POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

La política de seguridad de la información está fundamentada en el modelo de seguridad de y privacidad de la información propuesto por el Ministerio de las Tecnologías de la Información y las comunicaciones, el cual recopila las mejores prácticas para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo; lo anterior teniendo en cuenta las necesidades, objetivos, los requisitos de seguridad y los procesos misionales de la Dirección de Transito de Bucaramanga.

Con la adopción de dicha política se pretende lograr la preservación de la confidencialidad, integridad y disponibilidad de la Información, garantizando la privacidad de los datos mediante la aplicación de la gestión del riesgo. De esta forma se da cumplimiento al decreto único reglamentario 1078 de 2015 en el componente de seguridad y privacidad de la Información como parte integral de la estrategia Gobierno Digital. En el entendido de que la información es un activo valioso para la toma de decisiones, la gestión del cambio y el conocimiento, para establecer una política de seguridad de la información que ha de brindar a los usuarios y ciudadanos las herramientas para la defensa de lo público.

Es de vital importancia la gestión del conocimiento y las revisiones de la política que lleven a una mejora continua para lograr un mejor desempeño de las actividades y la articulación de la normatividad Colombiana e internacional en protección de datos, delitos informáticos y seguridad de la información además de tendencias tecnológicas para que puedan ser implementadas entorno a la eficacia de las actividades relacionadas, considerando siempre los tres principios de la seguridad de la información, confidencialidad, disponibilidad e integridad.

2. Alcance

La política en seguridad de la Información cubre todas las áreas de gestión de la DTB las cuales deben ser acatadas tanto por la alta dirección, funcionarios, contratistas y/o terceros que laboren o tengan algún tipo de relación con la Entidad, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

3. Objetivo

Determinar los lineamientos que permitan proteger la Información de la Dirección de Transito de Bucaramanga a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad de acuerdo a la estrategia Gobierno Digital de buenas prácticas en Seguridad y Privacidad para las entidades del Estado, con el fin de regular la gestión de la seguridad de la información al interior de la Entidad. Y asegurar el cumplimiento de la integridad, no repudio, disponibilidad, legalidad y confidencialidad de la información.

3.1. Objetivos Específicos

- Mantener la confianza de los ciudadanos en general y el compromiso de todos los funcionarios, contratistas y/o terceros, respecto al correcto manejo y protección de la información que es gestionada y resguardada en la DTB.
- Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad.
- Atender las necesidades para el cumplimiento de la función administrativa.
- Proteger los sistemas de información y la plataforma tecnológica de la DTB.
- Concientizar a los funcionarios, contratistas y/o terceros sobre el uso adecuado de los sistemas de información puestos a su disposición para la realización de las funciones y actividades diarias, garantizando la confidencialidad, la privacidad y la integridad de la información
- Dar cumplimiento a los lineamientos establecidos en la Estrategia de Gobierno en Digital respecto a la Seguridad de la Información.

4. Política

La DTB decide definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados con la misión, visión y funciones de la Entidad.

La DTB, se compromete a salvaguardar la información que genera en la ejecución de sus funciones o la que le es entregada en custodia por usuarios dentro de la ejecución de los trámites de la DTB, identificando y mitigando los riesgos asociados mediante la definición de lineamientos y directrices a las dependencias, funcionarios, contratistas y todo aquel que tenga interacción con esta información y la utilización físicamente o a través de equipos, plataformas o sistemas de información dispuestos para su gestión y resguardo.

Toda la información que es generada por los funcionarios, contratistas y/o terceros de la DTB en beneficio y desarrollo de las actividades propias de la Entidad son propiedad de la DTB, a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la información que pueda ser adquirida o cedida a la DTB de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la Entidad.

La DTB protege la información creada, procesada, transmitida o resguardada por los procesos de su competencia, su infraestructura tecnológica y activos, del riesgo que se genera con los accesos otorgados a terceros (ej.: contratistas, proveedores o ciudadanos).

La DTB protege la información creada, procesada, transmitida o resguardada por sus procesos de operación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

La DTB protege su información de las amenazas originadas por parte de sus funcionarios, contratistas y/o terceros.

La DTB protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

La DTB controla la operación de sus procesos de operación garantizando la seguridad de los recursos tecnológicos, redes y bases de datos.

