CORMAGDALENA

La energía de un río que impulsa a un país

CORPORACIÓN AUTÓNOMA REGIONAL DEL RÍO MAGDALENA

ESTRATEGIA DE ADOPCION DE LA NORMA ISO/IEC 27001:2013 (SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION)

Enero 2024

TABLA DE CONTENIDO

1. INTRODUCCION

Como parte de la iniciativa de la Corporación Autónoma Regional del Río Grande de la Magdalena - CORMAGDALENA, de abordar de manera integral y sistemática las mejores prácticas de seguridad de la información y de dar cumplimiento al marco normativo y regulatorio aplicable, se encuentra adelantando una iniciativa de asesoría en este aspecto, tendiente en primera instancia en definir cuál es a la fecha el estado actual y real de la gestión de la seguridad de la información en la entidad y con base en esto poder definir una estrategia y hoja de ruta para la definición, establecimiento e implementación de un Sistema de Gestión de Seguridad de la Información.

Dentro de este ejercicio y teniendo en cuenta los hallazgos en el proceso de diagnóstico o Análisis GAP, se establecen unas recomendaciones para iniciar una administración adecuada y alineada a un marco normativo aplicable.

La intranquilidad por la seguridad de los activos de información de las organizaciones se deriva de la gran cantidad de amenazas y riesgos que cada día se hacen más numerosos, complejos y recurrentes. Con el fin de mitigar los riesgos producidos por estas amenazas, todas las entidades están implementando controles que parten de las mejores prácticas conocidas y la normatividad aplicable.

Por lo anterior a la Corporación Autónoma Regional del Río Grande de la Magdalena - CORMAGDALENA se le planteara en el presente documento una estrategia o hoja de ruta para establecer, implementar, operar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), que permita gestionar los riesgos de seguridad de los activos de información de una manera estructurada, documentada, repetible y medible.

2. OBJETIVOS

1.1 Objetivo General

Presentar la estrategia o la hoja de ruta para establecer e implementar un Sistema de Gestión de Seguridad de la Información y/o una línea base del mismo, alineado con la norma NTC ISO/IEC 27001:2013

1.2 Objetivos Específicos

- Presentar un plan de acciones de alto nivel para subsanar los hallazgos encontrados frente a los requisitos de la norma NTC ISO/IEC 27001:2013.
- Plantear la implementación de la fase Hacer del ciclo PHVA para el Sistema de Gestión de Seguridad de la Información.
- Iniciar el cumplimiento y la implementación de las cláusulas y los controles NTC ISO/IEC 27001:2013.

3. ALCANCE

Presentar una estrategia, para establecer e implementar una línea base del Sistema de Gestión de Seguridad de la Información, entendiendo la estrategia como la descripción de un conjunto de acciones que se alinean con las metas y los objetivos de la entidad en este aspecto.

4. MARCO TEORICO

El marco teórico de este documento está estrechamente relacionado con la norma NTC ISO/IEC 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 normas debe ser una decisión estratégica para la entidad, con el objetivo de adoptar las mejores prácticas de la industria para la gestión de la seguridad, así como para cumplir con el marco normativo y regulatorio definido por el Ministerio de las TIC y su Decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital"*. El diseño y la posterior implementación del SGSI en una entidad deben estar basados en las necesidades, objetivos, requisitos de seguridad, procesos, empleados, tamaño y estructura de esta.

La gestión de la seguridad de la información es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la entidad de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. La gestión de la seguridad de la información requiere la participación de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información, así como el debido control de acceso a los recursos y activos de información.

Con base en los hallazgos, observaciones y recomendaciones del ejercicio de diagnóstico realizado en la asesoría de seguridad de la información, en su entregable ***"2_Informe estado actual Gestión Seguridad de la Información",*** se definen una serie de actividades orientadas a establecer la línea base del SGSI.

5. ESTRATEGIA PARA EL ESTABLECIMIENTO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Una estrategia consiste en la selección de un proceso a través del cual, desde un estado actual se prevé alcanzar un cierto estado futuro, con el desarrollo de una serie de actividades estrictamente ordenadas para alcanzar el objetivo.

Desde el inicio del reconocimiento de la necesidad de Gestionar la Seguridad de Información, se debe incluir y evidenciar de manera efectiva el compromiso y soporte de la alta dirección, organizando y administrando la iniciativa como un proyecto hasta su finalización y estabilización, cumpliendo con plazos acordados y los recursos presupuestales.

