INFORME DE AUDITORÍA INTERNA AL SISTEMA DE GESTIÓN

Fecha de informe: mayo 14 de 2021

Nombre del proceso o dirección territorial auditada: Gestión de la información

Dependencia líder del proceso: Oficina de tecnologías de la información y Red nacional de la información

Servidor responsable del proceso: Víctor Edgardo Duran Martínez - Sandra Del Pilar Ramirez Barrios.

Tipo de auditoría realizada: De primera parte, Sistema de gestión de seguridad de la información ISO 27001:2013.

Fecha de auditoría: mayo 3 de 2021.

Equipo Auditor: Alix Liliana Adame Araque

Jose David Murcia Rodriguez

Juan Manuel Fernández Tinjaca

0. OBJETIVO DE LA AUDITORIA

Verificar el cumplimiento de los requisitos de la norma ISO 27001:2013

1. ALCANCE DE LA AUDITORÍA

Inicia con la reunión de apertura de la auditoría y concluye con el seguimiento a los planes de mejoramiento por parte del auditor.

2. GESTIÓN DEL RIESGO AUDITOR

- Dificultad para acceder a las fuentes de información.
- Imposibilidad de cumplir con el cronograma de auditoría interna planeado en los términos de tiempo y oportunidad establecidos.
- Desechar la pertinencia del informe de auditoría interna que es producto del proceso auditor realizado.
- Alarma en los servidores auditados de la entidad por el desconocimiento del proceso auditor como herramienta gerencial de la Unidad.
- Perdida de información por falta de respaldo de esta.

3. CRITERIOS DE AUDITORÍA

Proceso, procedimientos y demás instrumentos asociados a los sistemas de gestión de la Unidad con relación al sistema de gestión de gestión de seguridad de la Información ISO 27001:2013.

El corte de la auditoria relacionado con la información documentada a auditar es del (01 julio 2020 - a la fecha del año 2021).

4. CONCEPTO DE AUDITORÍA NUMERAL 4 DE LA ISO 27001:2013

El proceso de Gestión de la información desarrolló el contexto estratégico de acuerdo con la metodología para la construcción del contexto que definió la oficina de planeación, dicha actividad se realizó mediante mesas de trabajo el día 20 de marzo del 2020 y de esta reunión quedo un documento con la identificación del análisis de la metodología DOFA referente a los factores internos y externos, como (financieros, comunicación interna, político, ambiental, estratégico, procesos y procedimientos, social y cultural), frente al desarrollo de sistemas de información en los siguientes aspectos:

Revisión de las preguntas del FURAG 2019, información del marco de arquitectura empresarial y el dominio asociado sistemas de información, marco de gobierno y gestión de TI, frente a sistemas de información y su dominio.

Los enlaces del Sistema Integrado enviaron correo electrónico a todo el proceso con las actualizaciones de este documento, y de los resultados de este contexto se tomó como insumo para la construcción de la matriz de riesgos, por tal razón se da como cumplida esta actividad.

Dentro de las necesidades y expectativas de las partes interesadas el proceso cuenta con el formato identificado, actualizado y el proceso de aprobaciónn por parte de la oficina de planeación.

Para este capítulo 4 no se identificaron no conformidades.

5. CONCEPTO DE AUDITORÍA NUMERAL 5 DE LA ISO 27001:2013

Se evidencia el compromiso del proceso en cuanto a la apropiación de la política y los objetivos del sistema de seguridad de la información, el cual se realiza mediante reuniones con el equipo de trabajo para la implementación del Sistema de gestión de seguridad en la información por parte de los líderes del proceso, sin embargo se evidencia que la información del sistema gestión de la información esta publicada en el link de transparencia lo cual hace ver desorden y dificultad para encontrar la política y los objetivos.

Se evidencia el cumplimiento de las necesidades de las partes interesadas a través de reuniones con el equipo de trabajo de cada una de sus actividades internas planeadas, así como el cumplimiento de la política y objetivos de seguridad en la información y el control a ataque cibernéticos de protección de la información referente a la situación actual que se está viviendo de la emergencia sanitaria y el trabajo en casa.