La DTB implementa control de acceso a la información, aplicativos, recursos de red, portales y sistemas de información internos y externos o con accesos remotos

La DTB garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La DTB garantiza 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.

La DTB garantiza la disponibilidad de sus procesos de operación y la continuidad de su operación basada en el impacto que pueden generar los eventos.

La DTB garantiza el cumplimiento de las obligaciones legales, regulatorias contractuales establecidas.

Las responsabilidades frente a la seguridad de la información de la DTB son definidas, compartidas, publicadas y deberán ser aceptadas por cada uno de los funcionarios, contratistas y/o terceros.

A este documento podrán integrarse en adelante lineamientos o políticas relativas a la seguridad de la información siempre y cuando no sea contrario a lo expresado en esta política.

5. Compromiso de la alta dirección

La Dirección General de la DTB aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Entidad, teniendo en cuenta el marco general del funcionamiento, sus objetivos institucionales y sus procesos misionales.

La Dirección General de la entidad demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.

- La promoción activa de una cultura de seguridad.

- Facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la Entidad.

- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.

- Monitoreo para determinar la efectividad y cumplimiento de las políticas aquí mencionadas.

- Asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones

6. Políticas para control de acceso

Todos los funcionarios, contratistas y/o terceros que hagan uso de los activos de información de la DTB, tienen la responsabilidad de seguir las reglas establecidas en la presente política y los documentos anexos a la misma, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la continuidad misional de la DTB.

La gestión de usuarios se asignará con previo conocimiento de la oficina asesora de sistemas, por lo tanto, el manejo de documentos, cuentas de correo, accesos a la red, sistemas de información y activos de información es responsabilidad de cada usuario, por lo cual la sensibilización de los usuarios frente a sus responsabilidades ha de ser constante.

La asignación de usuarios y contraseñas es un permiso que la DTB otorga a sus funcionarios, contratistas y/o terceros con el fin de que tengan acceso a los recursos tecnológicos, las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información institucional, teniendo en cuenta:

- Todos los funcionarios, contratistas y/o terceros deben tener conocimiento sobre los riesgos asociados con el uso de las credenciales de acceso (usuario y contraseña) y las consecuencias de exponer de manera inadecuada la identidad ante cualquier tercero, en el entendido que los usuarios y claves asignados a cada funcionarios, contratistas o practicantes son personales e intransferibles.
- Asegurar el correcto manejo de la información privada de la Entidad.
- La asignación de credenciales, usuarios (Login o UserId) y contraseñas (Clave o Password) a los diferentes funcionarios, contratistas y/o terceros así como su desactivación de los sistemas se harán de acuerdo a los procedimientos establecidos y según sea solicitado por la oficina de Recurso Humano y Gestión Contractual.
- Las cuentas de usuario son entera responsabilidad del funcionario, contratista o y/o tercero al que se le asigne. La cuenta y contraseña es para uso personal e intransferible.

- Las cuentas de usuario (usuario y clave) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como se definan.
- De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, debe solicitarlo por escrito y dirigido a la oficina asesora de sistemas.
- Si se detecta o sospecha que las actividades de una cuenta de usuario puede comprometer la integridad y seguridad de la información, el acceso a dicha cuenta será suspendido temporalmente y se reactivara sólo después de haber tomado las medidas necesarias a consideración de la oficina asesora de sistemas.

7. Políticas para el uso del correo electrónico

El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios, contratistas y/o terceros de la DTB, con los siguientes lineamientos:

- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad, por lo tanto, la responsabilidad del contenido es netamente del autor.
- Está prohibido el uso de correos masivos tanto internos como externos.
- Todo mensaje SPAM o CADENA debe ser inmediatamente reportado a la oficina asesora de sistemas, no está permitido el envío y/o reenvío de mensajes que contengan cadenas.
- Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado a la oficina asesora de sistemas,
- Las cuentas de correo institucional no debe ser reveladas en páginas o sitios ajenos a los fines de la Entidad.
- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido distribuir información de la DTB, no pública, a otras entidades o ciudadanos sin la debida autorización de la Dirección General.

