INFORME DE AUDITORÍA INTERNA AL SISTEMA DE GESTIÓN

Fecha de informe: Septiembre 1 de 2022

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 Martinez - Badir Alberto Ali Badran

Tipo de auditoría realizada: De primera parte, Sistema de Gestión y Seguridad en la información en la norma ISO 27001:2013.

Fecha de auditoría: Agosto 22 de 2022

Equipo Auditor: Alix Liliana Adame Araque - Diana Marcela Pinzón Franco - Marian Angelica Torres Cruz - Daniel Rene Rojas Marroquín

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:

Riesgos de la auditoria (ISO 19011:2018/5.3):

- Recursos (insuficiente tiempo y equipos para desarrollar el programa de auditoría o para realizar una auditoría).
- Canales de comunicación ineficientes por la modalidad remota.
- Falta de control de la información documentada (evidencias y registros).
- Disponibilidad y la cooperación del auditado y la disponibilidad de evidencias a muestrear.

3. CRITERIOS DE AUDITORÍA:

Proceso, procedimientos y demás instrumentos asociados a los sistemas de gestión de la Unidad del Sistema de gestión de seguridad de la Información ISO 27001:2013.

El corte de la auditoria relacionado con la información documentada a auditar es del (1 Julio de 2021 - a la fecha del año 2022).

4. CONCEPTO DE AUDITORÍA NUMERAL 4 DE LA ISO 27001:2013 – CONTEXTO DE LA ORGANIZACION

De acuerdo con la información suministrada por parte del equipo auditado se evidencia que el proceso Gestión de la información realizo la actualización del contexto estratégico el 24 de septiembre de 2021, lo cual se pudo evidenciar mediante acta de reunión.

Por otro lado, se están adelantando actividades de actualización del contexto estratégico con las Direcciones Territoriales y los procesos de la entidad para el año 2022.

El proceso cuenta con el formato actualizado, socializado e interiorizado por parte del proceso de las necesidades y expectativas de las partes interesadas, los requisitos y las interfaces con las entidades. Por tal razón se da como cumplida esta actividad.

Para este capítulo 4., no se identificaron no conformidades relacionados con los requisitos de la norma ISO 27001:2013.

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

Se evidencia el compromiso que tiene el líder del proceso en el mantenimiento del sistema de gestión de la información de acuerdo con lo informado en la auditoria, el proceso presento la Resolución 3157 de 10 de noviembre de 2021 *“por la cual se establecen los objetivos, política general y políticas específicas del sistema de gestión de seguridad de la información en la Unidad para la Atención y Reparación Integral a las Víctimas.”*

Se tiene definido los roles y responsabilidades a través de una matriz interna en el cual están definidos los cargos requeridos para el mantenimiento del sistema.

De acuerdo con lo observado en la auditoria se evidencia que el proceso ha establecidos canales que han permitido socializar la información del sistema de seguridad de la información a través de flash informativos, correos de SUMA, día de la tecnología y charlas de buenas practicas de seguridad y privacidad de la información. Por tal razón se da como cumplida esta actividad.

Para este capítulo 5., no se identificaron no conformidades relacionados con los requisitos de la norma ISO 27001:2013.

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

Se evidencia que el proceso de gestión de la información tiene definido el mapa de riesgos asi mismo el proceso informa que junto con la oficina asesora de planeación desde noviembre del 2021 han venido trabajando con otros procesos en la actualización del mapa de riesgos de acuerdo con la metodología definida por la entidad.

Dentro del plan de tratamiento de riesgos asociado al proceso de gestión de la información se tienen definidas las actividades, riesgos, control, tratamiento y el plan de acción de acuerdo con la metodología de administración del riesgo.

El proceso tiene implementado el seguimiento de los planes de tratamiento al riesgo de seguridad de la información donde se pudo evidenciar los lineamientos correspondientes a la materialización de riesgos de seguridad en la información.

