	(SVC) Servicio Contratado	Controlador Dominio Nuevo Secundario		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_37	CDANI3	(HD) Hardware	Controlador Dominio Nuevo Primario		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_38	SVCDANI3P	(HD) Hardware	Domain Controller INCO		Equipo Sistemas de Información y Tecnol	Gerente de Sistemas	3	3	3	9

							Valoración de activos (Seguridad de la Información)			
Código activo	Activo de Información	Tipo de activo	Descripción	UBICACIÓN	Proceso/Área	Propietario de Activo (Responsabilidad)	Integridad	Confidencialidad	Disponibilidad	Valor activo
					ogía					
A_GICO_39	SVPORFEO	(HD) Hardware	Servidor de Aplicación de ORFEO		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_40	CDANI1	(HD) Hardware	Controlador de Dominio - Segundario Antiguo		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_41	CDANI5	(HD) Hardware	Controlador Primario Antiguo - IIS		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_42	ORFEOO RACLE	(SW) Software	Base de datos		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9
A_GICO_43	DATA CENTER	(HD) Hardware	Lugar que por su alta seguridad debe alojar equipo de computo crítico y sensible para la operación de las actividades misionales de la		Equipo Sistemas de Información y Tecnología	Gerente de Sistemas	3	3	3	9

							Valoración de activos (Seguridad de la Información)			
Código activo	Activo de Información	Tipo de activo	Descripción	UBICACIÓN	Proceso/Área	Propietario de Activo (Responsabilidad)	Integridad	Confidencialidad	Disponibilidad	Valor activo
			Entidad							

Catálogo de amenazas

CATALOGO DE AMENAZAS
Uso no autorizado de recursos (equipos de comunicación, medios de almacenamiento, sistemas de información, computadores)
Abuso de derechos (de usuario, administrador)
Acceso no autorizado (a oficinas, edificio, sala, centro de cómputo, sistema de información, documentación, información, entre otros).
Actos fraudulentos (suplantación, fraude, venta de información, soborno, extorsión, falsificación de derechos, entre otros)
Ataque malicioso (explosivos, químicos, vandalismo, hurto, radiación electromagnética, entre otros).
Ataques contra el sistema (negación del servicio, manipulación de software, manipulación de equipo informático entre otros)
Cierre de operación de un proveedor o contratista crítico para la Entidad
Código malicioso (troyanos, gusanos, bomba lógica, entre otros)
Contaminación, Pandemias, virus
Daño físico (fuego, agua, humedad, contaminación química, construcción, entre otros)
Déficit de personal
Desastre natural (temblor, terremoto, inundación, incendio, rayos, contaminación química entre otros)
Destrucción de equipos o medios
Deterioro del sistema o medio de almacenaje
Divulgación no autorizada
Empleados (Acciones involuntarias y/o deliberadas)
Error en el uso (de equipos, medios, información, sistemas o servicios de información)
Errores de transmisión o almacenamiento
Espionaje (interceptación, ingeniería social)
Falla / degradación o mal funcionamiento del software o hardware
Falla de la red interna
Falla de suministro de servicios esenciales (agua, gas, aire acondicionado)
Falla en el suministro de energía (pérdida suministro de energía, planta eléctrica, UPS, banco de baterías)

CATALOGO DE AMENAZAS
Falla o corrupción del software.
Falla para respaldar la información.
Falla sistema de comunicaciones (Internet, canales, Radio, entre otros).
Fuego, agua, humedad, variaciones de temperatura/voltaje, radioactividad, polvo, gases, oxidación, campos electromagnéticos, entre otros.
Hurto o robo (información, documentos, medios o equipos)
Incumplimiento de leyes o regulaciones (propiedad intelectual, entre otros)
Incumplimiento de políticas o procedimientos internos.
Mal Funcionamiento
Incumplimiento en el mantenimiento
Incumplimiento en el servicio de mantenimiento
Incumplimiento en los SLA´s
Intrusión o acceso forzado (instalaciones, sistemas de información, información)
Intruso externo (Ej: Exempleados, delincuente informático, competidores)
Pérdida de información (contenida en documentación física o digital)
Piratería
Proveedor o contratista
Recuperación de medios reciclados o desechados
Saturación del sistema de información
Uso de software no licenciado o no autorizado

Catálogo de vulnerabilidades

CATALOGO DE VULNERABILIDADES
Acceso no controlado a información sensible / confidencial.
Acceso o uso no controlado del sistema de información (software, aplicativo).
Acceso o uso no controlado.
Almacenamiento de equipos sin protección.
Almacenamiento de información sin protección
Arquitectura insegura de la red.
Ausencia de "terminación/bloqueo de la sesión" cuando se abandona la estación de trabajo.
Ausencia de control de los activos que se encuentran fuera de la instalaciones.
Ausencia de controles y verificaciones en los procesos de selección y contratación de personal.
Ausencia de esquemas de respaldo.
Ausencia de logs o registros de auditoría.
Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros.

