CORMAGDALENA

La energía de un río que impulsa a un país

CORPORACIÓN AUTÓNOMA REGIONAL DEL RÍO MAGDALENA

DIAGNOSTICO DOCUMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Marzo 2024

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 controlada, 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.

Este sistema (SGSI) 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.

2. OBJETIVOS

2.1 Objetivo General

Realizar un análisis del cumplimiento de la documentación mínima requerida normativamente para la Seguridad de la Información con base en la norma NTC ISO 270001:20013 versus la documentación existente relacionada con seguridad de la información.

2.2Objetivos Específicos

- Presentar los resultados de la evaluación del estado actual de:
  - El cumplimiento de la documentación mínima requerida normativamente para la Seguridad de la Información con base en la norma NTC ISO 270001:20013.
  - La documentación existente relacionada con seguridad de la información.

Esto como parte del Análisis de Brecha (Gap Analysis, por su denominación en inglés) con respecto a los requisitos de la norma NTC/ISO 27001:2013, con el fin de comprender el estado real de la gestión de la seguridad de la información dentro de la entidad, el cual es un insumo para promover la implementación de políticas, lineamientos y controles a fin de reducir el riesgo de afectación en la confidencialidad, integridad y disponibilidad de la información.

- Evaluar el grado de implementación y cumplimiento de las cláusulas, los controles y objetivos de control descritos en la norma NTC/ISO 27001:2013.
- Suministrar información para los futuros procesos de 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 27001:2013.

3. ALCANCE

Este informe cubre los documentos que se recopilaron y analizaron durante las entrevistas, este ejercicio se orientó en la identificación de la documentación especializada en la gestión de la seguridad de la información, independiente de su tipo o formato (política, procedimiento, manual, guía, lista de chequeo, etc.), para realizar el análisis del cumplimiento de la documentación mínima requerida normativamente para la Seguridad de la Información con base en la norma NTC ISO 270001:20013 contra la documentación existente relacionada con la seguridad de la información verificando también calidad y pertinencia.

4. 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 críticas de los procesos críticos, afectando considerablemente la prestación de servicios públicos a una comunidad.
- **BIA**: (Business Impact Analysis) Proceso diseñado para priorizar las actividades criticas 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.

- **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.

5. Documentación Obligatoria mínima requerida normativamente para el SGSI con base en la norma NTC ISO 270001:20013.

5.1 Documentación Obligatoria

Después de la revisión de la norma ISO/IEC 27001 que termino a finales del 2013, se evaluó nuevamente el listado de los documentos llamados obligatorios para un Sistema de Gestión de la Seguridad de la Información (SGSI), que definen como los documentos más comúnmente usados en una implantación de la mencionada norma, que para el caso colombiano se utilizara la NTC-ISO-IEC 27001:2013, pues de hecho es la que aparece referenciada como requisito en la estrategia de Gobierno Digital, que impulsa el Ministerios de las TIC.

El análisis de brecha de la documentación obligada para el establecimiento e implementación de un SGSI, recorre todos los numerales que son requisito de la norma, así como algunos de los controles del anexo A de la misma. Se busca identificar el estadode cumplimiento de la documentación aplicable.

A continuación, se relacionan los documentos que se deben elaborar, aprobar, socializar e implantar, si se quiere cumplir con la norma NTC-ISO-IEC 27001:2013.

- El alcance del sistema de gestión de seguridad de la información (cláusula 4.3)
- Política de seguridad de la información y objetivos (cláusulas 5.2 y 6.2)
- Metodología de evaluación y tratamiento de riesgos (cláusula 6.1.2)
- Declaración de aplicabilidad (cláusula 6.1.3 d)
- Plan de tratamiento de riesgo (cláusula 6.1.3 e y 6.2)
- Informe sobre evaluación de riesgos (cláusula 8.2)
- Definición de roles y responsabilidades de seguridad (cláusulas A.7.1.2 y A.13.2.4)
- Inventario de activos (cláusula A.8.1.1)
- Uso aceptable de los activos (cláusula A.8.1.3)
- Política de control de acceso (cláusula A.9.1.1)