En la auditoria se evidencia que el proceso tiene definido los objetivos y están asociados a los indicadores del plan de acción del año 2022.

Teniendo en cuenta esta información no se identifican no conformidades para el capítulo 6. Planificación: relacionados con los requisitos de la norma ISO 27001:2013.

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

Se evidencia que el proceso cuenta con la matriz de comunicaciones la cual fue explicada por parte del equipo auditado donde se indicó que se comunica, cuando se comunica y a quien se comunica a través de los diferentes medios y canales de comunicación. De igual forma se cuenta con las evidencias de los requisitos y competencias de los profesionales encargados del mantenimiento de gestión de la información.

En la auditoria se evidencio que cuentan con la documentación mínima requerida por la norma ISO 27001:2013.

De acuerdo con lo verificado en la auditoria se deja una observación que afecta el capítulo 7.5.3 Control de la Información documentada, Se observa, en la documentación presentada por el equipo auditado de la aprobación del acta *"contexto institucional DT Chocó del 29 de Julio de 2022"* no contiene la totalidad de las firmas correspondientes a los responsables de la reunión y tampoco se adjunta el listado de asistencia, esto sucede en el proceso de gestión de la información.

Para este capítulo 7. Apoyo, se identificó una observación relacionada con el control de la información documentada, relacionado con los requisitos de la norma ISO 27001:2013.

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

En el ejercicio de la auditoria se revisaron los procedimientos Creación de usuarios en sistemas de la información v1 en el cual se pudo verificar el paso a paso de los requisitos para crear los usuarios y permisos en los aplicativos de la entidad y asi como la desactivación de usuarios cuando estos ya no hacen parte de la entidad Y el procedimiento Instrumentalización de la información V5 en el cual se verifico como se hace la recepción de las bases de datos recibidas a través de articulación interinstitucional y dinamización de la información AIDI y como esta información se dispone para uso o consulta de la organización o de las entidades que conforman el SNARIV.

Se evidencio que el proceso cuenta con la información documentada, para el mantenimiento y mejora continua del sistema de gestión de la información

Para este capítulo 8. Operación no se identificaron no conformidades, relacionado con los requisitos de la norma ISO 27001:2013.

9. CONCEPTO DE AUDITORÍA NUMERAL 9 DE LA ISO 27001:2013 – EVALUACIÓN Y SEGUIMIENTO

El proceso presenta seguimiento a la auditoría interna del año 2021 y el seguimiento del ejercicio de autoevaluación pedagógica el cual fue desarrollado para la preparación de la auditoria de certificación a finales del año 2021, a la fecha de esta auditoria se continúa desarrollando las actividades del plan de mejoramiento.

De acuerdo con la auditoria el proceso presenta el informe de revisión por la dirección de noviembre de 2021 donde se presentan los avances de la implementación de cada uno de los proyectos adelantados por el proceso de gestión de la información, las cuestiones externas e internas identificadas, avance en la implementación de los riesgos y oportunidades, avance de los indicadores de plan de acción y su relación con cada uno de los objetivos del sistema de gestión de la información, formulación de planes de mejoramiento y su respectivo seguimiento.

Teniendo en cuenta esta información no se identifican no conformidades para el capítulo 9. Evaluación y seguimiento; relacionados con los requisitos de la norma ISO 27001:2013.

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

El proceso ha venido realizando la mejora de cada uno de los controles del sistema de gestion de seguridad de la información, este se ve reflejado en la matriz de aplicabilidad, donde su alcance está definido de acuerdo con el proyecto de certificación de la norma ISO 27001:2013, como parte de la mejora continua el proceso tiene proyectado definir un nuevo alcance en el cual se incluyan los otros procesos de la entidad y las direcciones territoriales. Asi mismo el proceso explico el trabajo que se ha venido realizando para incluir dentro del mantenimiento del sistema la gestión de privacidad de la información la cual se encuentra definida en la norma ISO 27701:2020.