CATALOGO DE VULNERABILIDADES
Ausencia de planes de continuidad.
Ausencia de procedimiento de control de cambios.
Ausencia de procedimiento formal para la autorización de la información disponible al público.
Ausencia de responsables sobre la gestión en seguridad de la información y/o continuidad de negocio.
Ausencia de segmentación de la red.
Ausencia de sistemas y/o procedimientos de monitoreo de los recursos de procesamiento de información.
Ausencia o insuficiencia de procedimientos de control de cambios.
Ausencia o insuficiencia de actualizaciones.
Ausencia o insuficiencia de cláusulas contractuales y/o acuerdos de confidencialidad.
Ausencia o insuficiencia de contratos, acuerdos de nivel de servicio y/o confidencialidad con empleados o terceros.
Ausencia o insuficiencia de contratos, acuerdos de niveles de servicio y/o confidencialidad.
Ausencia o insuficiencia de control de cambios en la configuración.
Ausencia o insuficiencia de controles de acceso a las instalaciones.
Ausencia o insuficiencia de controles de monitoreo de las instalaciones (por ej. detección o extinción de incendios, líquidos inflamables, CCTV, entre otros).
Ausencia o insuficiencia de copias de respaldo.
Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los empleados y/o terceras partes.
Ausencia o insuficiencia de documentación de uso y/o administración.
Ausencia o insuficiencia de cláusulas contractuales y/o acuerdos de confidencialidad.
Hurto, fraude o sabotaje de equipos, medios, información o documentos.
Ausencia o insuficiencia de mantenimiento.
Ausencia o insuficiencia de mecanismos de identificación y autenticación.
Ausencia o insuficiencia de perfiles de acceso o falta de gestión de privilegios de acceso.
Ausencia o insuficiencia de planes de emergencia y simulacros de evacuación.
Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.
Ausencia o insuficiencia de procedimientos de monitoreo de los recursos de procesamiento de información.
Ausencia o insuficiencia de procedimientos para el manejo información clasificada.
Ausencia o insuficiencia de procesos disciplinarios definidos en el caso de incidente de seguridad de la información.
Ausencia o insuficiencia de pruebas.
Ausencia o insuficiencia de un procedimiento para el manejo de comunicaciones externas.
Ausencia o insuficiencia de un proceso de análisis y tratamiento de riesgos.
Ausencia o insuficiencia de un proceso de gestión de incidentes de seguridad.

CATALOGO DE VULNERABILIDADES
Ausencia o insuficiencia de un proceso para clasificar y etiquetar la información.
Ausencia o insuficiencia en el control de los activos que se encuentran fuera de la instalaciones.
Ausencia o insuficiencia en la definición y formalización de roles, funciones y responsabilidades en la seguridad de la información.
Ausencia o insuficiencia en la gestión de usuarios y contraseñas.
Canales de comunicación sin encriptación.
Capacidad inadecuada.
Conexión deficiente y/o desorganización del cableado estructurado / eléctrico.
Configuración incorrecta de parámetros o configuraciones por defecto.
Dependencia de personal clave, ausentismo y/o personal insuficiente.
Dependencia de proveedores.
Descarga y/o uso no controlado de software.
Desconocimiento, malinterpretación o no cumplimiento de las disposiciones legales, contractuales y/o regulatorias aplicables.
Disposición/reutilización de equipos sin borrado seguro.
Disposición/reutilización de medios de almacenamiento sin borrado seguro.
Documentación insuficiente o desactualizada.
Eliminación de información sin borrado seguro.
Especificaciones o requerimientos incompletos, inadecuados o no claros.
Falla en los servicios esenciales (internet, teléfonos, aire acondicionado, energía, agua, etc).
Falla, daño o degradación de equipos.
Fallas conocidas o defectos del software.
Falta de protección contra virus y/o código malicioso
Falta de segregación de funciones o incorrecta aplicación de las mismas.
Incumplimiento de las condiciones técnicas y/o ambientales provistas por el fabricante.
Incumplimiento de políticas o procedimientos internos.
Insuficiente entrenamiento, capacitación o sensibilización.
Personal inconforme o molesto.
Proveedor o contratista único en el mercado.
Puertos o servicios activos no requeridos.
Punto único de falla.
Relojes no sincronizados.
Transferencia y/o almacenamiento de información en texto claro.
Testeo inadecuado o insuficiente
Ubicación geográfica de las instalaciones en una zona de alto impacto por eventos externos (desastres naturales, orden público, entre otros).