8. Políticas para el uso de internet

La DTB establecerá reglas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, previa validación. Para el buen uso de los recursos de navegación de la Entidad se deben tener en cuenta los siguientes lineamientos:

- El uso del servicio de Internet está limitado exclusivamente para propósitos laborales.
- Los servicios a los que un determinado usuario (funcionario, contratista y/o tercero) pueda acceder desde internet dependerán del rol o funciones que desempeña el usuario y para los cuales esté formal y expresamente autorizado.

- Todo usuario es responsable de informar a la oficina asesora de sistemas los contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones.
- Está expresamente prohibido el envío, y/o descarga, y/o visualización, de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas, y/o de procedencia desconocida que puedan causar cualquier tipo de daños en los equipos y redes.
- Está expresamente prohibido acceder a páginas que agredan la ética y el buen comportamiento.
- Está expresamente prohibido acceder a sitios de juegos o apuestas en línea.
- Está expresamente prohibido acceder a sitios de divulgación, descarga o distribución de películas, videos, música, real audio, webcams, emisoras online, etc.
- Está expresamente prohibido acceder y/o descargar material pornográfico u ofensivo.
- Está expresamente prohibido utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por la oficina asesora de sistemas.
- Está expresamente prohibido emplear este servicio para la recepción, envió o distribución de información pública clasificada o reservada de la DTB a través de servicios y cuentas de correo públicos.
- Está expresamente prohibido realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
- Está expresamente prohibido cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.
- Está expresamente prohibido utilizar el servicio de Internet/Intranet para propósitos comerciales ajenos a la DTB.
- Está expresamente prohibido comprar o vender artículos personales a través de sitios web o de subastas en línea.
- Está expresamente prohibido publicar o enviar opiniones personales, declaraciones políticas y asuntos no propios de la DTB, dirigidos a funcionarios, contratistas y/o terceros y público en general, del sector oficial, de otras compañías y organizaciones, a través de este servicio.
- Está expresamente prohibido descargar, instalar y configurar navegadores distintos a los permitidos por la oficina asesora de sistemas
- La DTB a través de la oficina asesora de sistemas, se reserva el derecho de monitorear los accesos, y por tanto el uso del servicio de internet de todos sus funcionarios o contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad.

9. Políticas para la administración de redes y equipos

Los recursos informáticos de la DTB, son elementos de apoyo a las labores y responsabilidades de los funcionarios, contratistas y/o terceros, por esto, su uso está sujeto a las siguientes

directrices:

- Los equipos de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad del funcionario, contratista y/o tercero al cual han sido asignados, y únicamente para el correcto desempeño de las funciones del cargo o de las obligaciones contraídas. Por tanto, no pueden ser utilizados con fines personales o por terceros, no autorizados.
- Sólo está permitido el uso de software licenciado por la entidad y/o aquel que sin requerir licencia sea expresamente autorizado por la Dirección General de la DTB. De la misma manera aplicará para el software que llegue a ser desarrollado dentro de la Entidad.
- Los usuarios no deben mantener almacenados en los discos duros de los equipos de cómputo o discos virtuales de red o discos externos de la Entidad, archivos de video, música e imágenes que no sean de carácter institucional.
- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los recursos informáticos, además se debe tener organizado el puesto de trabajo para evitar incidentes con estos recursos.
- No está permitido por fallas en el suministro eléctrico a los equipos de cómputo, realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información.
- Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, es el personal de la oficina asesora de sistemas.
- Está prohibido utilizar almacenamiento externo no autorizado para almacenar información de la Entidad, si llegaré el caso esto solo debe ser autorizado para el personal de la oficina asesora de sistemas.
- Personal de la oficina asesora de sistemas realizará monitoreo sobre los dispositivos de almacenamientos externos, con el fin de prevenir o detectar fuga de información.
- La pérdida o daño de elementos o recursos informáticos, o de alguno de sus componentes, debe ser informada de inmediato a la oficina asesora de sistemas,
- La pérdida de información o de activos digitales debe ser informada con el detalle de la información extraviada al personal de la oficina asesora de sistemas.
- La oficina asesora de sistemas. es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
- Para poder acceder a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales, estos deben estar autorizados y controlados por la oficina asesora de sistemas.
- Cada vez que el funcionario, contratista y/o tercero no se encuentre en las instalaciones de la DTB, los equipos de cómputo deben quedar apagados, con el fin de evitar el ingreso de personal no autorizo a estos recursos informáticos además de contribuir al uso racional de la energía eléctrica.
- Es responsabilidad de cada funcionario, contratista y/o tercero velar por la seguridad y controlar el acceso exclusivo de los recursos informáticos asignados a su nombre, para

tal fin se recomienda que en cada ocasión que deba ausentarse de su puesto de trabajo el equipo de cómputo sea bloqueado para su ingreso.

