CORMAGDALENA

La energía de un río que impulsa a un país

CORPORACIÓN AUTÓNOMA REGIONAL DEL RÍO MAGDALENA

INFORME ESTADO ACTUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Marzo 2024

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCION

Cada día son más las amenazas y variantes de ataques informáticos o cibernéticos que pueden poner en riesgo los activos de información de una organización, así como a los sistemas utilizados para su tratamiento. Este contexto prácticamente obliga a las entidades a contar con una estrategia o sistema que les permita gestionar estos riesgos de una forma estructurada, para garantizar que se están protegiendo correctamente los activos de información de la organización.

El Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procedimientos y prácticas de administración de la información, basadas en la norma ISO/IEC 27001:2013 y tiene el objetivo asegurar que las organizaciones cuenten con la implementación de todos los controles convenientes para garantizar el nivel apropiado de protección sobre los activos de información, teniendo en cuenta los tres pilares fundamentales: la confidencialidad, la integridad y la disponibilidad.

El cumplimiento de la norma ISO 27001:2013 puede ayudar a las entidades a demostrar a sus partes interesadas, la seriedad con la que se abordan los temas relacionados con la seguridad de la información. La adopción del Sistema de Gestión de Seguridad de la Información (SGSI) garantiza el tratamiento de los problemas de seguridad de la información según las mejores prácticas actualmente aceptadas.

No contar con la operación de un SGSI aumenta el riesgo de que se presenten incidentes de seguridad que puedan tener las siguientes consecuencias:

- Posibles pérdidas financieras
- Reducción de productividad
- Daños a la reputación de la organización
- Pérdida de oportunidad y competitividad en mercado
- Penalizaciones económicas por incumplimiento de legislación vigente, entre otros.

La implantación de un SGSI, al igual que ocurre con otros sistemas de gestión como el de calidad, es una decisión estratégica para la entidad y siempre estará apoyado por un

proceso continuo de gestión de riesgos para asegurar el tratamiento adecuado de los riesgos identificados y deberá estar integrado con el resto de los procesos de la entidad para ayudar a la consecución de objetivos del negocio.

Este documento de informe básicamente consiste en la presentación de los resultados del análisis de brecha (diagnóstico de estado actual), entre las actividades de gestión de la seguridad de la información hoy en día versus las mejores prácticas de la industria, sumado a lo que dictan las normativas y regulaciones del estado colombiano sobre el tema para las entidades gubernamentales.

La seguridad de la información no es un producto sino más bien un proceso continuo que debe adoptarse dentro de la entidad para garantizar la confidencialidad, la integridad y la disponibilidad de la información. La información es uno de los activos más importantes para poder cumplir con la misión organizacional.

2. CONTEXTO DENTRO DEL EJERCICIO GAP

La Corporación Autónoma Regional del Río Grande de la Magdalena - CORMAGDALENA en desarrollo de los procesos misionales y en cumplimiento del marco normativo y regulatorio aplicable, especialmente a lo relacionado con la estrategia de Gobierno Digital, establecida en el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital, el cual en uno de sus habilitadores transversales, establece como criterio la adopción e implementación de la norma NTC ISO/IEC 27001:2013, y las guías del componente para el uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información. Por lo anterior se ha emprendido un ejercicio de diagnóstico, diseño e implantación del Sistema de Gestión de Seguridad de la Información (SGSI) para la entidad; en el marco de los requisitos de la norma NTC ISO/IEC 27001:2013 y los lineamientos del manual de Gobierno Digital.

La entidad se ha comprometido a proteger sus activos de información teniendo en cuenta la importancia que ellos tienen para el desarrollo de su misión. Para esto ha decido contar con un Sistema de Gestión de Seguridad de la Información, el cual, basado en el modelo de Planear, Hacer, Verificar y Actuar (PHVA), propone un proceso continuo, sistemático, reproducible y medible en donde las diferentes amenazas van siendo mitigadas por la implementación de los respectivos controles con base en lo definido en el Anexo A de la NTC ISO/IEC 27001:2013 y mejores prácticas de la industria.