También se tiene definido los roles y responsabilidades en el proceso a través de la matriz interna donde se tienen establecidos cargos y funciones.

De acuerdo con lo informado para este numeral se deja una observación que afecta el numeral 5.2 Política, numeral 5.2.1 Establecimiento de la política de Seguridad de la Información en la mejora del cumplimiento del literal c) de estar disponible para las partes interesadas, según sea apropiado.
Esta observación se debe que la política y los objetivos están publicados, pero no son de fácil acceso y se recomienda que estos se puedan encontrar en la sección de sistema integrado de gestión junto con los otros sistemas en la página web.

6. CONCEPTO DE AUDITORÍA NUMERAL 6 DE LA ISO 27001:2013

De acuerdo con lo auditado al proceso gestión de la información se evidencia que tiene construido el mapa de riesgos de acuerdo con la metodología de administración de riesgos así como la identificación de estos en cada uno de los procesos de la entidad, con el fin de dar cumplimiento a los objetivos teniendo los controles que permiten evitar la materialización de los mismos, esta matriz de riesgos se encuentra formalizado y aprobado por la OAP el día 28 de diciembre de 2020 través de correo electrónico.

Para verificar la efectividad de los controles se indago por el desarrollo de ARCADOC con el fin de comprobar como el proceso ha venido trabajando y que desviaciones se han venido presentando en cada etapa del desarrollo e implementación, ya que a través de este gestor documental y sus avances tanto en la creación como en las pruebas y requerimientos con otras áreas de la entidad con las cuales se debe interactuar y a la espera de que la información se encuentre organizada a través de un código único por expediente.

Teniendo en cuenta esta información no se identifican no conformidades para el capítulo 5.

7. CONCEPTO DE AUDITORÍA NUMERAL 7 DE LA ISO 27001:2013

Se evidencia que el proceso construyo la matriz de roles y responsabilidades donde se definen los cargos, las funciones de los profesionales, la responsabilidad, la autoridad y los controles de acuerdo con la norma ISO 27001 de gestión de seguridad de la información que se encuentran en este proceso para dar cumplimiento a los objetivos del proceso, también se tienen definidas las líneas de trabajo de acuerdo con los equipos de trabajo

internos que se encargan de desarrollar las diferentes actividades del proceso. Este documento se encuentra en formalización, sin embargo, al preguntar al proceso los colaboradores tienen conocimiento de este.

Se evidencia que los colaboradores del proceso son personas idóneas y cuentan con las competencias necesarias para realizar sus respectivos trabajos al interior del proceso.

La comunicación de la información del sistema de seguridad de la información se está realizando a través del correo institucional para los lineamientos desde seguridad en la información, así como las alertas de malware o programas malignos.

En cuanto a la documentación del sistema se evidencia que el proceso ha venido construyendo los documentos exigidos en la norma, pero se evidencio que el documento actual de la identificación de partes interesadas no se encuentra publicado en la página web, por tal razón se deja observación que afecta el numeral 7.5 Información documentada y el numeral 7.5.3 Control de la información documentada, con relación a la mejora del cumplimiento del literal a) de disponibilidad y adecuación para su uso, donde y cuando se necesite.

8. CONCEPTO DE AUDITORÍA NUMERAL 8 DE LA ISO 27001:2013

De acuerdo con lo auditado el proceso gestión de la información ha venido desarrollando los proyectos para la unificación de los sistemas, con el fin de brindar la información clara, exacta, completa y confiable, por tal razón el proceso requiere del trabajo en equipo con otros procesos y operadores, dando cumplimiento al procedimiento desarrollo sistemas de información OBS V2 y al PETI - Transformación Digital V5.

En la auditoria se revisó el procedimiento de “desarrollo sistemas de información Código: 130,06,08-5 versión 2” para el desarrollo de ARCADOC de lo cual se puede identificar que las actividades, responsables y las salidas corresponden a lo documentado en el procedimiento, adicionalmente en el ejercicio de la auditoria se evidencio que los controles descritos están siendo aplicados para evitar desviaciones. También el proceso explico que en el desarrollo de un sistema de información requieren el acompañamiento y la interacción con las diferentes áreas, para lo cual hicieron un cronograma de apropiación con las áreas misionales y administrativas, donde se hicieron mesas de trabajo y pruebas con la Dirección de Registro, Subdirección de Gestión Social y Humanitaria y Gestión documental.