CATALOGO DE VULNERABILIDADES

Uso de Software ilegal / No autorizado / Software Malicioso.

No obstante lo anterior, la metodología aplicada por la Entidad es la tradicional y evidencia el mapa de riesgos publicado en la página web de la entidad, bajo el enlace https://www.ani.gov.co/sites/default/files/u410/matriz_de_riesgos_de_sistemas_de_la_informacion_y_comunicaciones_2018_3.xls, en lo que al proceso de apoyo "Gestión de la información y las comunicaciones" respecta e identifica 7 riesgos a saber:

SIGLA	RIESGO	VALORACIÓN
GIC-1	Desarticulación de la estrategia de la organización y el Plan Estratégico de Tecnología de Información	MODERADO
GIC-2	Incumplimiento normativo asociado a TIC	MODERADO
GIC-3	Indisponibilidad de los servicios tecnológicos	MODERADO
GIC-4	Reducción de recursos presupuestales por inadecuada ejecución presupuestal	BAJO
GIC-5	Incumplimiento del plan de acción de TI	MODERADO
GIC-6	Pérdida de la confidencialidad e integridad de la información	[redacted]
GIC-7	No cumplir con los objetivos de los proyectos TI	ALTO

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

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:

[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.

• 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

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

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

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

En virtud de todo lo anterior el proceso **CUMPLE** con lo dispuesto en la Norma ISO 27001:2013. Se recomienda hacer seguimiento permanente, obedeciendo a la dinámica propia del proceso.

7.4. Revisión de los compromisos de la auditoría de seguridad de la información PEI 124 de abril de 2018.

En la revisión de antecedentes a las auditorías relacionadas con aspectos de seguridad de la información, específicamente, la evaluación integral de hardware, software y seguridad de la información PEI 124,

adelantada por la Oficina de Control Interno en el mes de abril de 2018, se evidenciaron dos no conformidades 42-2018 y 43-2018 que impactan los controles contenidos en el Anexo A de la Norma ISO 27001:2013.

Por lo anterior, en este ejercicio auditor se evaluaron las acciones adoptadas para estas dos no conformidades y la efectividad en la corrección de la causa raíz que les dio origen determinando lo siguiente:

CÓDIGO	AÑO	DESCRIPCIÓN E IDENTIFICACIÓN NO CONFORMIDAD REAL O POTENCIAL.	CONCESIÓN / ÁREA (RESPONSABLE DE LA IMPLEMENTACIÓN)	AUDITOR	FECHA AUDITORÍA (dd/mm/aa)	CUMPLE / %	ACCIÓN
42	2018	3. El centro de datos del piso 2 presenta un daño en el sistema de refrigeración, permitiendo la elevación de la temperatura y el incremento en el riesgo de daño de los equipos core de la LAN. Lo anterior se originó por la carencia de mantenimiento preventivo en los equipos de refrigeración y de respaldo de energía. El mal funcionamiento de este equipo ha obligado a la Administración de la Entidad a dejar la puerta abierta, perdiendo el control de acceso por parte de terceros a un área restringida por la sensibilidad de lo que contiene.	**VAF - Grupo Interno de Trabajo Administrativo y Financiero.** **VPRE- Equipo de Sistemas de información y tecnología**	**JDT**	**Abril 2018**	**SI / 100%**	**Cerrar** **Fue corregida la causa que dio origen a la no conformidad**

CÓDIGO	AÑO	DESCRIPCIÓN E IDENTIFICACIÓN NO CONFORMIDAD REAL O POTENCIAL.	CONCESIÓN / ÁREA (RESPONSABLE DE LA IMPLEMENTACIÓN)	AUDITOR.	FECHA AUDITORÍA (dd/mm/aa)	CUMPLE / %	ACCIÓN
43	2018	4. Actualmente la Entidad no cuenta con mantenimientos contratados ni planes de mantenimiento vigentes para la infraestructura tecnológica para los equipos de cómputo (excluyendo los equipos nuevos que fueron adquiridos con dos mantenimientos al año por tres años), equipos del core de la LAN, equipos de respaldo de refrigeración y energía, entre otros, aumentando el riesgo de daño.	**VAF - Grupo Interno de Trabajo Administrativo y Financiero.** **VPRE- Equipo de Sistemas de información y tecnología**	**JDT**	**Abril 2018**	**SI / 100%**	**Cerrar** **Fue corregida la causa que dio origen a la no conformidad**