El primer paso para lograr este cometido es el diagnóstico del análisis de brecha (GAP); por tanto, este documento presenta los resultados de la evaluación de implementación y cumplimiento de las cláusulas, controles y objetivos de control en los catorce (14) dominios descritos en la norma.

Cada análisis debe ir acompañado de un plan de acción que sugiere las acciones a implementar frente a cada hallazgo. La seguridad de la información no es un producto, es un proceso continuo que debe integrarse dentro de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información.

La información es uno de los activos más importantes para poder cumplir con la misión organizacional, de ahí la importancia de dar a conocer a la entidad su estado real frente a lo requerido normativamente.

De otra parte, Cormagdalena como ente corporativo especial del orden nacional, con la implementación de un SGSI, daría también acatamiento y cumplimiento a los lineamientos generados por el Ministerio de Tecnologías de la Información y las comunicaciones “MinTic” dentro del marco de la Estrategia de Gobierno Digital, específicamente en uno de sus habilitadores transversales; “Seguridad de la información: busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información -MSPI, que contempla 6 niveles de madurez”.

3. OBJETIVOS

1.1 Objetivo General

Presentar los resultados del ejercicio de GAP Análysis - Análisis de Brecha (diagnóstico de estado actual) con respecto a los requisitos de la norma NTC ISO/IEC 27001:2013, con el fin de comprender el estado real de la gestión de la seguridad de la información al interior de la entidad.

1.2 Objetivos Específicos

- Analizar las prácticas utilizadas actualmente por la entidad en comparación con las mejores prácticas existentes en la industria para la gestión de la seguridad de la información.
- Evaluar el grado de implementación y cumplimiento de las cláusulas descritas en la norma NTC ISO/IEC 27001:2013.
- Suministrar información para la implementación del Sistema de Gestión de la Seguridad de la Información o SGSI.
- Recomendar un plan de acción de alto nivel para los hallazgos encontrados referente a los requisitos de la norma NTC ISO/IEC 27001:2013.

4. ALCANCE

Realizar el GAP Analysis (determinar el estado actual de la gestión de la seguridad de la información), basado en los requisitos de la norma NTC ISO/IEC 27001:2013.

Va desde la evaluación y cuantificación a alto nivel del grado de implementación y cumplimiento de las cláusulas, hasta el establecimiento del nivel de definición y el porcentaje de implementación.

5. TERMINOS Y DEFINICIONES

- **Actividades críticas:** Operaciones críticas y/o actividades que soportan los objetivos de la entidad.
- **Activo**: Cualquier cosa que tenga valor para la organización.
- **Activos de información:** Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio, servicio y soporte.
- **Análisis de riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.
- **BCP**: Por sus siglas en inglés (Business Continuity Planning) el plan de continuidad del negocio es un proceso de desarrollo y documentación de procedimientos que permiten a una organización responder ante eventos que interrumpan las actividades de los procesos críticos.
- **BIA**: (Business Impact Analysis) Proceso diseñado para priorizar las actividades críticas del negocio evaluando el impacto potencial principalmente de manera cuantitativa.
- **Confidencialidad**: Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Consultor**: Persona idónea en capacidad de prestar servicios de asesoría, diseño, y creación de propiedad intelectual.
- **Contratistas**: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.
- **Control**: Define la declaración específica del control para satisfacer el objetivo del control.
- **Criterio**: Regla o norma conforme a la cual se establece un juicio o se toma una determinación.
- **Custodio**: Encargado de proteger la información por delegación del propietario. Generalmente este rol es ejecutado por el Área IT.

- **Declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la entidad.

- **Desastre**: Evento que causa grandes daños o pérdidas. En el ambiente del negocio, es un evento que crea incapacidad en la organización sobre la ejecución de las actividades críticas del negocio por un periodo de tiempo.

- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- **DRP (PRD):** Por sus siglas en inglés (Disaster Recovery Planning). Es un documento en que definen los recursos, acciones, tareas y datos requeridos para gestionar el esfuerzo de recuperación de los sistemas de información y tecnología en general ante un evento catastrófico.

- **Estado de Implementación:** Nivel de implementación de los controles.

- **Gap Analysis** (del inglés, **análisis** de brecha) es un servicio que permite identificar la distancia existente entre la organización actual de la seguridad de la información en la empresa y las buenas prácticas más reconocidas en la industria.

