

# **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**Enero - 2021**



**MOVILIDAD SEGURA  
Y SOSTENIBLE**



**iCDAV evoluciona por TIC!**

## CONTENIDO

<b>1. INTRODUCCION .....</b>	<b>2</b>
<b>2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION .....</b>	<b>2</b>
<b>3. POLÍTICA DE GOBIERNO DIGITAL: TIC PARA LA GESTIÓN.....</b>	<b>2</b>
<b>4. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. ....</b>	<b>6</b>
<b>5. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>6</b>
<b>6. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....</b>	<b>6</b>

## 1. INTRODUCCION

El Centro de Diagnóstico Automotor del Valle Ltda. (CDAV), reconoce y declara la información como un activo que tiene valor y el cual es indispensable para la consecución de los objetivos definidos por la estrategia de Gobierno de la Entidad, por esta razón, es necesario establecer un plan en el cual se asegure que la información administrada, generada y custodiada es protegida y tratada de una manera adecuada, independientemente de la forma en la que la misma ésta sea procesada, transportada y/o almacenada en medio físico o digital.

Este documento describe el plan de seguridad y privacidad de la información definido por el Centro de Diagnóstico Automotor del Valle Ltda., con base en la Norma ISO/IEC 27001 y las recomendaciones establecidas en el estándar ISO/IEC 27002.

La Privacidad y Seguridad de la Información es una prioridad para la Entidad y por lo tanto, es responsabilidad de todos sus servidores públicos, proveedores y contratistas velar porque todas las actividades que realizan cumplan con la esencia y el espíritu de cada una de sus políticas.

Teniendo en cuenta lo anterior, se elabora el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, elaborando el Plan de implementación de Seguridad y Privacidad de la Información al interior del Centro de Diagnóstico Automotor de Valle Ltda. (CDAV), aprobado mediante acta de Comité Institucional de Gestión y Desempeño del 29 de enero de 2021.

## 2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Establecer y dar a conocer las actividades que se contemplaran en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001, la Política de Gobierno Digital del CDAV.

## 3. POLÍTICA DE GOBIERNO DIGITAL: TIC PARA LA GESTIÓN

La Política de Gobierno Digital: TIC para la Gestión es la declaración general que representa la posición de la gerencia del **Centro de Diagnóstico Automotor del Valle Ltda.**, con respecto a la protección de los activos de información (servidores públicos, contratistas y proveedores, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la entidad y apoyan la implementación del **Modelo de Seguridad y Privacidad de la Información (MSPI)**, por medio de la generación y publicación de las políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de dicho modelo, lo que garantiza que la Entidad trabaje para promover la cultura de movilidad, seguridad vial y respeto por el medio ambiente; a través de la

formación y evaluación de la capacidad de conducción, revisión del estado de los vehículos, servicios y programas de tránsito y transporte<sup>1</sup>.

El **Centro de Diagnóstico Automotor del Valle Ltda.**, para asegurar la dirección estratégica de la entidad, establece la compatibilidad de la política y los objetivos del Modelo de seguridad de la información y Gobierno Digital: TIC para la Gestión con los objetivos institucionales, en donde, los objetivos del Modelo corresponden a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad y privacidad de la información.
- Cumplir con los principios de la función pública.
- Mantener la confianza de los servidores públicos, contratistas y proveedores.
- Apoyar la innovación tecnológica.
- Implementar el Modelo de seguridad y privacidad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información y de Gobierno Digital: TIC para la Gestión.
- Fortalecer la cultura de seguridad de la información y de Gobierno Digital: TIC para la gestión en los servidores públicos, contratistas y terceros del **Centro de Diagnóstico Automotor del Valle Ltda.**
- Garantizar la continuidad en la prestación del servicio a través de la mejora de la eficiencia e incremento de la capacidad de los servicios de movilidad y seguridad vial.

## ALCANCE/APLICABILIDAD

Esta política aplica a todos los servidores públicos, contratistas y proveedores del **Centro de Diagnóstico Automotor del Valle Ltda.**, y la ciudadanía en general.

## NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento al 100% de la presente política.

El **Centro de Diagnóstico Automotor del Valle Ltda.**, ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros enfocados a las necesidades de movilidad y seguridad vial, en el cumplimiento de las funciones de la **Entidad**, y a los requerimientos regulatorios que le aplican por su naturaleza.

A continuación, se establecen las políticas de seguridad (10) que soportan el Modelo Seguridad y Privacidad de la Información del Centro de Diagnóstico Automotor del Valle Ltda.:

- 1) Política para dispositivos móviles
- 2) Política para teletrabajo
- 3) Política para control de acceso
- 4) Política para controles criptográficos
- 5) Política para seguridad física y del entorno
- 6) Política para escritorio y pantalla limpia
- 7) Política para transferencia de información
- 8) Política para desarrollo seguro
- 9) Política para relaciones con proveedores
- 10) Política para privacidad y protección de datos personales

El cumplimiento de estas políticas garantizará que:

- Las responsabilidades frente a la seguridad de la información y al Gobierno Digital: TIC para la Gestión serán definidas, compartidas, publicadas y aceptadas por cada uno de los servidores públicos, contratistas y proveedores.
- La **Entidad** protegerá la información generada, procesada y/o resguardada por los procesos en la prestación de los servicios de movilidad y seguridad vial y en el cumplimiento de las funciones del **Centro de Diagnóstico Automotor del Valle Ltda.**, y de activos de información que hacen parte de estos.
- La **Entidad** protegerá la información creada, procesada, transmitida y/o resguardada por los procesos en la prestación de los servicios de movilidad y seguridad vial y en el cumplimiento de las funciones del **Centro de Diagnóstico Automotor del Valle Ltda.**, con el fin de minimizar impactos financieros, operativos y/o legales debido a un uso incorrecto de esta. Para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad y/o en custodia.