Lo que se pretende con el desarrollo de la presente estrategia se explica en la siguiente gráfica:

Ilustración 1. – Objetivos de la estrategia

Se menciona el establecimiento e implementación del SGSI dentro de un proyecto, dado que dentro del ciclo PHVA, las dos primeras fases (planear y hacer) tienen un inicio y un fin que se pueden proyectar y programar como se hace con cualquier otro proyecto, finalizada estas fases e incorporando las dos restantes (verificar y actuar), ya se convierte en el proceso requerido (no tiene fin), para asegurar la aplicación de controles de seguridad efectivos que protejan los activos de información y brinden confianza a las partes interesadas de la entidad.

La estrategia que se plantea básicamente contiene los siguientes pasos:

a) Establecimiento e implementación de un SGSI con base en la NTC-ISO/IEC 27001:2013.
b) Incorporar la gestión de la seguridad de la Información dentro de un nuevo proceso documentado y formalizado dentro del mapa de procesos con dependencia directa de la alta dirección o mínimo como un proceso estratégico.
c) Se deben incorporar proyectos de seguridad de la información dentro de planes y objetivos estratégicos de la entidad.
d) Se debe establecer y ejecutar un Plan Estratégico de Tecnologías de la Información y las Comunicaciones “PETIC”, donde se involucren proyectos y actividades de seguridad de la información.
e) La entidad debe considerar la relación de los requisitos del SGSI con los lineamientos de política y el Manual de Gobierno Digital, con el objetivo de cumplir los requisitos normativos y regulatorios de Ministerio de Tecnologías de la Información y las Comunicaciones en lo relacionado con la seguridad de la información.

6. ESTABLECIMIENTO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) CON BASE EN LA NTC-ISO/IEC 27001:2013

La Corporación Autónoma Regional del Río Grande de la Magdalena – CORMAGDALENA debe iniciar como una decisión estratégica y como la única manera de dar cumplimiento al marco normativo y regulatorio que le aplica, desde la estrategia de Gobierno Digital, (reglamentada por el Ministerio de las TIC con el Decreto 1008 de 2018), la adopción de la norma NTC-ISO/IEC 27001:2013, teniendo en cuenta que es el único criterio descrito en el habilitador transversal “Seguridad y Privacidad” además de ser la norma más usada en la industria y se contempla como una de las mejores prácticas para la gestión de la seguridad de la información.

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización.

El Sistema de Gestión de Seguridad de la Información (SGSI), planteado tiene un enfoque basado en los procesos internos de la entidad. El SGSI se incorpora a la organización mediante la adopción de un modelo PHVA que define las etapas de establecimiento, implementación, operación, seguimiento, mantenimiento y mejora del sistema frente a la seguridad de la información.

Para el funcionamiento eficiente del Sistema de Gestión de Seguridad de la Información, se deben identificar y gestionar las actividades involucradas para la protección de la información del proceso de tecnología, buscando que estas prácticas de seguridad de la información sean integradas en el día a día.

Este enfoque basado en procesos hace énfasis en la importancia de:

- Comprender los requisitos de seguridad de la información de la entidad y la necesidad de establecer políticas, normas y procedimientos con relación a la seguridad de la información.
- Determinar, diseñar, implementar y operar controles para dar tratamiento a los riesgos de seguridad de la información de la entidad, en el contexto de los riesgos que impactan los procesos.
- Incorporar actividades de protección de información a nivel de los procesos dentro del alcance de SGSI.
- El seguimiento y revisión permanente del desempeño y eficacia del SGSI.
- La mejora continua basada en la medición de los objetivos planteados inicialmente.

Con la estrategia planteada, el Sistema de Gestión de Seguridad de la Información adopta el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA), aplicándolo para estructurar todos los procesos que apoyan el sistema. El SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas planteadas por la entidad, y a través de las acciones y procesos diseñados para soportar el SGSI, produce resultados de seguridad de la información que buscan cumplir estos requisitos y expectativas.

Ilustración 2. - Ciclo PHVA para el SGSI

Las etapas del modelo de procesos que enmarcan el SGSI se definen de la siguiente forma:

- ***Planificar (establecer el SGSI):*** Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
- ***Hacer (implementar y operar el SGSI):*** Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
- ***Verificar (hacer seguimiento y revisar el SGSI):*** Evaluar, y en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica y reportar los resultados a la dirección para su revisión.
- ***Actuar (mantener y mejorar el SGSI):*** Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

En la fase de planeación que corresponde a la primera que debe abordar la entidad, comprende la definición y desarrollo de las siguientes actividades:

- Definir el alcance del SGSI y política de seguridad.
- Definir el contexto organizacional del SGSI.