- **Falla**: Daño o afectación de un dispositivo por un periodo determinado.

- **Incidente**: Un evento o una serie de eventos no deseados o inesperados que tienen una posibilidad significativa de comprometer las operaciones del servicio y amenazar la continuidad del Sistema.

- **Información**: Entendemos por INFORMACIÓN cualquier manifestación (ya sea visual, auditiva, escrita, electrónica, óptica, magnética, táctil...) de un conjunto de conocimientos.

- **Integridad**: Propiedad de salvaguardar la exactitud y estado completo de los activos.

- **Objetivo de control:** establece lo que se va a lograr.

- **Plan de contingencia:** Un plan específicamente de respuesta a un evento que es posible, pero es incierta su ocurrencia.

- **Procedimientos:** Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

- **Propietario**: Es el responsable y dueño del activo de información. Define también sus niveles de clasificación.

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

- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **Terceros**: Entendemos por terceros a proveedores, contratistas, clientes y visitantes al Sistema.
- **Usuario**: Es el que utiliza los activos de información para llevar a cabo las funciones de su trabajo.

6. MARCO TEORICO

El cuidado de la información debe tener una importancia fundamental para el funcionamiento e inclusive para que la entidad logre en el corto, mediano y largo plazo la consecución de su misión y además garantiza su supervivencia en un entorno cada vez más dinámico y lleno de riesgos.

El hecho de disponer de una serie de controles para mitigar el riesgo según la norma NTC/ISO 27001:2013 ayuda a gestionar y proteger los activos de información; activos indispensables para la operación y correcto funcionamiento de los procesos de la entidad.

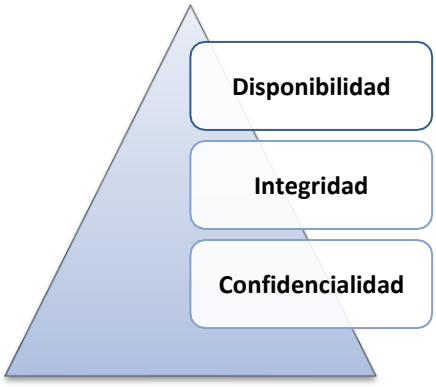

Ilustración 1. Objetivos de la seguridad de la información.

El marco teórico propio de este documento está estrechamente relacionado con la norma NTC/ISO 27001:2013. Esta norma ha sido concebida para ofrecer un modelo basado en el ciclo PHVA (planear, hacer, verificar y actuar) para el establecimiento, implementación, operación, seguimiento, revisión y mejora de un Sistema de Gestión de la Seguridad de la

Información (SGSI). La adopción de este tipo de sistemas debe ser una decisión estratégica para Cormagdalena.

El diseño y la posterior implementación del SGSI en una entidad deben estar basados en necesidades, objetivos, requisitos de seguridad, procesos, empleados, tamaño y estructura de esta. La protección de los activos de información debe ser parte fundamental de la estrategia de la entidad al abordar la implementación de un SGSI. La seguridad de la información según la norma NTC/ISO 27001:2013 consiste en preservar la confidencialidad, integridad y disponibilidad de la información. Por tanto, la entidad debe identificar y estimar los activos de información en relación con esta triada según sus necesidades.

Cormagdalena es ente corporativo especial del orden nacional por tanto está obligada a dar cumplimiento a los lineamientos generados por el Ministerio de Tecnologías de la Información y las comunicaciones “MinTic” dentro del marco de la Estrategia de Gobierno Digital, establecida en el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones 1008 de 2018.

7. METODOLOGIA UTILIZADA

El análisis GAP (*GAP Analysis* por sus siglas en inglés) o análisis de brechas es una herramienta de estudio para comparar el estado y desempeño real de una organización o entidad, en un momento determinado, respecto a uno o más puntos de referencia seleccionados de orden normativo, local, regional, nacional y/o internacional.

Ilustración 2. Metodología utilizada

En efecto, el presente análisis GAP se realizó a fin de determinar el estado actual de la gestión de la seguridad de la información en la Corporación Autónoma Regional del Río Grande de la Magdalena - CORMAGDALENA con relación a los requisitos de la norma NTC/ISO 27001:2013, la cual se considera como el punto de arranque de la definición de una estrategia de la arquitectura de seguridad de la información, perfectamente alineada con la visión de la entidad, dentro de su entorno de operación.