Teniendo en cuenta esta información no se identifican no conformidades para el capítulo 10. Mejora; relacionados con los requisitos de la norma ISO 27001:2013.

11. OBSERVACIONES

Sistema de Gestión de Seguridad de la información (Proceso Gestión de la Información - 27001:2013)

1. Se observa, en la documentación presentada por el equipo auditado de la aprobación del acta "contexto institucional DT Chocó del 29 de Julio de 2022" no contiene la totalidad de las firmas correspondientes a los responsables de la reunión y tampoco se adjunta el listado de asistencia, esto sucede en el proceso de gestión de la información, lo anterior se evidencia a través de la entrevista realizada al proceso en el ejercicio de la auditoria. Por lo anterior se deben realizar prácticas de mejora continua para asegurar el cumplimiento de los requisitos de la norma ISO 27001:2013, capitulo 7. Apoyo, numeral 7.5.3. Control de la Información documentada.

12. NO-CONFORMIDADES

En el desarrollo de la auditoria no se identificaron no conformidades, relacionado con los capítulos generales de la norma ISO 27001:2013.

13. FORTALEZAS Y DEBILIDADES

13.1 Fortalezas

- Se evidencia en la auditoria el liderazgo por parte los directivos y lideres de cada uno de los equipos de trabajo.

- Compromiso por parte del proceso de gestión de la información, en la implementación y mejora continua del sistema de gestión de la información, bajo los requisitos de la norma ISO 27001:2013 en cada uno de sus numerales auditados.

- Disposición de los lideres y equipo de trabajo en la ejecución y la buena actitud en el desarrollo de la auditoria.

- Compromiso del enlace del SIG, respecto al registro de la evidencia en la plataforma OneDrive.

- Organización de la información para atender la auditoria.

- Cumplimiento por parte del equipo auditado en el cronograma establecido para el programa de auditoría.

- Se evidencia un trabajo de equipo para lograr una mejora continua en el mantenimiento de los procesos, acciones y planes asociados al sistema de gestión de la información.

- Se observa compromiso previo por parte del equipo de trabajo en la gestión y verificación de numerales de acuerdo con sus debilidades, oportunidades de mejora y el ejercicio de autoevaluación realizado el año anterior.

13.2 Debilidades

- Continuar con la cultura del conocimiento difundiendo los temas relevantes del SIG, para dar cumplimiento a los requisitos mínimos requeridos en la documentación.

14. RESUMEN ESTADÍSTICO DE AUDITORÍA

PROCESO DE GESTIÓN DE LA INFORMACIÓN

A continuación, se identifican los resultados de los datos estadísticos generados en la herramienta papel de trabajo de la auditoría interna de seguridad de la información ISO 27001:2013 del proceso de gestión de la información.

