Atlántico para la Gente

GOBERNACIÓN DEL ATLÁNTICO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSION 1.0

Principales modificaciones por versión de este documento

Historial de Versiones

Versión	Autor	Fecha	Descripción de la Modificación
1.0	Ing. Adriana Martínez Ing. Xavier Mejia	10 nov del 2023	Elaboración de Estructura y Contenido

Este documento ha sido revisado y aprobado por:

Versión	Revisor	Firma
1.0	Secretaría General – Grupo de Gestión de TI	

CONTENIDO

Tabla de contenido

1. INTRODUCCIÓN

Las disposiciones de la política de gobierno digital en Colombia provienen del Decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, del 1078 de 2015, y fueron ajustadas con el decreto 767 de 2022. Su objetivo es mejorar la relación Estado-Ciudadano, prestando servicios por parte de las entidades, para interceptar una confianza mayor mediante el uso de las TIC. Hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de Gestión y Desempeño Institucional.

La nueva Política de Gobierno Digital articula elementos de gobernanza digital, innovación pública centrada en el ciudadano, habilitadores clave, líneas estratégicas centrales e iniciativas impulsoras. Estas líneas se desarrollan mediante directrices y estándares, que son requisitos mínimos para lograr los objetivos planteados por la política.

Este habilitador fundamental se basa en el Modelo de Seguridad y Protección de Datos, emitido por el Ministerio de Tecnología e Información, y cuya adopción por parte de las entidades estatales conduce a salvaguardar la confidencialidad, integridad y disponibilidad de la información sensible, apoyado en un proceso de gestión de riesgos que crea las condiciones adecuadas para el uso fidedigno en el entorno digital, otorgando seguridad a los interesados.

Este documento hace parte integral del programa de seguridad y privacidad de la Información de la Gobernación del Departamento del Atlántico, enfocados en el Modelo de Seguridad y privacidad de la información – MSPI propuesto por el gobierno nacional.

La Gobernación del Atlántico comprometida con la gestión de la seguridad de la información de sus procesos misionales, expresa la adopción de la gestión de la seguridad de sus activos de información apoyado en un proceso de gestión del riesgo.

La adopción, implementación y evaluación del modelo mencionado es una actividad obligatoria, según lo establece el decreto 612 de 2018 en su artículo 1. Este debe ser integrado y planificado en los planes institucionales en el ámbito de aplicación del modelo integrado de planeación y gestión.

Además, la resolución 0500 del 10 de marzo de 2021 precisa la necesidad de que los sujetos obligados adopten medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información, con el fin de mitigar los riesgos relacionados con la protección y la privacidad de la información, así como los incidentes de seguridad digital.

En atención a lo anterior, se presenta el plan para fortalecer la implementación del modelo de seguridad y privacidad de la información de la entidad.

2. OBJETIVO

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en los procesos de la Entidad.

2.1 Objetivos Específicos

• Identificar y salvaguardar los activos de información de la Gobernación del Atlántico, considerado los principios de confidencialidad, integridad y disponibilidad.

• Analizar los riesgos de seguridad de la información

• Concientizar a funcionarios y contratistas acerca del modelo de seguridad y privacidad de la información, para reforzar su comprensión sobre la importancia de proteger los activos de información críticos de la Gobernación.

• Implementar acciones correctivas y de mejora para el marco de seguridad y privacidad de la información.

3. ALCANCE

Los límites y la aplicabilidad de la adopción, establecimiento, implementación, operación, verificación y mejora del Modelo de seguridad y privacidad de la información- MSPI de la Gobernación del Atlántico, en el marco del modelo de operación del MSPI de la entidad es concordante al cumplimiento legal actual y futuro que se determine como lineamiento nacional referente al MSPI, además está encaminado a fortalecer la seguridad de toda la información física y digital de propiedad o en custodia de la Gobernación del Atlántico en su sede principal ubicada en la ciudad de Barranquilla en la calle 40 # 45-46, por lo cual rige de forma transversal a todos los procesos, cualquier tecnología propia o de terceros que la soporte y de obligatorio cumplimiento para todos sus funcionarios,

contratistas y terceros de la entidad, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la Entidad compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por la Entidad, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

4. ROLES Y RESPONSABILIDADES

La dirección de la Gobernación del Departamento del Atlántico reconoce que la confidencialidad, integridad y disponibilidad de la información son fundamentales para cumplir su misión institucional. Consciente de que la información es uno de sus activos más importantes, se compromete a asignar los recursos necesarios para establecer, implementar, operar, dar seguimiento, mantener y mejorar de forma continua la postura de seguridad de la información. En cumplimiento de las responsabilidades legales y con el fin de salvaguardar los activos de información, la dirección de la entidad se compromete a implementar el Modelo de Seguridad y Privacidad de la información propuesto por MinTIC.

