MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

1. PRÓLOGO

En el contexto actual de transformación digital y crecimiento exponencial de las amenazas cibernéticas, la Dirección de Tránsito de Bucaramanga reconoce la necesidad imperiosa de implementar mecanismos sólidos y estructurados para proteger su infraestructura tecnológica, sus sistemas críticos y la información que administra. Este modelo responde a ese compromiso, siendo una herramienta fundamental para salvaguardar la confidencialidad, integridad y disponibilidad de los datos, así como para garantizar la continuidad en la prestación de servicios digitales de movilidad. El presente documento está alineado con las buenas prácticas internacionales, la normatividad colombiana y los lineamientos internos definidos en los procedimientos y políticas institucionales vigentes.

2. INTRODUCCIÓN

La Dirección de Tránsito de Bucaramanga es una entidad pública encargada de la regulación, control y gestión de la movilidad en la ciudad. Su función principal es garantizar la seguridad vial, el cumplimiento de las normas de tránsito y la prestación de servicios relacionados con la movilidad, tales como la expedición de licencias de conducción, la administración del parque automotor y la regulación del transporte público.

Dado su papel crítico en la movilidad urbana y la alta dependencia de los sistemas de información para la gestión de trámites y procesos administrativos, es fundamental contar con un Modelo de Seguridad de la Información y Ciberseguridad que garantice la protección de los activos digitales, minimice los riesgos cibernéticos y fortalezca la confianza de los ciudadanos en la seguridad de los datos y servicios electrónicos de la entidad.

3. OBJETIVO DEL MODELO

Estructurar un Modelo de Seguridad de la Información y Ciberseguridad basado en

lineamientos de buenas prácticas y estándares nacionales, con el fin de proteger y minimizar los riesgos sobre los activos de información de la Dirección de Tránsito de Bucaramanga. Este modelo permitirá garantizar la disponibilidad, integridad y confidencialidad de la información, brindando credibilidad y confianza a la ciudadanía en los servicios de movilidad.

4. PRINCIPIOS FUNDAMENTALES DEL MODELO

- **Confidencialidad:** Garantizar que la información solo sea accesible por personal autorizado.
- **Integridad:** Asegurar la exactitud y confiabilidad de los datos, evitando alteraciones no autorizadas.
- **Disponibilidad:** Garantizar que los sistemas y servicios de movilidad estén operativos y accesibles en todo momento.
- **Autenticidad:** Verificar la identidad de los usuarios para evitar suplantaciones.
- **Trazabilidad:** Registrar todas las acciones sobre los sistemas de información para auditorías y control.

5. DEFINICIONES

- **Seguridad de la Información:** Conjunto de medidas, políticas y controles destinados a proteger la confidencialidad, integridad y disponibilidad de la información, asegurando su correcto uso y evitando accesos no autorizados.
- **Ciberseguridad:** Disciplina enfocada en la protección de sistemas informáticos, redes y datos frente a ataques cibernéticos, vulnerabilidades y riesgos tecnológicos.
- **Activo de Información:** Cualquier recurso de valor para la entidad,

incluyendo bases de datos, sistemas informáticos, plataformas digitales, documentos electrónicos y dispositivos tecnológicos.

- **Gestión de Riesgos:** Proceso sistemático para identificar, analizar y mitigar amenazas que pueden afectar la seguridad de los activos de información.

- **Política de Seguridad de la Información:** Documento que define los lineamientos, principios y directrices que rigen la protección de la información dentro de la entidad.

- **Plan de Tratamiento de Riesgos:** Estrategia que describe las acciones correctivas y preventivas para reducir la exposición a amenazas y garantizar la seguridad de la información.

- **Gestión de Identidades y Accesos (IAM):** Conjunto de procesos y tecnologías para garantizar que solo los usuarios autorizados puedan acceder a sistemas y datos críticos.