De acuerdo con esta información para este capítulo 8 no se dejan no conformidades.

9. CONCEPTO DE AUDITORÍA NUMERAL 9 DE LA ISO 27001:2013

El proceso de gestión de la información durante la auditoria presenta los informes con el seguimiento de los controles y la información del desempeño del sistema. Los logros de los objetivos planteados son:

- En la revisión de la formulación del PETI a corte del 30 de abril de 2021 los entrevistados informaron los avances de este proyecto para el año 2021, teniendo en cuenta los componentes: Habilitadores, Gobierno Digital, Capacidades de TI (Tecnologías de la Información), para un avance del 63.2 % del 72% que se tiene planeado para este año.

- Consolidación de los reportes que presentan los procesos en cuanto al seguimiento y los controles y el plan de tratamiento que se tienen planteados para los riesgos de seguridad de la información, el proceso informa que a la fecha no se han materializado los riesgos identificados en la Matriz de Riesgos.

- El proceso de gestión de la información tiene definido un cronograma de actividades para la actualización de los activos de información que permiten gestionar, identificar y realizar seguimiento a los riesgos de los activos críticos, también la actualización y socialización de políticas de seguridad de la información clasificadas por componente de aplicación (datos, aplicaciones, infraestructura, factor humano) y la implementación de políticas de seguridad de la información a los procesos.

- Presentación ante el comité institucional de gestión y desempeño de los avances del proceso el día 29 de enero de 2021 en cuanto a: Plan de tratamiento de riesgos de seguridad y privacidad de la información y el Plan de seguridad y privacidad de la información.

Este es un ejercicio de autoevaluación debido a que el proceso tiene por primera vez una auditoría interna para revisar el cumplimiento de los requisitos de los numerales de la norma ISO 27001:2013.

De acuerdo con lo anterior no se dejan no conformidades para este capítulo 9.

10. CONCEPTO DE AUDITORÍA NUMERAL 10 DE LA ISO 27001:2013

El proceso presenta como mejora continua los avances en cuanto a la actualización del PETI y la creación del procedimiento estrategia y gobierno TI, los cuales están orientados a fortalecer las capacidades de arquitectura empresarial de acuerdo con lo establecido en el modelo de gestión y gobierno TI.

El proceso informa que el procedimiento estrategia y gobierno TI está enfocado a la alineación con la estrategia de la Unidad y la mejora de capacidad al hacer sinergia entre procesos.

La actualización del PETI de la vigencia con base al marco estratégico, el plan indicativo, la política de gobierno digital y el PND en el año 2020, logró una madurez del 60% y la meta para el 2021 es del 72% de madurez, información que fue indicada en el momento de la auditoria y la cual presenta como evidencia.

De acuerdo con esta información para este capítulo 10 no se dejan no conformidades.

11. OBSERVACIONES

1. Se observa que dentro del enlace del sistema integrado se encuentra información de todos los sistemas menos del sistema de la información. Esto sucede en el Proceso de Gestión de la Información asociado al sistema de gestión de seguridad de la información. Lo anterior se evidencia al verificar en la página web la política de seguridad, esta no es de fácil acceso, así como los principios de ingeniería de sistemas de seguros clausula A.14.2.5 y la política para proveedores clausula A 15.1.1., sin embargo, el equipo auditado informa que se encuentra aprobada la política por la Resolución 740 de 2014 y se ubicada en el link de transparencia y acceso a la información pública, por tal razón da a entender al equipo auditor que la información está dispersa y no se encuentra fácilmente, por lo cual es importante que esta se integre en un solo lugar. Por lo anterior se deben realizar prácticas de mejora continua para asegurar el cumplimiento del capítulo 5. Liderazgo, numeral 5.2 Política, numeral 5.2.1 Establecimiento de la política de Seguridad de la Información en la mejora del cumplimiento del literal c. Estar disponible para las partes interesadas, según sea apropiado.