Para ello, se inició con la definición del alcance, luego se planearon y se ejecutaron las entrevistas, inspecciones en sitio y revisiones documentales a los responsables asignados por la entidad, con el fin de verificar el cumplimiento para cada una de las cláusulas establecidos por la norma NTC/ISO 27001:2013. La información se consolidó en una matriz en la que luego se dio la calificación objetiva a cada una de las cláusulas evaluadas aplicando los niveles de calificación establecidos.

Finalmente, se identificaron y documentaron los respectivos hallazgos, describiendo un plan de acción para cada una de las cláusulas y dominios evaluados, consolidando los resultados en el presente informe, acompañado de recomendaciones para mejorar el nivel actual de la seguridad de la información en la entidad.

7.1 Niveles y criterios de calificación

A continuación, se detallan los niveles y criterios de calificación:

NIVEL	PORCENTAJE	CRITERIOS
Inexistente	0%	La organización o entidad ha identificado una situación que debe ser tratada.
		Carencia total de procesos relacionados con el SGSI.
Planeado	1 - 25 %	Se ha identificado la necesidad de implementar acciones y se evidencia una planeación para tratarla.
		No se cuenta con un procedimiento y/o política documentada, pero se ejecutan algunas acciones que dan cumplimiento parcial a los controles.

Inicial	26 - 50 %	Se cuenta con un procedimiento y/o política documentada pero no se ejecutan las actividades, acciones o lineamientos descritos en estos documentos.
		Se realizan acciones o actividades que dan cumplimiento parcial a los controles, pero no se evidencian registros.
Definido	51 - 75 %	Se cuenta con un procedimiento y/o política documentada y se ejecutan las actividades, acciones o lineamientos descritos en estos documentos.
		Se ejecutan acciones o actividades que dan cumplimiento a todos o la mayoría de los controles, y se evidencian registros.
Medible	76 % - 100 %	Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua.
		Las acciones o controles organizaciones implementados pueden ser evaluados por medio de métricas definidas

Tabla 1. Niveles y criterios de calificación

EL propósito al final del ejercicio es enmarcar el nivel del grado de implementación y cumplimiento de la entidad (estado real) frente a los requisitos requeridos por la norma (estado ideal) para la implementación y conformidad de un Sistema de Gestión de Seguridad de la Información:

- **Estado Real:** Porcentaje y nivel de cumplimiento con las condiciones actuales de la entidad.
- **Estado Ideal:** Para efectos de esta metodología, el estado ideal estará enmarcado en un 70%, es decir, en un nivel **Definido**, siguiendo las mejores prácticas existentes en entidades de tamaño y naturaleza similar a Cormagdalena.
- **Meta:** 100% de establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información frente a lo requerido por norma.

8. GRADO DE IMPLEMENTACION Y CUMPLIMIENTO DE LAS CLAUSULAS

Los requisitos establecidos en la norma NTC/ISO 27001:2013 son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Considerando que la Corporación Autónoma Regional del Río Grande de la Magdalena - CORMAGDALENA declara conformidad con esta norma, la evaluación y análisis de brechas se hizo frente a cada requisito especificado en los numerales 4 al 10, puesto que no es aceptable excluir ninguno de ellos.

A continuación, se presenta gráficamente la brecha existente entre las prácticas de seguridad actuales de la entidad y las mejores prácticas existentes en la industria.

Analizando el grafico, se evidencia que todas las cláusulas presentan un estado de cumplimiento por debajo del estado ideal, lo que indica que requiere una intervención

inmediata sí el objetivo es la implementación del SGSI.

En seguida, se presenta el grado actual de implementación y cumplimiento de la entidad frente a las cláusulas.