- Procedimientos de operación para gestión de TI (cláusula A.12.1.1)
- Principios de ingeniería de sistemas seguros (cláusula A.14.2.5)
- Política de seguridad para proveedores (cláusula A.15.1.1)
- Procedimiento para gestión de incidentes (cláusula A.16.1.5)
- Procedimientos de Continuidad de negocio (cláusula A.17.1.2)
- Requerimientos legales, regulatorios y contractuales (cláusula A.18.1.1)

Registros obligatorios:

- Registros de formación, habilidades, experiencia y calificaciones (cláusula 7.2)
- Seguimiento y resultados de medición (cláusula 9.1)
- Programa de auditoría interna (cláusula 9.2)
- Resultados de auditorías internas (cláusula 9.2)
- Resultados de la Revisión por Dirección (cláusula 9.3)
- Resultados de acciones correctivas (cláusula 10.1)
- Registros de las actividades de usuario, excepciones y eventos de seguridad (cláusulas A.12.4.1 y A.12.4.3)

5.2 Análisis documentación Obligatoria

Con base en las entrevistas y correos electrónicos con diferentes funcionarios de la entidad se realiza el ejercicio de validar la existencia de la documentación relacionada con la gestión

de la seguridad de la información. Igualmente, para dar un panorama general de cumplimiento se utiliza una escala de colores que indica en cuales documentos se debe trabajar prioritariamente, la escala de colores es la siguiente:

Estado	Significado
	Existe, está documentado, cumple 100% con lo que la norma solicita, es conocido y aplicado por todos los involucrados en el SGSI.
	Cumple parcialmente con la documentación o existe algún documento base que puede ser utilizado para cumplimiento del punto luego de algún o actualización.
	No existe ninguna documentación.

Tabla 1. Valoración de cumplimiento de documentos.

Documento	*Clausula*	*Cumplimiento*
Política de Alto Nivel de Seguridad de la Información	5.2 y 6.2	
El alcance del sistema de gestión de seguridad de la información	4.3	
Metodología de evaluación y tratamiento de riesgos	6.1.2	
Declaración de aplicabilidad	6.1.3 d	
Plan de tratamiento de riesgo	6.1.3 e y 6.2	
Informe sobre evaluación de riesgos	8.2	
Definición de roles y responsabilidades de seguridad	A.7.1.2 y A.13.2.4	
Inventario de activos	A.8.1.1	
Política de uso aceptable de los activos	A.8.1.3	

Política de control de acceso	A.9.1.1	
Procedimientos de operación para gestión de TI	A.12.1.1	
Política de seguridad para proveedores	A.15.1.1	
Procedimiento para gestión de incidentes de seguridad	A.16.1.5	
Procedimientos de Continuidad de negocio	A.17.1.2	
Definición y política de los requerimientos legales, regulatorios	A.18.1.1	

Registros de seguimiento y resultados de medición	9.1	
Programa de auditorías internas e informes de estas	9.2	
Registros de los resultados de la revisión por la Dirección	9.3	
Registros de los resultados de las acciones correctivas	10.1	

Realizadas las entrevistas y solicitadas las evidencias de la documentación relacionada, se observa que no se pueden analizar documentos en los aspectos de calidad y pertinencia por la ausencia de estos.

6. Conclusiones

- La Corporación Autónoma Regional del Río Grande de la Magdalena - CORMAGDALENA debe generar la documentación necesaria para el Sistema de Gestión de la Seguridad de la Información, pero también debe garantizar una correcta gestión de la documentación, estableciendo procedimientos para el controly protección de dicha documentación.
- Todos los documentos deben de ser identificados y distribuidos correctamente en formato papel o digital, garantizando la disponibilidad y acceso en el momento quese necesite, además de ser revisados y aprobados para garantizar que son formales y obedecen a decisiones de la alta dirección, tal y como establece la norma.
- Con base en la revisión y análisis de la documentación recabada se puededeterminar el nivel de cumplimiento con la documentación base u obligada para el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI),la cual actualmente presenta un nivel muy bajo cumplimiento de la documentaciónnecesaria (se estima entre un 3% a 5%).

- Con base en la documentación recopilada, revisada y analizada se puede concluir que la entidad no cuenta con un Sistema de Gestión de Seguridad de la Informacióny no se ha iniciado la implantación de la norma NTC-ISO-IEC 27001:2013.

Elaboró: Ingenieros TIC- Secretaría General