- **Respaldo y Recuperación de Datos:** Estrategias y procedimientos para realizar copias de seguridad y restaurar información en caso de pérdida, daño o ataque cibernético.

- **Incidente de Seguridad:** Evento que compromete la confidencialidad, integridad o disponibilidad de los sistemas de información, incluyendo accesos no autorizados, malware o fugas de datos.

- **Procedimiento de Gestión de Incidentes:** Protocolo establecido para detectar, responder y mitigar incidentes de seguridad en la entidad.

- **Continuidad del Negocio:** Conjunto de medidas y planes que garantizan la operatividad de los sistemas de tránsito y movilidad en caso de fallos tecnológicos o ataques cibernéticos.

- **Autenticación Multifactor (MFA):** Método de seguridad que requiere dos o más factores de verificación (contraseña, token, biometría) para

conceder acceso a sistemas sensibles.

- ❖ **Phishing:** Técnica de ciberdelincuencia que busca engañar a usuarios mediante correos electrónicos o mensajes fraudulentos para robar credenciales o información confidencial.
- ❖ **Firewall:** Dispositivo o software de seguridad que monitorea y controla el tráfico de red para prevenir accesos no autorizados.
- ❖ **Auditoría de Seguridad:** Evaluación sistemática de las políticas, procedimientos y controles de seguridad de la información para detectar vulnerabilidades y garantizar el cumplimiento normativo.

6. CICLO DE OPERACION

- **Identificación de Activos:** Se identifican los sistemas, datos y recursos críticos de la entidad.
- **Análisis de Riesgos:** Se evalúan amenazas y vulnerabilidades que podrían afectar la seguridad de la información.
- **Implementación de Controles:** Se aplican medidas de seguridad para mitigar riesgos.
- **Monitoreo y Detección:** Se supervisa la infraestructura en busca de anomalías o intentos de ataque.
- **Respuesta a Incidentes:** Se activan protocolos de mitigación ante eventos de seguridad.
- **Mejora Continua:** Se ajustan y optimizan los controles con base en auditorías y nuevos riesgos.

7. ACTIVIDADES CLAVE DE LA FASE DE DIAGNOSTICO

1. **Identificación y Clasificación de Activos de Información**
2. **Evaluación de Controles de Seguridad Existentes**
3. **Análisis de Riesgos y Vulnerabilidades**
4. **Evaluación de Cumplimiento Normativo**
5. **Documentación del Estado Actual de la Seguridad de la Información**

8. LINEAMIENTOS Y BUENAS PRACTICAS

Este modelo se basa en los documentos oficiales de la Dirección de Tránsito de Bucaramanga para establecer lineamientos claros en la seguridad de la información y ciberseguridad.

8.1 Marco Normativo y Estándares de Seguridad

El modelo de gestión sigue los lineamientos de las políticas internas y normativas nacionales e internacionales, incluyendo:

- POL-GTIC-002 Política de Seguridad de la Información
- Plan de Seguridad y Privacidad de la Información
- Plan de Tratamiento de Riesgos
- PR-GTIC-009 Procedimiento de Atención y Solución a Incidentes en Plataforma
- PR-GTIC-005 Procedimiento de Solicitud y Uso de Activos de Información

- PR-GTIC-014 Continuidad de los Servicios Tecnológicos

8.3. Protección de Activos de Información

- Clasificación de la Información: Identificación de datos sensibles relacionados con trámites de tránsito.
- Gestión de Accesos y Privilegios: Aplicación de controles de identidad, autenticación multifactor y monitoreo.
- Respaldo y Recuperación de Datos: Copias de seguridad según FT-GTIC-013.
- Seguridad en Infraestructura: Firewalls, segmentación de red y encriptación.

8.4. Gestión de Riesgos y Ciberseguridad

- Plan de Tratamiento de Riesgos.
- Monitoreo y Respuesta a Incidentes.
- Actualización de Sistemas con PR-GTIC-006.