Con el fin de garantizar la pertinencia y la efectividad del nuevo Sistema de Gestión de Seguridad de la Información, dentro de las políticas de seguridad se incluyó la realización de auditorías internas y la realización de revisiones periódicas al MSPI por parte de la secretaria de Control Interno.

A continuación, se describen los roles y responsabilidades dentro del Modelo de Seguridad y privacidad de la información de la Gobernación del Atlántico.

ROL	DEFINICIÓN	RESPONSABILIDADES
Alta Dirección	La alta dirección de la gobernación del Atlántico en cabeza de su gobernador tiene el rol de actuar como líder del MSPI, mostrando compromiso aprobando todas las políticas, objetivos y demás documentos conformantes del MSPI; asegurando la integración del MSPI en los procesos de negocio y asegurando que se asignen y comuniquen los roles y responsabilidades del MSPI.	✓La Alta Dirección de la Gobernación del Atlántico debe definir, establecer e informar los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo. ✓ La Alta Dirección deberá definir y establecer el procedimiento de contacto con las autoridades, y establecer cuando y que autoridades se deben contactar para diferentes escenarios, además de definir el responsable para establecer dicho contacto. ✓ La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento. ✓ La Alta Dirección debe exigir a todo el personal de la entidad que aplique las políticas y procedimientos de seguridad de la información. ✓ La Alta Dirección debe promover activamente una cultura de concienciación relacionada con seguridad de la información. ✓La Alta Dirección debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios, contratistas y personal provisto por terceras partes que desarrollen actividades en la Gobernación del Atlántico. ✓ La Alta Dirección debe incluir dentro de los ejes y objetivos estratégicos acciones que garanticen el cumplimiento de política y asignar los recursos adecuados, de infraestructura física, lógica y de personal con las habilidades necesarias para la gestión de la seguridad de la información.

ROL	DEFINICIÓN	RESPONSABILIDADES
Comité de seguridad y privacidad de la información	Órgano de tipo estratégico, conformado por los lideres de áreas estratégicas designados por acto administrativo y que deben a través de reuniones periódicas abordar acciones de aprendizaje de incidentes pasados y estrategias para mejora continua del MSPI.	✓ Actualizar anualmente las políticas de seguridad de la Información de la institución. ✓ Coordinar las decisiones de seguridad de la información, nuevas políticas, normas, análisis de riesgos, planes de continuidad del negocio, recuperación de incidentes, etc. ✓ Identificar las necesidades, establecer y mantener un plan de entrenamiento para el personal encargado de la seguridad de la información en la entidad. ✓ Aprobar las medidas de seguridad de la información, incluyendo planes de continuidad del negocio, análisis de riesgos, actualización de controles, normas y cambios en las políticas de seguridad. ✓ Coordinar los esfuerzos de todos los grupos internos con responsabilidades sobre la seguridad de la información. ✓ Aprobar los acuerdos de confidencialidad que deben realizarse con proveedores de servicios, servicios de outsourcing y demás terceros. ✓ Coordinar todos los proyectos de mejora respecto a la seguridad de la información dentro de la organización. ✓ Promover auditorias periódicas de seguridad de la información con el fin de identificar desviaciones y subsanarlas. ✓ Apoyar al oficial de seguridad en la coordinación de las actividades de capacitación y sensibilización referentes a la seguridad de la información en la organización.

ROL	DEFINICIÓN	RESPONSABILIDADES
Responsable de la Seguridad y privacidad de la información	Responsable de los lineamientos tácticos del MSPI, por lo cual debe desarrollar, implementar y mejorar continuamente el MSPI de la Gobernación del Atlántico, según las estrategias definidas por el oficial de seguridad de la información. .	✓Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del MSPI, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo ✓ Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad ✓ Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información. ✓ Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido. ✓ Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos. ✓ Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo ✓ Encarrilar el MSPI hacia el cumplimiento de los lineamientos definidos por MINTIC. ✓ Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del MSPI para darle solución oportuna y escalar al Comité de seguridad y privacidad en caso de ser necesario. ✓ Monitorear el estado del MSPI en términos de calidad de los productos, tiempo y los costos. ✓ Trabajar de manera integrada con el grupo o áreas asignadas.

ROL	DEFINICIÓN	RESPONSABILIDADES
Grupo de Gestión de TI	El rol del grupo de gestión de TI es el de proponer y operacionalizar las políticas y lineamientos referentes a la seguridad informática del MSPI de la entidad.	✓El Grupo de Gestión de TI debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario. ✓ El Grupo de gestión de TI debe liderar la generación de lineamientos para gestionar la seguridad informática de la Gobernación del Atlántico y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad. ✓ El Grupo de Gestión de TI debe validar y monitorear de manera periódica la implantación de los controles de seguridad informática establecidos. ✓ El Grupo de Gestión de TI debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la Gobernación. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas. ✓ El Grupo de Gestión de TI debe establecer y mantener un flujo adecuado de información relevante y actualizada que permita tomar acciones preventivas referentes a nuevas tecnologías, amenazas o vulnerabilidades; además de servir como punto de enlace en la gestión de incidentes de seguridad de la información.

ROL	DEFINICIÓN	RESPONSABILIDADES
Oficina asesora jurídica	El rol de la oficina Jurídica es de acompañamiento a todos los demás actores del MSPI en cuanto a la completitud y mantenimiento de las matrices de cumplimiento, y brindar asesoría en temas jurídicos y legales correspondientes al MSPI.	✓Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. ✓ Brindar asesoría al Comité de seguridad y privacidad de la información temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes. ✓ Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso. ✓ Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información. ✓ Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.
Oficina de Gestión del Talento Humano	El rol de la oficina de Gestión del Talento Humano es de acompañamiento en el cumplimiento en el Plan de capacitaciones del MSPI	✓Controlar y salvaguardar la información de datos personales del personal de planta de la entidad, en concordancia con la normatividad vigente. ✓ Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

ROL	DEFINICIÓN	RESPONSABILIDADES
Oficina Control Interno	El rol de la oficina de Control Interno es el de auditar el cumplimiento de lo estipulado desde la parte estratégica en cuanto al MSPI. Monitorizar constantemente el estado del MSPI de la entidad con respecto a los objetivos planteados.	✓Control Interno debe planear y ejecutar las auditorías internas al Modelo de Seguridad y Privacidad de la Información, a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables. ✓ Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del MSPI, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades. ✓ Control Interno debe informar a las áreas responsables los hallazgos de las auditorías realizadas al MSPI.
Grupo interno de trabajo de gestión documental	El rol del grupo de interno de trabajo de gestión documental es el de operacionalizar las políticas y lineamientos referentes a la seguridad de la información impresa o en medios físicos de la entidad	✓El grupo interno de Gestión Documental deberá establecer dentro de Programa de gestión documental todas las medidas necesarias para salvaguardar la confidencialidad, integridad y disponibilidad de la información creada, procesada, transportada y almacenada en los documentos físicos producidos o recibidos por la entidad ✓ En el procedimiento de Planeación Documental, se deben determinar su permanencia y medidas de seguridad en las diferentes fases del archivo y determinar cómo su disposición final no permite la recuperación de la información de forma no autorizada

ROL	DEFINICIÓN	RESPONSABILIDADES
Equipo técnico del MSPI	Conjunto de funcionarios operativos que se encargan en traducir las políticas en realidad, el equipo técnico debe estar compuesto por miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente del área de gestión de TI	✓Apoyar al líder de proyecto al interior de la entidad. ✓ Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del MSPI. ✓Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura. ✓ Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder del MSPI. ✓ Las que considere el líder del proyecto o el comité de seguridad de la entidad
Usuario final	Son todos los demás funcionarios, contratistas y personal provisto por terceras partes que realice labores en o para la Gobernación del Atlántico, los cuales tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información y ser un agente activo y participe en el Modelo de Seguridad y Privacidad de la información.	✓Cumplir con las políticas de seguridad y privacidad de la información y todos sus los documentos estipulados en el marco de Modelo de Seguridad y Privacidad de la información. ✓ Reportar cualquier indicio de incidente de seguridad siguiendo el procedimiento estipulado para ello. ✓ Ser un usuario final precavido y responsable con el uso de la información que cree, reciba o procese. ✓ Asistir a los entrenamientos o capacitaciones relacionados por los demás órganos del MSPI, en relación con la seguridad de la información e informática

5. CONCIENTIZACIÓN, CAPACITACION Y ENTRENAMIENTO

La ciberseguridad no debe ser un tema exclusivo del área de tecnología de la Gobernación del Atlántico, sino que debe considerarse como un tema de interés común por todos los funcionarios, contratistas y terceros, ya que cada uno de estos genera, manipula, procesa, almacena y/o transporta datos e información referente a su labor o necesidad particular.

Es por lo anterior que se debe diseñar, ejecutar y mantener un plan de capacitaciones referentes a conceptos, ataques, contra medidas y técnicas asociadas a la ciberseguridad, con el fin de minimizar el riesgo de que las personas sean aprovechadas para obtener información de forma malintencionada; además al conocer el actuar de los cibercriminales es menos probable sucumbir ante las técnicas conocidas.

Para el éxito de este plan se deben garantizar el compromiso de todas las personas que dentro o fuera de esta interactúan con la Gobernación del Atlántico, desde la alta dirección hasta la parte operativa, funcionarios o contratistas; considerando que se deben aunar esfuerzos a favor de resguardar la confidencialidad, integridad y disponibilidad de toda información propia o de terceros que tenga en custodia la Gobernación del Atlántico.

El plan de concientización, capacitación y entrenamiento al personal es un punto siempre recurrente en cualquier normativa relacionada con seguridad, en ISO 27002 versión 2022 numeral 6.3 “Concientización, educación y capacitación en seguridad de la información” , en el MSPI numeral 7.4.2 “Competencia, toma de conciencia y comunicación”, por lo cual se deben plantear las pautas necesarias para desarrollar este punto con éxito dentro de la Gobernación del Atlántico; este documento presenta y formaliza todas aquellas acciones que se encaminen con respecto a este tema.

Al diseñar este plan se consideró aspectos de logística como cronogramas sugeridos, presupuestos, responsables, locaciones, etc. y aspectos técnicos como temas, perfil del entrenador, material de capacitación, etc.; todo lo anterior debe considerarse para el buen desarrollo y cumplimiento de los objetivos planteados

6. AUDITORIAS INTERNAS DEL MSPI

La Entidad realizará anualmente auditorías internas, orientadas a validar el cumplimiento de los objetivos de control, la efectividad de los controles administrativos, técnicos y a los procedimientos del Sistema de Gestión de Seguridad de la Información.

La Secretaría de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información, a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.

La Secretaría de Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

La Secretaría de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías realizadas

7. GESTIÓN DE RECURSOS

La Gobernación del Departamento del Atlántico, consciente de la importancia que reviste el Modelo de Seguridad y Privacidad de la Información - MSPI, ha presupuestado recursos para garantizar la gestión permanente de la seguridad de la Información

8. COMPATIBILIDAD DEL MSPI CON OTROS SISTEMAS DE GESTION

El Sistema de Gestión de la Seguridad de la Información adoptado por la entidad, estará alineado con la norma NTC ISO/IEC 27001, con el fin de facilitar la integración el Sistema de Gestión de Calidad existente, basado en la norma NTC ISO 9001:2018 y cualquier otro sistema de gestión relacionado

9. TERMINOS Y DEFINICIONES

Las expresiones utilizadas en este documento deben ser entendidas con el significado que a continuación se indica. Los términos definidos son aplicados en singular y en plural de acuerdo como lo requiera el contexto en el cual son considerados. Y aquellos que no se encuentren definidos a continuación, deben entenderse con su significado natural.

Los Términos y Definiciones mostrados a continuación fueron tomados de las referencias listadas al final del documento.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización. [1]

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. [2]

Antimalware: [Definición modificada tomando como base la definición de Antivirus de MinTIC]. Antimalware es una categoría de software de seguridad que protege un equipo de malware, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los softwares maliciosos. El antimalware debe ser parte de una estrategia de seguridad estándar de múltiples niveles. [3]

Archivo: Es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. [4]

Autenticidad: Propiedad de que una entidad es lo que afirma ser. [2]

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales. [5]

Ciberseguridad: Preservación de la confidencialidad, la integridad y la disponibilidad de la información y/o de los sistemas de información a través del medio cibernético. Asimismo, pueden estar involucradas otras propiedades, tales como la autenticidad, la trazabilidad, el no repudio y la confiabilidad.[2]

Confidencialidad: Propiedad según la cual la información no está disponible para personas, entidades, procesos o sistemas no autorizados, ni se da a conocer a personas, entidades, procesos o sistemas no autorizados. [2]

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. [3]

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. [2]

Evaluación de Riesgo: Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables. [6]

Gestión de Incidentes de Seguridad de la Información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. [2]

Gestión Documental: Es el conjunto de actividades administrativas y técnicas tendientes a la planificación, procesamiento, manejo y organización de la documentación producida y recibida por los sujetos obligados, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación. [4]

Incidente de Seguridad de la Información: Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una

probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información [2]

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. [4]

Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. [4]

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. [4]

Información Pública Reservada: Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley. [4]

Integridad: propiedad exactitud y completitud. [2]

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. [2]

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. [2]

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. [2]

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. [2]

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información. [2]

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. [2]

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. [5]

10. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan comprende la ejecución y seguimiento del siguiente cronograma.

CRONOGRAMA 2024								
ACTIVIDAD	#	TAREA	RESPONSABLE	AÑO	TRIMESTRES			
					1	2	3	4
FASE DE DIAGNOSTICO (GAP)	1	***Actividades Administrativas***						
	1.1	Revisión y actualización del proceso e identificación de subprocesos internos	Secretaria TIC	**2024**				
	1.2	Revisión y actualizacion de la documentación de procesos y procedimientos	Secretaria TIC	**2024**				
	1.3	Revisión y actualizacion de controles administrativos y técnicos instalados	Secretaria TIC	**2024**				
	1.4	Revisión de documentos de auditorías anteriores	Secretaria TIC	**2024**				
	1.5	Revisión y actualizacion del Análisis de brecha documental (apoyados e el instrumento de MinTIC)	Secretaria TIC	**2024**				
	1.6	Cuantificar los puntos de acceso a la red.	Secretaria TIC	**2024**				
	1.7	Identificar los principales recursos Accesibles a través de cada punto de acceso.	Secretaria TIC	**2024**				
FASE 2 (PLANIFICACION)	2	***Entender a la organización y el contexto proceso de "gestión Tecnológica".***						
	2,1	Revisar y actualizar el alcance de las políticas de seguridad y privacidad de la información.	Secretaria TIC	**2024**				
	2,2	Revisar y actualizar acto administrativo con las funciones de seguridad y privacidad de la información	Secretaria TIC	**2024**				
	2,3	Revisar y/o actualizar el documento de políticas de seguridad y privacidad de la información.	Secretaria TIC	**2024**				
	2,4	Revisar y/o actualizar el documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información.	Secretaria TIC	**2024**				
	2,5	Revisar y/o actualizar el plan de capacitación, sensibilización y comunicación de seguridad de la información.	Secretaria TIC	**2024**				
	2,6	Revisar y actualizar la Identificación , clasificación y gestión de los activos de información	Secretaria TIC	**2024**				
	2,7	Revisar y actualizar el análisis de riesgos asociados a los activos de la información.	Secretaria TIC	**2024**				
	2,8	Construcción del plan de implementación de controles.	Secretaria TIC	**2024**				
	2,9	Construcción de la declaración de aplicabilidad.	Secretaria TIC	**2024**				
VALOR AGREGADO	3	Charla de sensibilización sobre ciberseguridad y ciberdefensa.	Talento Humano	**2024-2027**				

11. REFERENCIAS

Los conceptos especificados en los términos y condiciones fueron tomados de las siguientes referencias:

1. Modelo de Seguridad y Privacidad de la Información – MinTIC, https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf
2. Norma Técnica Colombiana NTC-ISO/IEC 27000:2018, NTC-ISO/IEC 27001:2022,NTC-ISO/IEC 27002:2022, ISO /IEC 27032:2012
3. Glosario MinTIC, https://www.mintic.gov.co/portal/inicio/Glosario/
4. Ley 1712 de 2014.
5. Ley 1581 de 2012.