2. Se observa que se debe solicitar la actualización del formato de partes interesadas. Esto sucede en el proceso de gestión de la información asociado al sistema de gestión de seguridad de la información. Lo anterior se evidencia al preguntar por el formato de las partes interesadas, donde los auditados presentaron un documento con información actualizada el cual no se encuentra publicado en la página web. Por lo anterior se deben realizar prácticas de mejora continua para asegurar el cumplimiento del capítulo 7. Apoyo, numeral 7.5 Información documentada numeral 7.5.3 Control de la información documentada, mejora del cumplimiento del literal a Su disponibilidad y adecuación para su uso, donde y cuando se necesite.

12. NO-CONFORMIDADES

No se encontraron No Conformidades

13. FORTALEZAS Y DEBILIDADES

1. Se logró el objetivo de esta auditoria el cual era revisar el cumplimiento de los numerales de las normas nombradas y el grado de madurez en el proceso Gestión de la información.

2. Compromiso del proceso de gestión de la información con respecto a la implementación del sistema de los sistemas de gestión.

3. Liderazgo y disposición de los líderes del proceso y compromiso de todo el grupo de trabajo en el desarrollo de actividades implementadas para la creación del sistema de información.

4. Se evidencio eficacia por parte del proceso de gestión de la información para la entrega de las evidencias así mismo la buena disposición, puntualidad y compromiso de los auditados para dar respuesta a las preguntas en el momento de la auditoria.

5. Organización por parte de los enlaces del sistema integrado para el avance y actualización de la documentación correspondiente, así mismo como la socialización de los lineamientos en cuanto al sistema integrado.

6. Se evidencia utilización de herramientas de autocontrol para reportes y seguimientos de las actividades de los diferentes planes del proceso.

7. Se evidencia espacios de reunión de equipo para abordar temas del proceso y seguimiento para la toma de decisiones.

14. RESUMEN ESTADÍSTICO DE AUDITORÍA.

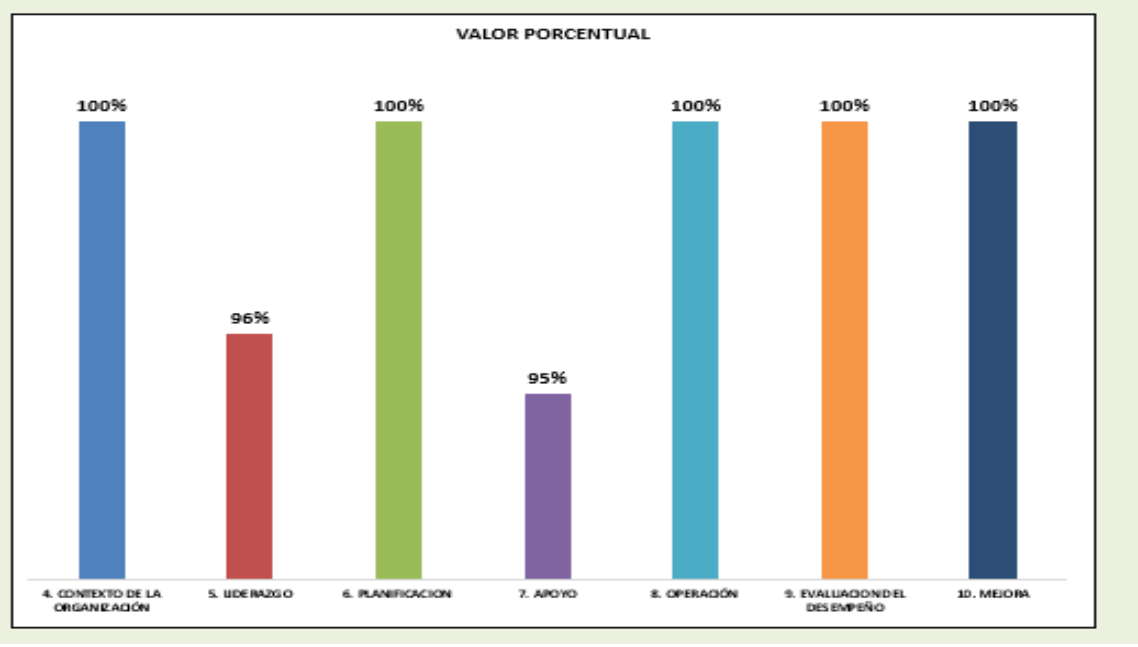
Se presenta el resumen estadístico de la Auditoría Interna del sistema de seguridad de la información al proceso de gestión de la información, la cual presenta un promedio de cumplimiento de los requisitos de la Norma ISO 27001:2013 del 99%, representados así:

