Centro De Diagnóstico Automotor

De Caldas Limitada

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Manizales 2022-2026

Centro De Diagnóstico Automotor De Caldas Limitada
Av. Kevin Ángel Calle 63-77 Manizales (Caldas) / Tel: 875 28 28
www.cdac.gov.co

**CONTENIDO**

## Contenido

## HOJA DE AUTORIZACIONES

| Elaboró: | Revisó: | Aprobó: |
|---|---|---|
| **Christian Felipe Martínez Meza**<br>**Juan David Galvis Cano** | | |

## REVISIONES Y MODIFICACIONES

| No. Revisión | Apartado Modificado | Página(s) Modificada | Naturaleza del Cambio | Motivo del cambio | Fecha de Vigencia | Elaboró | Aprobó |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |

## INTRODUCCIÓN

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2; como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual, se ha articulado con el Modelo Integrado de Planeación y Gestión como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

El Manual de Política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Según el manual, la implementación de la política de Gobierno Digital se ha definido en dos componentes: TIC para el Estado y TIC para la sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información,

Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos, se desarrollan a través de lineamientos y estándares que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

El manual en mención, precisa que el habilitador de 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, disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la información –MSPI-.

No obstante, el manual está amparado en el Decreto 1008 del 2018, que en su artículo 2.2.9.1.1.3 define que la política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos adoptados en Colombia, en particular, al principio de Seguridad de la Información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano.

El documento denominado Modelo de Seguridad y Privacidad de la Información – MSPI, expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción del mismo, por las entidades del Estado, conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2., en el numeral 2, en los literales A, B y C, el cual debe ser planificado en atención a lo establecido en el decreto 612 de 2018, que en el artículo 1 señala la importancia de la integración de los planes institucionales y estratégicos al Plan de Acción institucional, en el ámbito de aplicación del modelo integrado de planeación y gestión.

## OBJETIVO

Establecer un marco de acción para la implementación del Modelo de Seguridad y Privacidad de la Información, en atención al contexto organizacional de la entidad, las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

## ALCANCE

La adopción del Modelo de Seguridad y Privacidad de la Información, para la vigencia 2021, se enfocará en fortalecer la implementación de acciones de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados a la seguridad informática de la plataforma tecnológica del Centro de Diagnostico Automotor de Caldas, teniendo en cuenta las capacidades y recursos disponibles para mejorar la confianza de los ciudadanos,usuarios, socios y demás partes interesadas.

## PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Centro de Diagnóstico automotor de Caldas ha adoptado la Política de Seguridad de la Información como parte del sistema integral de gestión. Para lograr su implementación y fortalecimiento, ha diseñado un conjunto de planes orientados a avanzar en diferentes actividades, para dar cumplimiento a las orientaciones del Ministerio de Tecnologías de Información y de las Comunicaciones, en cuanto a la adopción e implementación del modelo de seguridad y privacidad de la información.

Para viabilizar una propuesta, se ha organizado un plan maestro de implementación que define el conjunto de planes que se deben ejecutar para fortalecer las acciones encaminadas a la implementación de la Política de seguridad de la información, como habilitador fundamental, para dar cumplimiento a lo estipulado en la Política de Gobierno Digital.

Así mismo, en atención, tanto a lo especificado en el modelo de seguridad y privacidad, como lo estipulado en el estándar NTC ISO 27001:2013, se aborda la identificación, valoración, tratamiento y gestión de riesgos de seguridad digital, como parte fundamental del modelo y en cumplimiento en lo dispuesto en la Política de Seguridad Digital.

A continuación, se presenta el Plan Maestro para la fortalecer la implementación del modelo de seguridad y privacidad del Centro de Diagnostico Automotor de Caldas, enfocado desde la Seguridad Informática.

| PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | |
|---|---|
| **NO.** | **DESCRIPCIÓN DE LA ACTIVIDAD** |
| 1 | Realizar Diagnóstico del Modelo de Seguridad y Privacidad de la Información. |
| 2 | Identificación, clasificación, valoración y asignación de responsables de Activos de Información (Software, Hardware, Redes y Telecomunicaciones, Servicios de Tecnologías de Información y de las Comunicaciones, Soportes, Servicios de Tecnologías de Información y de las Comunicaciones contratados). |
| 3 | Identificación, valoración y tratamiento de riesgos de Seguridad Digital desde el Componente de Seguridad Informática. |
| 4 | Gestión de Incidentes de Seguridad Informática. |
| 5 | Apropiación de la Seguridad Informática. |
| 6 | Implementación de Controles de Seguridad Informática. |
| 7 | Implementación de acciones para la continuidad de la seguridad informática, de la infraestructura y servicios de tecnologías de información. |
| 8 | Definir lineamientos para la Seguridad Informática e infraestructura tecnológica de los servicios de tecnologías de información y comunicaciones, que la entidad adquiera en la Nube. |
| 9 | Acciones para apoyar la transición de IPv4 a IPv6 de la plataforma tecnológica de la entidad. |

Los responsables adelantarán las actividades concernientes con el propósito de aportar al fortalecimiento del modelo de seguridad y privacidad de la información empresarial.