NUMERAL	CLAUSULA	ESTADO REAL	ESTADO IDEAL	META	NIVEL
4	CONTEXTO DE LA ORGANIZACIÓN	15%	70%	100%	*Planeado*
5	LIDERAZGO	15%	70%	100%	*Planeado*
6	PLANIFICACIÓN	20%	70%	100%	*Planeado*
7	SOPORTE	15%	70%	100%	*Planeado*
8	OPERACIÓN	10%	70%	100%	*Planeado*
9	EVALUACIÓN DEL DESEMPEÑO	15%	70%	100%	*Planeado*
10	MEJORA	10%	70%	100%	*Planeado*
Grado actual de implementación y cumplimiento frente a las clausulas		**14%**			***Planeado***

Ilustración 3. Grado actual de implementación y cumplimiento frente a las clausulas

En promedio, la entidad presenta un estado real de cumplimiento del 14%, en un nivel **Planeado**, es decir, ha identificado la necesidad de implementar acciones y se evidencia una planeación para tratar dicha necesidad.

9. HALLAZGOS Y PLAN DE ACCION DETALLADOS POR CLAUSULAS

9.1 Contexto de la organización

NUMERAL	CLAUSULA	ESTADO REAL	NIVEL	HALLAZGO	PLAN DE ACCIÓN
4	**CONTEXTO DE LA ORGANIZACIÓN**	15%	*Planeado*	La entidad no ha determinado el contexto externo e interno que es pertinente para un SGSI.	Se debe identificar y documentar los problemas Internos y externos de la entidad, las fortalezas, las cuestiones legales, de mercado, social y económica, entre otras, que puedan afectar o impactar la seguridad de la información.
				La entidad no ha determinado las necesidades y expectativas de las partes interesadas.	Se debe identificar y documentar las necesidades y expectativas de las partes interesadas.
				La entidad no ha determinado el alcance del SGSI, las interfaces y sus dependencias.	Se debe determinar y documentar los límites y la aplicabilidad (alcance) del SGSI.

9.2 Liderazgo

NUMERAL	CLAUSULA	ESTADO REAL	NIVEL	HALLAZGO	PLAN DE ACCIÓN
5	**LIDERAZGO**	15%	*Planeado*	La entidad no ha establecido y documentado como va a demostrar el liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información	Se debe establecer una política de seguridad de la información que sea adecuada al propósito de la entidad, a los objetivos y requisitos aplicables y que sea aprobada por la alta dirección.

			NIVEL	HALLAZGO	PLAN DE ACCIÓN
				No se evidencia la definición de roles y responsabilidades de seguridad de la información.	Dar el formalismo dentro de una resolución y asignar roles y responsabilidades que aseguren la conformidad del SGSI y que informe a la alta dirección sobre el desempeño del SGSI. Se debe crear dentro del mapa de procesos de la entidad, un proceso estratégico que corresponda a las Gestión de la Seguridad de la Información

9.3 Planificación

NUMERAL	CLAUSULA	ESTADO REAL	NIVEL	HALLAZGO	PLAN DE ACCIÓN
6	**PLANIFICACIÓN**	20%	*Planeado*	La entidad no ha aplicado un proceso para el análisis, valoración y tratamiento de los riesgos.	Se debe crear un proceso o procedimiento, que aplique una metodología de valoración y tratamiento de riesgos y formular un plan de tratamiento de riesgos.
				La entidad no ha generado una declaración de aplicabilidad que contenga los controles necesarios y la justificación de las exclusiones de los controles del Anexo A.	Se debe producir una declaración de aplicabilidad que sea aprobada por la alta dirección.
				La entidad no ha definido los objetivos de seguridad de la información.	Se debe establecer los objetivos de seguridad de la información que sean coherentes con la política de seguridad de la información y que tengan en cuenta los resultados de la valoración y tratamiento de riesgos.

9.4 Soporte

NUMERAL	CLAUSULA	ESTADO REAL	NIVEL	HALLAZGO	PLAN DE ACCIÓN
7	**SOPORTE**	15%	*Planeado*	La entidad no ha determinado los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.	Se debe revisar los perfiles e incluir componentes de educación, formación y experiencia en seguridad de la información en todos los perfiles que interactúen con la misma.
				El procedimiento de la entidad para la administración y control de la documentación no contempla todos los componentes de seguridad de la información.	Se debe alinear el procedimiento de administración y control de la documentación a lo requerido por la norma en cuanto a seguridad de la información.