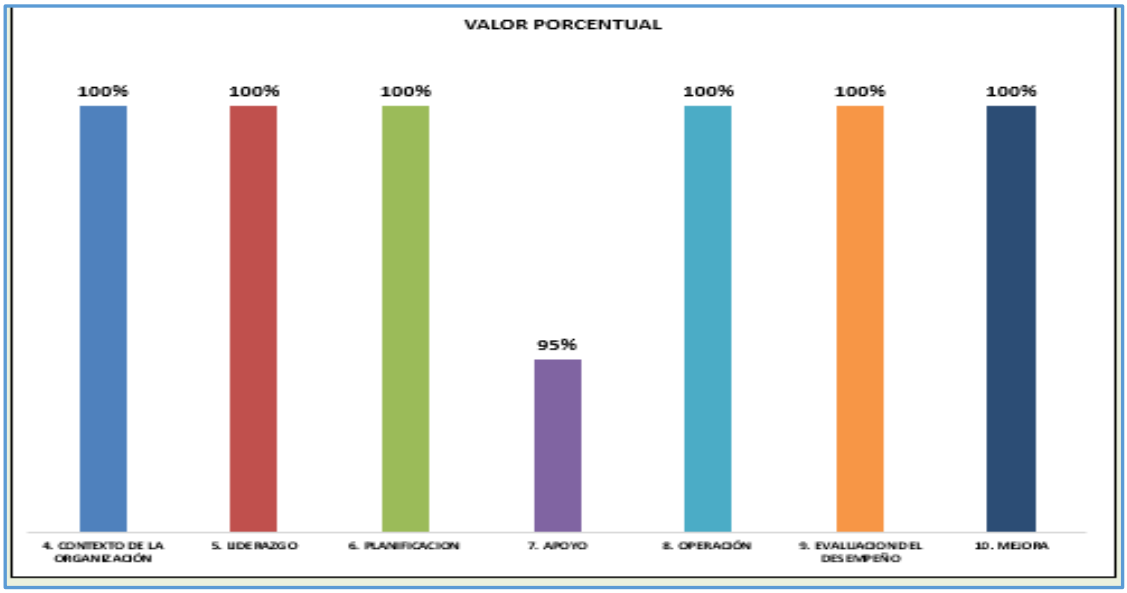
a) Numeral de porcentajes

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

ITEM DE NORMA	VALOR PORCENTUAL
4. CONTEXTO DE LA ORGANIZACIÓN	100%
5. LIDERAZGO	100%
6. PLANIFICACION	100%
7. APOYO	95%
8. OPERACIÓN	100%
9. EVALUACION DEL DESEMPEÑO	100%
10. MEJORA	100%

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

El porcentaje promedio de cumplimiento del nivel de madurez asociado a los requisitos del Sistema de gestión de seguridad de la información NTC ISO 27001:2013 a los capítulos generales, es del 99%.

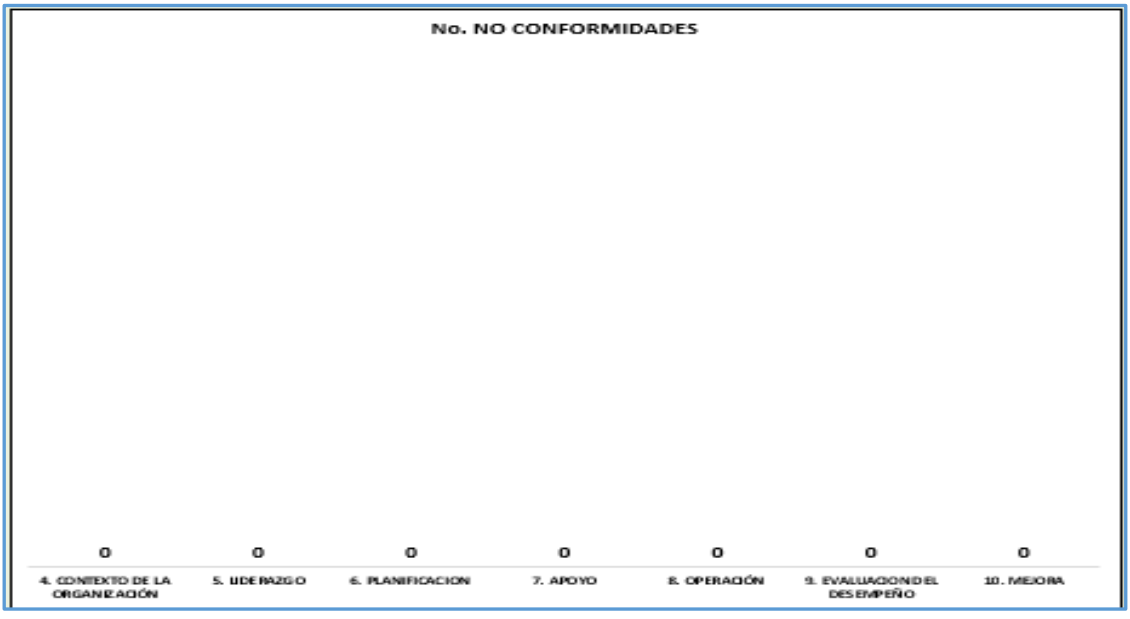
b) Numero de no conformidades y observaciones