8.5. Continuidad de Servicios Tecnológicos

- Planes de contingencia.
- Recuperación ante desastres.
- Pruebas de resiliencia.

8.6. Capacitación y Cultura de Seguridad

- Sensibilización sobre riesgos digitales.
- Capacitación en procedimientos.
- Simulacros de seguridad.

- Formación continua en temas de Gobierno Digital, Seguridad y Privacidad de la Información, dirigida a funcionarios, contratistas y terceros vinculados con la entidad.

9. Implementación del Modelo

La ejecución del modelo se realizará en fases progresivas, integrando medidas de control y estrategias de mejora continua:

1. **Diagnóstico y Evaluación Inicial:** Identificación del estado actual de la seguridad de la información en la Dirección de Tránsito de Bucaramanga.
2. **Diseño y Adopción de Políticas:** Implementación de normativas internas de seguridad digital y planes de protección de datos.
3. **Despliegue de Controles de Seguridad:** Aplicación de medidas técnicas y organizativas para mitigar riesgos.
4. **Monitoreo y Auditoría:** Evaluaciones regulares y auditorías de cumplimiento en seguridad informática.
5. **Mejora Continua:** Revisión y actualización constante del modelo para adaptarse a nuevas amenazas y tecnologías.

10. Modelo de Gestión de Seguridad de la Información y Ciberseguridad

10.1. Política de Seguridad de la Información y Ciberseguridad

La Dirección de Tránsito de Bucaramanga debe establecer y documentar una Política de Seguridad de la Información y Ciberseguridad, la cual debe ser aprobada por la Junta Directiva de la entidad. La política debe ser aprobada y divulgada al interior de la Dirección.

Directrices para la Seguridad de la Información y la Ciberseguridad Estas directrices estarán definidas en el manual de políticas institucionales (POL-GTIC-001), que garantizará el adecuado uso de activos de información al interior de la Dirección de Tránsito de Bucaramanga; definiendo responsabilidades generales y específicas para la gestión de la seguridad de la información y la ciberseguridad.

Roles y Responsabilidades de Seguridad de la Información y Ciberseguridad
La Dirección debe definir los roles y las responsabilidades para la Seguridad de la Información y Ciberseguridad en los diferentes niveles (directivo, de procesos y operativos) conforme a lo estipulado en el PR-GTIC-005 Procedimiento Solicitud y Uso de Activos de Información, que permita la correcta toma de decisiones y una adecuada gestión para el cumplimiento de los objetivos institucionales.

10.2. Procedimientos de Seguridad de la Información y Ciberseguridad

Los siguientes procedimientos, contemplados dentro del marco del Modelo de Gestión de la Dirección de Tránsito de Bucaramanga, se formalizan en conformidad con los documentos PR-GTIC-009, PR-GTIC-005, POL-GTIC-001, entre otros:

10.2.1. Seguridad de los Recursos Humanos

Propósito: Asegurarse de que los funcionarios, contratistas y terceros comprendan sus responsabilidades frente a la seguridad de la información, protegiendo los intereses de la Dirección incluso después de la terminación del vínculo contractual.

Plan de Sensibilización para la Seguridad de la Información y Ciberseguridad: De acuerdo con el PR-GTIC-001 Procedimiento Comunicación y Prensa y el Plan de Gestión de Talento Humano, se debe definir una estrategia integral de capacitación, comunicación y sensibilización en seguridad de la información y ciberseguridad para todos los niveles de la entidad.

10.2.2. Gestión de Activos

Propósito: Identificar los activos de información institucionales y definir responsabilidades para su protección, uso y divulgación según el PR-GTIC-005 y el inventario actualizado definido en la caracterización CP-GTIC-001.

Guía para la gestión de activos de información: El inventario debe estar alineado a las directrices de criticidad, propietarios, custodios y usuarios que permiten clasificar y proteger la información conforme a su importancia institucional.