9.5 Operación

NUMERAL	CLAUSULA	ESTADO REAL	NIVEL	HALLAZGO	PLAN DE ACCIÓN
8	**OPERACIÓN**	10%	*Planeado*	La entidad no ha realizado valoraciones de riesgo a intervalos planificados, así tampoco ha implementado un plan de tratamiento de riesgos.	Se debe aplicar una metodología de valoración y tratamiento de riesgos, hacer seguimiento y revisión por periodos planificados y los hallazgos no conformes tratarlos con planes de remediación.

9.6 Evaluación del desempeño

NUMERAL	CLAUSULA	ESTADO REAL	NIVEL	HALLAZGO	PLAN DE ACCIÓN
9	**EVALUACIÓN DEL DESEMPEÑO**	15%	*Planeado*	La entidad no ha implementado una medición para evaluar el desempeño de la seguridad de la información y la eficacia del SGSI.	Se debe establecer indicadores de seguimiento, medición y análisis para evaluar el desempeño y eficacia del SGSI.
				La entidad no ha planificado, establecido, implementado y mantenido programas de auditoria para evaluar la conformidad del SGSI.	Se debe establecer un procedimiento de auditorías internas para proporcionar información acerca de la conformidad del SGSI.
				La entidad no ha definido los intervalos para la revisión por la alta dirección.	Se debe planificar las revisiones por la alta dirección contemplando cada uno de los requisitos de la norma y dejar evidencia de la ejecución de dichas revisiones, determinando el nivel de eficacia del SGSI.

9.7 Mejora

NUMERAL	CLAUSULA	ESTADO REAL	NIVEL	HALLAZGO	PLAN DE ACCIÓN
10	**MEJORA**	10%	*Planeado*	La entidad al no contar con la operación de un SGSI no ha identificado no conformidades o acciones correctivas relacionadas con seguridad de la información, por tanto, no mantiene evidencia de sus resultados.	Formular un procedimiento de tratamiento de las no conformidades y acciones correctivas aplicable a la seguridad de la información, a fin de llevar a la entidad a mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

10. CONCLUSIONES

Una vez finalizado el análisis GAP (análisis de brecha) o diagnóstico y haciendo un comparativo entre la realidad de la Corporación Autónoma Regional del Río Grande de la Magdalena - CORMAGDALENA frente a la norma NTC/ISO 27001:2013, se evidenciaron hallazgos que afectan el cumplimiento de los requisitos básicos de la norma. Teniendo en cuenta la relevancia para un Sistema de Gestión en Seguridad de la Información, se considera importante resaltar lo siguiente:

- Queda en evidencia la ausencia del Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad, dado que las cláusulas o requisitos establecidos por la norma NTC/ISO 27001:2013, no se están cubriendo o presentan un nivel inexistente de implementación.
- La entidad presenta un estado real de cumplimiento del 14%, en un nivel **Planeado**, lo que implica la necesidad de implementar acciones inmediatas, aunque se evidencia una planeación para tratar dicha necesidad.
- Es necesario que la entidad emprenda un proyecto para el establecimiento e implementación del SGSI.
- La adopción de un Sistema de Gestión en Seguridad de la Información debe ser una decisión estratégica, por tanto, por lo que se debe demostrar el interés, aprobación y revisión de la alta dirección.
- La entidad debe asignar personal altamente capacitado y especializado a las funciones de implementación, operación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la información (SGSI), que contribuya al proceso de alineación con la NTC/ISO 27001:2013 dar alineación y cumplimiento con las regulaciones y normatividad aplicable.

11. BIBLIOGRAFIA

Filter, F. A. (25 de 01 de 2015). *El portal de ISO 27001 en Español*. Obtenido de Implantación del SGSI: http://www.iso27000.es/sgsi.html#home

ICONTEC. (2009). *NTC ISO 27005:2009.* Bogota: ICONTEC.

ICONTEC. (2013). *NTC ISO 27001:2013.* Bogota: ICONTEC.

ICONTEC. (2013). *NTC ISO 27002:2013.* Bogota: ICONTEC.

https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/
Ministerio de Tecnologías de la Información y las Comunicaciones .

Elaboró: Ingenieros TIC- Secretaría General .