Tabla No. 1. Porcentaje por numeral de la Norma ISO 27001:2013

ITEM DE NORMA	VALOR PORCENTUAL	No. NO CONFORMIDADES
4. CONTEXTO DE LA ORGANIZACIÓN	100%	0
5. LIDERAZGO	96%	0
6. PLANIFICACION	100%	0
7. APOYO	95%	0
8. OPERACIÓN	100%	0
9. EVALUACION DEL DESEMPEÑO	100%	0
10. MEJORA	100%	0
TOTAL DE NO COMFORMIDADES	99%	0
	MANTENER	0,00%

Fuente: Herramienta de evaluación auditoría interna de ISO 27001:2013

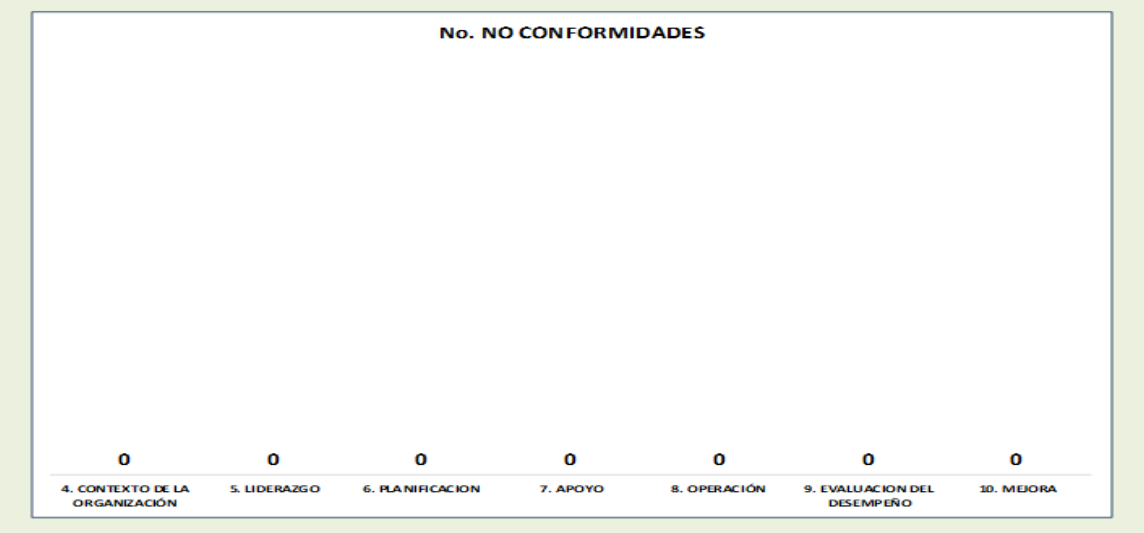
Gráfica No. 1. Porcentaje por numeral de la Norma ISO 27001:2013



Fuente: Herramienta de evaluación auditoría interna de ISO 27001:2013

En cuanto al desempeño del proceso gestión de la información se evidencia que el capítulo 5. Liderazgo tiene un porcentaje de avance del 96 % y el capítulo 7. Apoyo tiene un porcentaje de avance del 95% y los capítulos 4. Contexto de la organización, 6. Planificación, 8. Operación 9. Evaluación del desempeño y 10. Mejora, tiene un porcentaje de avance del 100%.