10.2.3. Riesgos de Seguridad de la Información y Ciberseguridad

Propósito: Establecer un marco de administración de riesgos conforme al POL-GTIC-001 y al procedimiento PR-GTIC-009, que permita identificar amenazas y vulnerabilidades que afecten la confidencialidad, integridad y disponibilidad de la información institucional.

Sistema de Administración de Riesgo de Seguridad de la Información y Ciberseguridad: Deberá establecerse una metodología enfocada en procesos de negocio que identifique, evalúe, trate y haga seguimiento a los riesgos, incluyendo la declaración de aplicabilidad.

10.2.4. Control de Acceso

Propósito: Definir las directrices necesarias para limitar el acceso a la información institucional de forma segura, evitando accesos no autorizados a los sistemas y plataformas utilizadas.

Guía Prevención de Fuga de Información: La Dirección de Tránsito deberá implementar el principio de mínimo privilegio para el acceso a la información sensible, como lo establece el PR-GTIC-005.

Guía de Disposición Final de la Información: Los criterios para la disposición segura de soportes físicos y digitales se regirán por los lineamientos del procedimiento PR-GTIC-008.

Procedimiento Administración de Identidades y Accesos: La creación, modificación y eliminación de usuarios deberá seguir el PR-GTIC-009 y estar alineada con la definición de roles en los sistemas institucionales.

10.2.4.1. Procedimiento de Gestión de Incidentes de Seguridad de la Información

Propósito: Gestionar los incidentes de seguridad de la información y garantizar la correcta comunicación y respuesta, conforme al PR-GTIC-009 Procedimiento Atención y Solución a Incidentes en Plataforma.

El procedimiento debe indicar cómo responder ante un incidente que afecte la disponibilidad, integridad o confidencialidad de la información. Se deben definir claramente los roles, responsabilidades, fases de respuesta, documentación,

recolección de evidencias y, si es necesario, la activación del plan de continuidad del negocio (PR-GTIC-011).

10.2.5. Seguridad Física y del Entorno

Propósito: Prevenir el acceso físico no autorizado a las instalaciones de procesamiento de información, así como el daño, pérdida o robo de activos.

Procedimiento de Seguridad Física y del Entorno: Este procedimiento deberá contemplar el acceso controlado y los mecanismos de protección física descritos en el PR-GTIC-012, incluyendo registro de ingreso, control de visitantes y solicitudes a zonas restringidas.

Protección de Activos: Deberá garantizarse mediante ubicaciones seguras, protección contra riesgos ambientales y medidas contra intrusiones físicas, conforme a lo establecido en el plan de seguridad perimetral.

Retiro de Activos: Se deberán seguir los lineamientos institucionales de control para la salida temporal o definitiva de activos de información, incluyendo su cifrado y control de uso externo, conforme a PR-GTIC-005 y POL-GTIC-001.

11. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información será el órgano encargado de la dirección estratégica, coordinación y seguimiento de las iniciativas en materia de seguridad digital dentro de la Dirección de Tránsito de Bucaramanga. Este comité se reunirá trimestralmente o cuando se presenten incidentes de seguridad relevantes.

Integrantes:

- **Oficina Asesora de Sistemas:** Lidera la estrategia tecnológica y asegura la implementación de controles técnicos.
- **Profesional de Ciberseguridad:** Encargado de identificar vulnerabilidades, evaluar amenazas, ejecutar pruebas de seguridad y liderar la respuesta ante incidentes.

- **Talento Humano:** Coordina los programas de formación y sensibilización sobre seguridad de la información para todos los funcionarios.
- **Jurídica, Planeación y Control Interno:** Asegura el cumplimiento normativo, la planeación estratégica de la seguridad y la ejecución de auditorías de control.
- **Atención al Usuario:** Representa la visión del usuario final y contribuye en la detección temprana de fallos o amenazas reportadas desde los canales ciudadanos.