- La **Entidad** protegerá su información de las amenazas originadas por parte del personal custodio, responsable o usuario de esta.
- La **Entidad** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La **Entidad** controlará la operación de sus procesos misionales, garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La **Entidad** implementará el control de acceso a la información, sistemas y recursos de red.
- La **Entidad** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La **Entidad** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad y privacidad de la información.
- La **Entidad** garantizará la disponibilidad de sus procesos en la prestación de los servicios de movilidad y seguridad vial y en el cumplimiento de las funciones de esta y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La **Entidad** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas. El incumplimiento a la Política de Gobierno Digital: TIC para la Gestión, traerá consigo, las consecuencias legales que apliquen a la normativa de esta, incluyendo lo establecido en las normas que competen al Gobierno Nacional y territorial en cuanto a Seguridad, Privacidad de la Información y Gobierno Digital se refiere.
- La **Entidad** garantizará a la ciudadanía el cumplimiento de la presente política a través de la gestión de los objetivos institucionales, los cuales se encuentran desarrollados en torno a: Reestructurar el proceso comercial y de servicio al cliente, Fortalecer la infraestructura interna y externa aportando a la movilidad y a la seguridad vial, Potencializar la rentabilidad de la empresa, Renovar nuestra tecnología y automatizar procesos, Fomentar una cultura de orientación al resultado, Fortalecer el talento humano, orientados a la prestación del servicio y seguridad de la información de la misma.

La Política de Seguridad Digital adoptada por el **Centro de Diagnóstico Automotor del Valle Ltda.**, estará regida por los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), acorde a lo incorporado en el documento CONPES 3854 de 2016 y la definición de figura de enlace territorial para la implementación de dicha política, así como las instancias respectivas para la articulación con el Coordinador Nacional de Seguridad Digital, acorde a lo dispuesto en el documento Modelo Integrado de Planeación y Gestión (MIPG).

#### **4. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.**

Aplica a todos los niveles del Centro de Diagnóstico Automotor del Valle Ltda., a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del CDAV 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 el CDAV, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

#### **5. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**

Las funciones del comité de Seguridad de la Información son asumidas por el Comité Institucional de Gestión y Desempeño.

#### **6. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.**

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes.

LITERAL	OBJETO QUE SE PRETENDE ALCANZAR DE ACUERDO A PROPUESTA	ACCIONES	RESPONSABLE	FECHA DE INICIO	FECHA FINAL
<b>OBJETIVOS</b>					
a	Diagnostico	Identificar las evidencias asociadas a la gestión de seguridad y privacidad de la información para aspectos administrativos y técnicos	Direccion de Tecnologia	mar-21	mar-21
b	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad	Identificar las brechas existentes frente a cada uno de los aspectos evaluados			
c	Determinar el nivel de madurez de los controles de seguridad de la información	Evaluar los aspectos administrativos y técnicos requeridos dentro del instrumento de evaluación MSPI que determinan el nivel de cumplimiento			
d	Identificar el avance de la implementación del ciclo de operación al interior de la entidad	Establecer las buenas prácticas implementadas en relación con ciberseguridad	Direccion de Tecnologia	mar-21	abr-21
f	Identificación del uso de buenas prácticas en ciberseguridad				
e	Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales	Identificación de las actividades y avances realizados en torno a la protección de datos personales.  Valoración de avances, gestión y evidencias de cumplimiento frente a los requisitos de protección de datos personales.  Identificación de brechas en relación a los requisitos de cumplimiento establecidos en el marco normativo de protección de datos personales.	Direccion de Tecnologia	Abr-21	abr-21
<b>PLANIFICACIÓN</b>					
a	Revisar la política de seguridad y privacidad de la información, reflejada en un documento de alto nivel, para guiar a la Alta Dirección de la Entidad en la implementación del Modelo de Seguridad y Privacidad de la Información	Revisar la política general para la seguridad y privacidad de la información	Direccion de Tecnologia	Abr-21	may-21
b	Revisar las Políticas de Seguridad y Privacidad de la Información	Revisar las políticas requeridas por la organización en alineación con los requisitos establecidos en el MSPI de MINTIC	Direccion de Tecnologia	may-21	may-21
c	Establecer procedimientos de Seguridad de la Información (Desarrollar o revisar los procedimientos que permitan gestionar la seguridad de la información, enfocados a las vulnerabilidades de los procesos definidos en la entidad)	Identificar la existencia de procedimientos, practicas, actividades relacionadas con gestión de vulnerabilidades	Direccion de Tecnologia	may-21	jun-21
		Desarrollar o actualizar los procedimientos asociados a la gestión de vulnerabilidades	Direccion de Tecnologia	jun-21	oct-21
d	Roles y Responsabilidades de Seguridad y Privacidad de la Información	Elaborar y gestionar el acto administrativo que permita crear o mejorar la distribución de roles y responsabilidades	Direccion de Tecnologia	ago-21	ago-21
e	Inventario de activos de información	Revisar la metodología de identificación y valoración de activos de información	Direccion de Tecnologia	sep-21	oct-21
		Actualizar el inventario de activos de información	Direccion de Tecnologia	nov-21	dic-21