Tabla No. 2 Número de NC y Observaciones

ITEM DE NORMA	No. NO CONFORMIDADES	No. OBSERVACIONES
4. CONTEXTO DE LA ORGANIZACIÓN	0	0
5. LIDERAZGO	0	0
6. PLANIFICACION	0	0
7. APOYO	0	1
8. OPERACIÓN	0	0
9. EVALUACION DEL DESEMPEÑO	0	0
10. MEJORA	0	0

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

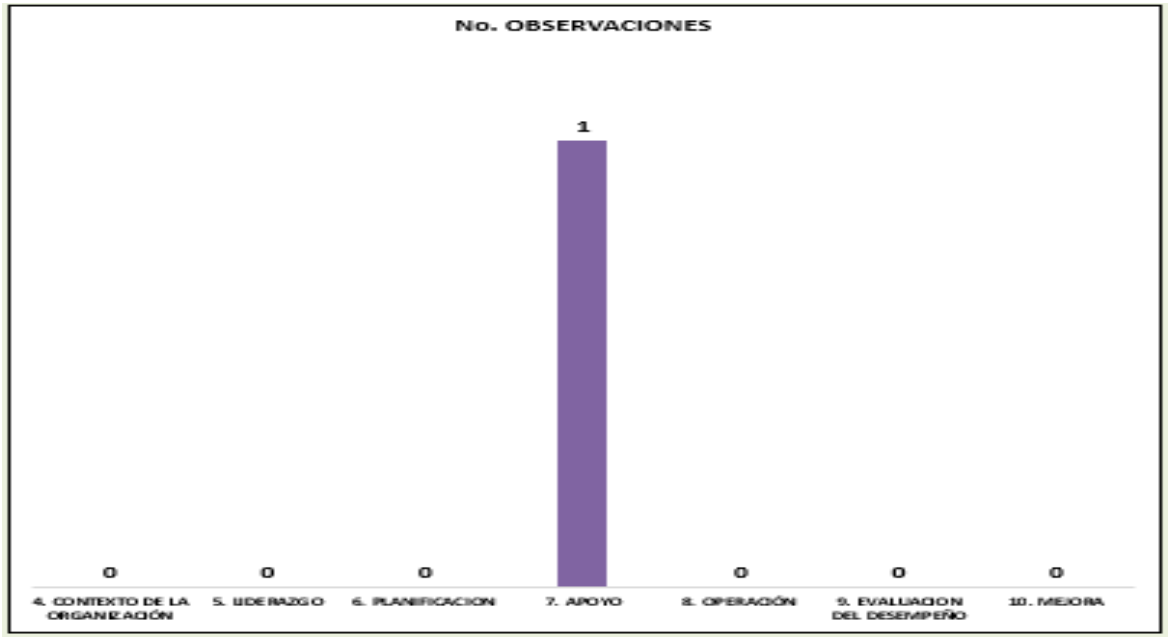
Grafica No. 2. Número de No Conformidades



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

Se identificaron cero (0) no conformidades en los capítulos 4, 5, 6, 7, 8, 9, 10; respecto al cumplimiento del nivel de madurez asociado a los requisitos generales del sistema de gestión de seguridad de la información NTC ISO 27001:2013, logrando un 100%.

Grafica No. 3. Número de Observaciones



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

Se presento una (1) observación en el capítulo 7. Apoyo, 7.5.3. Control de la Información documentada; respecto a la aplicación de la herramienta de evaluación de cumplimiento del nivel de madurez asociado a los requisitos generales del sistema de gestión de seguridad de la información NTC ISO 27001:2013.

En conclusión, el nivel de cumplimiento de los requisitos generales de la Norma ISO 27001:2013 del sistema de gestión de seguridad de la información del 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 auditoría, 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.