8. CALIFICACIÓN DE LA AUDITORÍA Y CONCEPTO DEL AUDITOR

RESULTADO FINAL						
Subcapítulo	DESCRIPTOR	CUMPLIMIENTO			PUNTAJE	OBSERVACIONES
		NO CUMPLE	CUMPLE CON RECOMEN.	CUMPLE		
		0-60%	61%-80%	81%-100%		
7.1.	*Verificación del cumplimiento de los objetivos de control y controles de referencia*		1		1	70,76%
7.2.	*Verificación del cumplimiento de requisitos*	0			0	58,50%
7.3.	*Verificación del proceso de valoración de riesgos de la seguridad de la información*			2	2	85,00%
CUMPLIMIENTO					**71,42%**	**CUMPLE CON RECOMENDACIONES**

Consecuente con la calificación final, el proceso CUMPLE CON RECOMENDACIONES, razón por la cual será necesario atender y solucionar las situaciones descritas en el siguiente capítulo.

9. NO CONFORMIDADES Y RECOMENDACIONES

9.1. Fortalezas

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

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

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

3. El talento humano contratado para la implementación del SGSI es idóneo y ha desarrollado la gestión alineada con lo dispuesto en la Norma ISO 27001:2013.

9.2. No conformidades

El presente ejercicio presenta no conformidades, que obedecen a incumplimientos de los requisitos o de los controles asociados a los objetivos de seguridad que presenta la Norma ISO 27001:2013

1. La Política de Seguridad de la información debe ser aprobada por la alta dirección y actualizada periódicamente; esto se constituye en la evidencia del compromiso de la alta dirección con la adopción de un derrotero que acompañe el cumplimiento de los requisitos y controles contenidos bajo la Norma ISO 27001:2013. Al respecto, se evidenció que la política no ha sido aprobada y supera 3 años desde la la primera versión de un documento que debe ser revisado y actualizado permanentemente con los cambios emanados por las políticas de Gobierno Digital y demás cambios normativos. Lo anterior incumple el requisito 5.1. Liderazgo y compromiso de la Norma.

2. La Política de Seguridad vigente no contempla los lineamientos para el cumplimiento de la totalidad de los requisitos y controles requeridos por la Norma para la implementación del Sistema de Gestión de Seguridad de la Información, incumpliendo el literal c) del requisito 5.2 Política y el literal a) del requisito 5.3. Roles, responsabilidades y autoridades en la Organización.

3. Se evidenció el incumplimiento de los requisitos **8. Operación** al no poder llevar a cabo actividades, tales como, seguimiento al tratamiento de los riesgos o el control operacional y **9. de Evaluación de desempeño** al no poder revisar internamente el SGSI, al no realizar auditorías internas del SGSI, aplicar indicadores y métricas y a partir de ello adoptar acciones correctivas y de mejora.

9.3. Recomendaciones

1. La política de Seguridad Versión 002, pendiente de revisión y aprobación por la alta dirección, no cumple con los controles: transferencia de medios físicos, derechos de acceso y transferencia de información. Lo anterior no cumple con los controles 8. Gestión de activos y 13. Seguridad de las comunicaciones. Se recomienda antes de la liberación de esta nueva versión incorporar lo referente a estas temáticas.

2. 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.

3. Se recomienda realizar unas jornadas para la valoración y tratamiento de los riesgos, en todos los procesos de la Entidad, que incluya la identificación de sus activos de información, su listado de amenazas y vulnerabilidades. Es importante tener presente que los activos de información no reposan únicamente en el área de sistemas, sino que también son importantes los documentos con información sensible, tales como, la información de los procesos judiciales de la entidad, información de contratación, información de seguimiento de los proyectos por mencionar algunas.

4. Es importante que el equipo de apoyo al Sistema de Gestión de Calidad acompañe y practique auditorías internas a los procesos de implementación de otros sistemas de Gestión como el de SGSI y el de SGST, como garante experimentado en la implementación de estos sistemas y en la búsqueda de un Sistema Integrado de Gestión.

Elaborado por:	Juan Diego Toro	Auditor Control Interno	FIRMA:
Apoyo auditor	Sergio Pulido Caycedo	Oficina Control Interno	FIRMA:
Aprobado por:	Gloria Margoth Cabrera Rubio	Jefe Oficina de Control Interno.	FIRMA: