PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IMTRAC 2024

1. INTRODUCCIÓN

La nueva Política de Gobierno Digital tiene como uno de sus habilitadores la Seguridad y Privacidad de la información. Esto con el fin de desarrollar y adoptar todos los mecanismos que garanticen salvaguardar los activos de información. El MINTIC ha establecido que para proteger los activos de información y garantizar su disponibilidad, integridad y confidencialidad debe adoptarse y aplicarse el Modelo de Seguridad y Privacidad de la información.

De acuerdo a lo establecido por MINTIC, el Decreto 2573 de 2014, el Decreto 1078 de 2015 Decreto Único Sectorial y el Decreto 1008 de 14 de Jun 2018, Art.2.2.9.1.2.1 estructura, donde sus componentes son:

"TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las tecnologías de la información y las comunicaciones.

TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el estado, en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño, conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común."

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procesos referentes a la seguridad de la información y recursos, todos los servidores público, están en cumplimiento de sus funciones expuestos a riesgos que puedan hacer fracasar una gestión; por tal razón es necesario tomar medidas para identificar las causas y consecuencias de la materialización de dichos riegos.

El presente documento contiene el Plan de Seguridad y Privacidad de la información para el Instituto Municipal de Transportes y Tránsito de Corozal -IMTRAC-, orientado por un conjunto de actividades basadas en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar las actividades del Plan de Seguridad y Privacidad de la Información alineadas con la NTC/IEC ISO 27001:2013, la estrategia de gobierno digital, la Política de Seguridad Digital y Continuidad del servicio, para fortalecer el aseguramiento de los servicios de TI y la información que se genera u obtiene en el Instituto Municipal de Transportes y Tránsito de Corozal, para preservar la confidencialidad, integridad y disponibilidad de la información, en cumplimiento de las disposiciones legales vigentes y así asegurar la adopción integral del Modelo de Seguridad y Privacidad de La Información (MSPI) con un enfoque de mejora continua.

2.2 OBJETIVOS ESPECIFICOS

● Establecer un cronograma fundamentado en el ciclo de mejora continua para la adopción completa del MPSI en el IMTRAC.
● Realizar un análisis y valoración de los riesgos de seguridad de la información en cuanto al impacto y la probabilidad de ocurrencia para el IMTRAC.
● Ejecutar actividades en el marco de una metodología de gestión de la seguridad, para establecer un modelo de madurez aplicable y repetible en el IMTRAC.
● Implantar medidas de ejecución y de verificación de los controles previstos dentro del MPSI con base en los riesgos identificados de seguridad de la información en el IMTRAC.

3. CONTEXTO NORMATIVO

El Estado colombiano cuenta con normatividad vigente que obliga el adecuado tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

• Resolución 500 del 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
• Ley 1437 de 2011, Capítulo IV, “utilización de medios electrónicos en el procedimiento administrativo”.
• Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales”.
• Ley 1712 de 2014. “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.”
• Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado: de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
• Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012
• Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
• Decreto 2573 de 2014. “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea…” donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.
• Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
• Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
• Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

• NTC / ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

• NTC/ISO 27002:2013 Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

• Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

• Decreto 1083 de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, ("11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital).

• CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

• CONPES 3854 de 2016. Política de Seguridad Digital del Estado Colombiano.

• Decreto 1413 de 2017, artículo 2.2.17.6.6, "Seguridad de la información".

• Guía para la administración de los riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública – DAFP.

• CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.

• Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

4. ALCANCE

Este documento es aplicable a los procesos estratégicos, misionales, de apoyo y de evaluación del IMTRAC todos servidores, contratistas, proveedores y terceros que, en cumplimiento de sus funciones utilicen, recolecten, procesen, intercambien, consulten y en general participen en el ciclo de vida de la información institucional, apuntado a proteger y preservar la integridad, confidencialidad y disponibilidad de los activos de información del instituto.

5. DEFINICIONES

A continuación, se definen los términos esenciales para comprender el Plan de Seguridad y Privacidad de la Información, así mismo los contemplados en la Norma

ISO 27001. (ISO/IEC 27000), igualmente se toman como referencia los términos y definiciones establecidos en la Norma NTC-ISO/IEC 27000, Norma NTC-ISO/IEC 27005, Norma NTC-ISO/IEC 31000 y la Guía # 7 Gestión de Riesgos del Modelo de Seguridad y Privacidad de la Información:

Acceso a la Información Pública: derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

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

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

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

Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.

Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software),

redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

Confiabilidad de la Información: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones.

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.

Datos Abiertos: son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012).

Derecho a la Intimidad: derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

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.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una

organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma técnica NTC-ISO/IEC 27001:2013.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante los clientes.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros: pérdida de reputación, implicaciones legales, etc.

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.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. La información de la Superintendencia Nacional de Salud debe ser clara y completa, y solo podrá ser modificada por el personal expresamente autorizado para ello. La falta de integridad de la información puede exponer a la empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas económicas.

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. (Ley 1712 de 2014, art 6).

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 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Integridad: es la protección de la exactitud y estado completo de los activos de información.

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.

Probabilidad: Medida para estimar la ocurrencia del riesgo.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Recursos de tratamiento de la información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Responsable de Seguridad Informática: En la Alcaldía existe un comité de seguridad de la información será el grupo encargado de realizar el seguimiento y monitoreo al sistema de Gestión de la Seguridad de la información (SGSI) cuando este implementado.

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.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Selección de controles: Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de la Seguridad de la Información: 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 del riesgo y de mejora continua.

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

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

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

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. ESQUEMA DEL PLAN

El Plan de Seguridad y Privacidad de la Información es la declaración general que representa la posición del Instituto Municipal de Transportes y tránsito de Corozal con respecto a la protección de los activos de información que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

7. DESARROLLO METODOLÓGICO

De acuerdo con el contexto institucional y la metodología definida en el Modelo de Seguridad y Privacidad de la Información – MSPI, se contempla la operación del Subsistema de Gestión de Seguridad de la Información y seguridad digital basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten gestionar y mantener adecuadamente la seguridad y privacidad de los activos de información.

Fase 1- Diagnóstico. Su objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Determinar el estado actual de la gestión de

seguridad y privacidad de la información al interior del IMTRAC, Utilizando la Herramienta de Diagnostico brindada por el MINTIC.

Fase 2- Planificación. Se determinan las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta el mapa de procesos y en general el contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

Fase 3- Operación. En esta fase se Implementan los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación. La información del IMTRAC, debe ser es decisiva para el desarrollo de sus procesos, su correcto desempeño dentro de la política y su relación con el ciudadano, es por ello que debe ser protegida de cualquier posibilidad de salida de eventos de riesgo de seguridad de la información y que pudiese parecer un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la entidad.

Fase 4 – Evaluación de desempeño. Determina el sistema y forma de evaluación de la adopción del modelo en el IMTRAC. El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Fase 5 – Mejoramiento Continuo. Establece procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición. En esta fase el IMTRAC debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

7. PLAN DE IMPLEMENTACION DEL MSPI

De acuerdo al diagrama de operación del Modelo de Seguridad y Privacidad de la Información, se realiza el siguiente Plan de implementación, el cual comprende el siguiente cronograma y se le hace seguimiento mes a mes:

Identificar el nivel de madurez de seguridad y privacidad de la información en que se encuentra la Entidad, como punto de partida para la implementación del MSPI.

Establecer las funciones de seguridad y privacidad de la información.

Establecer roles y responsabilidades asociadas a la seguridad y privacidad de la información.

Definir el formato para el levantamiento de activos de información de las Dependencias.

Publicación y Registros activos de información ley 1712.

Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información
Implementar los planes y controles para lograr los objetivos del MSPI Realizar auditorías con el fin de obtener información sobre el cumplimiento del MSPI.

Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

8. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

El IMTRAC evaluará el plan de seguridad y privacidad de la información, por medio de un monitoreo esencial para revisar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo anual o en el momento que se determine, debe estar a cargo de los responsables de los procesos, el jefe de Control Interno director del IMTRAC, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.