- Establecer, documentar y aprobar una política de seguridad de la información.
- Definir las partes interesadas para el SGSI.
- Establecer los objetivos del SGSI.
- Definir, asignar y comunicar los roles, responsabilidades y autoridades para la seguridad de la información.
- Realizar un inventario de todos los activos de información.
- Definir y aplicar un proceso de valoración de riesgos que permita realizar evaluaciones y tratamientos repetidos de riesgos de la seguridad de la información y se produzcan resultados consistentes, válidos y comparables.
- Aplicar una metodología de evaluación del riesgo.
- Hacer una evaluación de riesgos periódica, mínimo una vez al año.
- Hacer la selección de controles para el tratamiento de riesgos.
- Establecer una declaración de aplicabilidad.
- Definir el plan de tratamiento de riesgos.
- Hacer la implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definir un método de medida de la eficacia de los controles y puesta en marcha de este.
- Llevar a cabo programas de formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Realizar la monitorización constante y registro de todos los incidentes de seguridad de la información.
- Realizar auditorías internas.
- Hacer una evaluación periódica del SGSI y de su alcance.
- Mejorar continuamente el SGSI.

Todas las acciones relacionadas anteriormente se pueden ejecutar o desarrollar en varias ordenaciones o estructuras, lo relevante es su desarrollo. Para llevar a cabo las actividades propuestas para el diseño y establecimiento del Sistema de Gestión de Seguridad de la entidad, se plantea en la siguiente gráfica, la organización y el agrupamiento de las actividades a realizar:

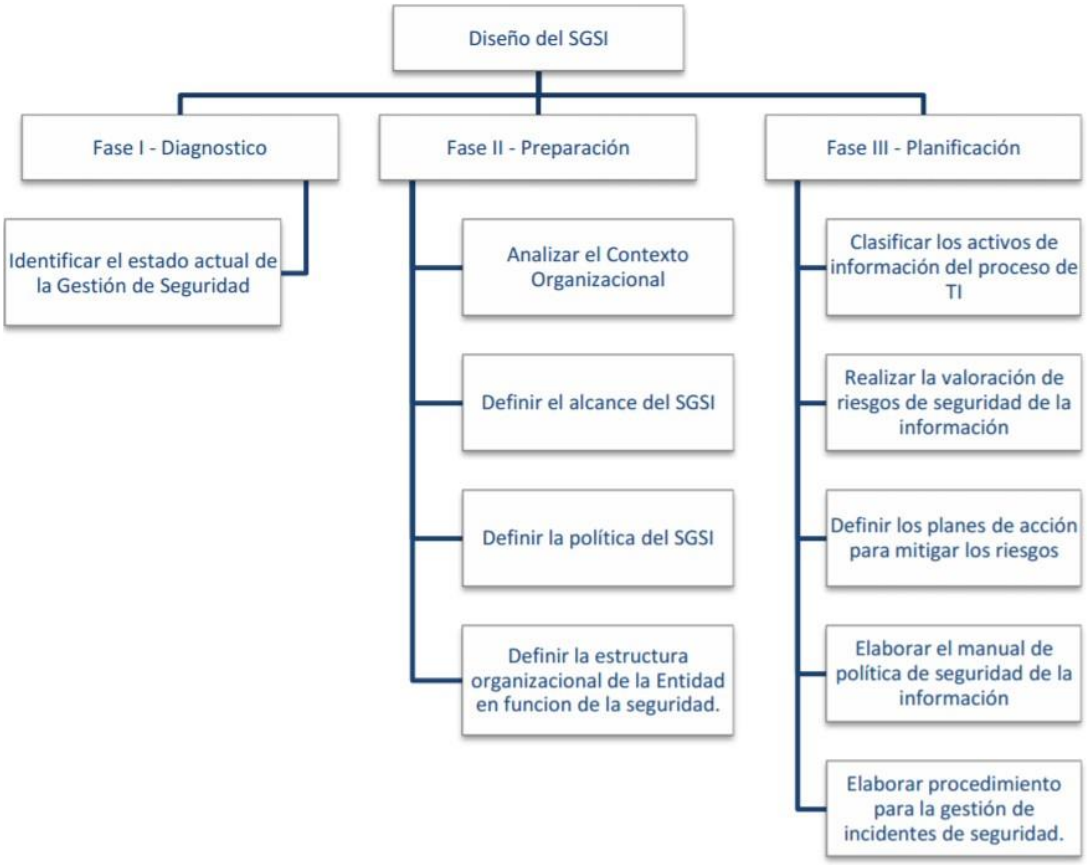

Ilustración 3. – Actividades propuestas para el diseño del SGSI

Los subprocesos o procedimientos que se deben definir y documentar dentro de la gestión de la seguridad de la información en la Corporación Autónoma Regional del Río Grande de la Magdalena - CORMAGDALENA, son los siguientes:

Ilustración 4. – Subprocesos o procedimientos de la Gestión de la Seguridad de la Información.

Para el desarrollo de las actividades de establecimiento e implementación del Sistema de Gestión de la Seguridad de la Información de la entidad se debe plantear un cronograma para las vigencias 2021 y 2022.

7. 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