12. Responsabilidades Clave

- **Oficina Asesora de Sistemas:** Diseñar, aplicar y supervisar los controles técnicos sobre la infraestructura de TI, incluyendo redes, servidores, bases de datos, sistemas críticos y dispositivos de seguridad como firewalls y antivirus.
- **Talento Humano:** Diseñar e implementar programas de capacitación continua en temas de ciberseguridad, políticas institucionales, prácticas seguras de manejo de la información y cultura de prevención.
- **Control Interno:** Verificar el cumplimiento del modelo mediante auditorías internas periódicas, elaboración de planes de mejora y seguimiento a hallazgos.
- **Usuarios:** Adoptar prácticas seguras en el uso de sistemas y datos, incluyendo el cumplimiento de políticas, reportar incidentes de forma oportuna y proteger sus credenciales de acceso.

13. Indicadores de Seguimiento y Evaluación

Para medir la eficacia del modelo se implementarán los siguientes indicadores:

- **Número de incidentes reportados:** Total de eventos de seguridad registrados en un periodo específico.
- **Tiempo de Respuesta ante Incidentes (MTTR):** Promedio de tiempo desde la detección hasta la mitigación completa de un incidente.

- **Porcentaje de funcionarios capacitados:** Relación entre el número de funcionarios formados frente al total del personal activo.
- **Nivel de cumplimiento de controles:** Resultado de auditorías y revisiones técnicas con relación a las políticas y estándares definidos.
- **Frecuencia de actualizaciones de sistemas y parches aplicados:** Porcentaje de infraestructura con software actualizado frente al total instalado.

14. Plan de Actualización y Revisión del Modelo

El modelo será objeto de revisión sistemática para garantizar su vigencia y adaptación a nuevas amenazas y requisitos:

- **Revisión anual:** Evaluación integral del modelo, sus políticas, controles e indicadores.
- **Revisión por eventos relevantes:** Se realizará una actualización cuando se presenten incidentes graves, cambios tecnológicos o modificaciones regulatorias.
- **Inclusión de nuevas tecnologías o riesgos:** Se integrarán nuevas prácticas o herramientas ante la aparición de amenazas emergentes como IA, IoT o ransomware avanzado.
- **Actualización de procedimientos:** Se ajustarán los manuales y formatos operativos relacionados, con sus respectivas socializaciones y capacitaciones.
- **Socialización con funcionarios:** Se garantizará que todos los funcionarios conozcan los cambios mediante comunicados, talleres y actualizaciones en la intranet institucional.

15. Conclusión

El Modelo de Seguridad de la Información y Ciberseguridad para la Dirección de Tránsito de Bucaramanga garantizará la protección de los activos digitales de la entidad y la continuidad de los servicios de movilidad. A través de la implementación de estándares nacionales y mejores prácticas, se busca mitigar los riesgos cibernéticos y fortalecer la credibilidad de la entidad en la prestación de servicios electrónicos seguros y confiables para la ciudadanía

CONTROL DE CAMBIOS						
VERSION	**FECHA DE APROBACIÓN**	**FECHA DE IMPLEMENTACIÓN**	**DESCRIPCION DEL CAMBIO**	**CONSTRUYE O PROYECTA EL DOCUMENTO**	**RECONOCE DOCUMENTO PARA SIG**	**ADMITE DOCUMENTO PARA SIG**
02	27/ 04/ 2026	11/ 02/ 2026	Ajuste del plan por cambio en la normatividad	**MIGUEL ALEXANDER PORTILLA V Jefe Oficina Asesora de Sistemas**	**DIANA CAROLINA SARMIENTO SOLANO Asesor de Calidad**	**SENAIDA TELLEZ DUARTE** Secretaria General Representante de la Alta Dirección ante el SIG

CONTROL DE CAMBIOS			
VERSIÓN	FECHA DE APROBACIÓN	FECHA DE IMPLEMENTACIÓN	DESCRIPCIÓN DEL CAMBIO
01	Noviembre 15 de 2024	Noviembre 15 de 2024	Emisión Inicial.