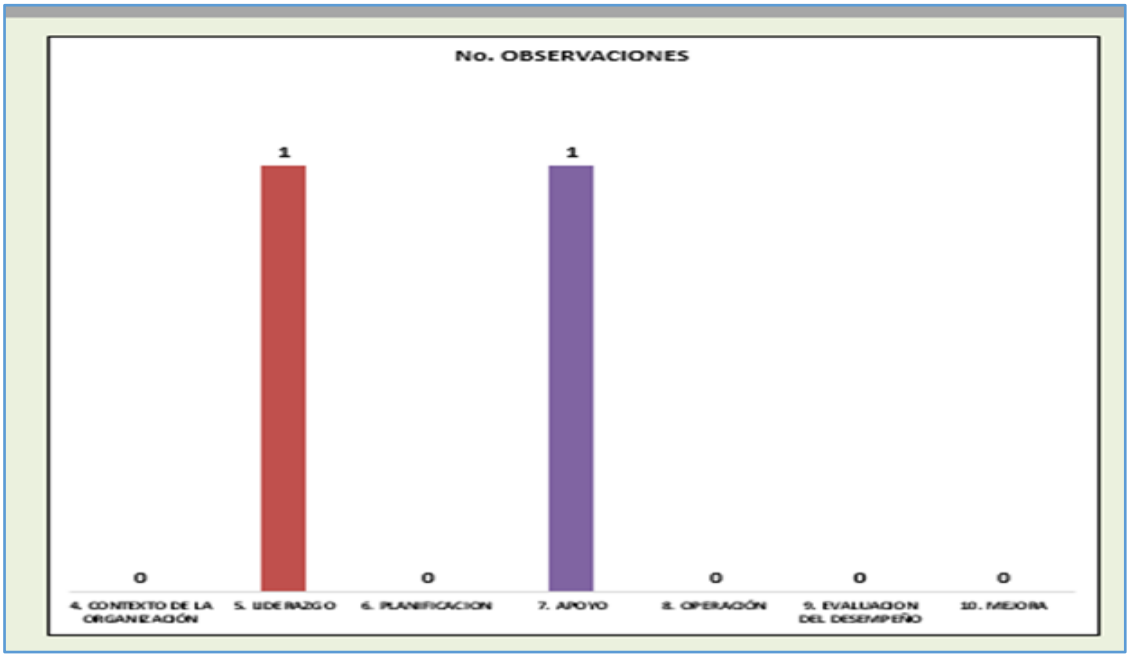
Grafica No. 2. Número de No Conformidades



Fuente: Herramienta de evaluación auditoría interna de ISO 27001:2013

De acuerdo con lo auditado no se presentan No conformidades para el Proceso de Gestión de la Información en cuanto a la implementación de la Norma ISO 27001:2013.

Grafica No. 3. Número de Observaciones



Fuente: Herramienta de evaluación auditoría interna de ISO 27001:2013

Se presentaron dos observaciones una en el capítulo 5. liderazgo y la otra en el capítulo 7. Apoyo, de la Norma ISO 27001:2013.

En conclusión, el nivel de cumplimiento de los requisitos de la Norma ISO 27001: 2013 para el proceso de gestión de la información es del 99%.

Cordialmente;

ALIX LILIANA ADAME ARAQUE
Auditor líder

CARLOS ARTURO ORDOÑEZ CASTRO
Jefe Oficina de Control Interno

Versión	Fecha del cambio	Descripción de la modificación
1	30/05/2014	Creación del formato
2	24/02/2015	Se adicionó el número de auditoria, la definición de cada una de términos, la agenda de la auditoria, informe de la auditoria, conformidad, aspectos positivos, fortalezas, oportunidades de mejora, observaciones, no conformidades, ficha técnica y responsables de la auditoria.
3	6/11/ 2015	Se restructura la presentación de la no conformidad
4	26/07/2017	Se modifica el nombre del formato de acuerdo con el procedimiento.se adiciona firma aprobación del jefe Oficina de Control Interno
5	22/05/2018	Se modifica formato de acuerdo con nuevos lineamientos del jefe de la Oficina de Control Interno, se eliminan cuadros en Excel.
6	05/02/2021	Se modifica el formato en el encabezado, se elimina el texto 9001:2015 de los numerales del 4 al 10 y se deja el texto (Describir la Norma auditada) para que sea diligenciado y se anexa el numeral 13 relacionado con las fortalezas y debilidades de la auditoria.