- Está prohibido el uso de aplicaciones para el control remoto de equipos de cómputo e igualmente de aplicaciones para video conferencia que no estén autorizados por la oficina asesora de sistemas es responsabilidad de los funcionarios, contratista y/o tercero de la entidad informar cuando se desea hacer uso de estas aplicaciones.
- Se debe evitar guardar documentos en el escritorio de trabajo del sistema operativo optando dichos documentos deberán ser almacenados en carpetas en el disco duro del equipos asignado debidamente organizados de tal forma que se facilite realizar copias de respaldo.

10. Políticas para el uso de software y sistemas de información

Todos los funcionarios, contratistas y/o terceros de la DTB. Son responsables de la protección de la información que acceden y/o procesan y de evitar su pérdida, alteración, destrucción y/o uso indebido, para lo cual se dictan los siguientes lineamientos:

- Las credenciales de acceso a la red y/o recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y/o contratistas no deben revelar éstas a terceros ni utilizar claves ajenas.
- Todo funcionario, contratista y/o tercero es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente o cuando el sistema de in formación así los solicite.
- Todo funcionario, contratista y/o tercero es responsable de los registros y/o modificaciones de información que se hagan desde los activos digitales que estén asignados a su nombre, toda vez que las claves de acceso son de carácter personal e intransferible.
- En ausencia de los funcionarios, el acceso al equipo de cómputo le será inactivado con una solicitud elaborada por el área de recursos humanos dirigida a la oficina asesora de sistemas. Con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. El área de recursos humanos o quien haga sus veces debe reportar las novedades del personal que impliquen la ausencia del mismo y los supervisores de contratos o quien haga sus veces las suspensiones temporales y/o permanentes de los contratistas y/o terceros.
- Cuando un funcionario cesa en sus funciones o culmina la ejecución de su contrato laboral con la DTB, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente previo aviso del área de recurso humano; la información del funcionario serán almacenados en un repositorio de la Entidad.
- Cuando un contratista y/o tercero cesa en sus funciones o culmina la ejecución de un contrato con la DTB, el supervisor del mismo es el encargado informar a la oficina asesora de sistemas. para la suspensión inmediata de los privilegios sobre los recursos informáticos otorgados y la información del funcionario será almacenada en un repositorio de la Entidad.

- Solo las aplicaciones aprobadas por Dirección General de la DTB. serán instaladas o utilizadas en cada dispositivo destinado al procesamiento de información clasificada o sensible, además de garantizar su debida aprobación de uso y licenciamiento de acuerdo a los permisos y controles asignados a los usuarios.

11. Políticas de seguridad física

Hace referencia al tratamiento de amenazas tales como acceso no autorizado, robo, pérdida, daño, entre otros (riesgos físicos y ambientales) que puedan afectar los activos de información, medios de procesamientos y comunicaciones, así como las instalaciones donde se encuentran ubicados. Hace referencia al control de medios extraíbles, control sobre dispositivos a puertos de red y seguridad del entorno.

La Dirección General de la DTB a través de la Secretaria General debe garantizar el control de acceso seguro a las instalaciones al personal autorizado. Se debe establecer un procedimiento que pueda incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso de acceso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por la oficina asesora de sistemas; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha oficina durante su visita al centro de cómputo o los centros de cableado.
- La oficina asesora de sistemas debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.
- La oficina asesora de sistemas debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo.
- La oficina asesora de sistemas debe velar porque los recursos de la plataforma tecnológica de la DTB ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.
- La oficina asesora de sistemas debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- La oficina asesora de sistemas debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

12. Normatividad

La política de seguridad de la información de la DTB se basa en los lineamientos dados por el decreto 1008 de 2018 para la implementación de la estrategia Gobierno Digital, el cual establece el habilitador transversal de seguridad que 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.

La implementación de dicha estrategia, articula toda la normatividad vigente en la ley colombiana en cuanto a delitos informáticos, protección de datos personales y transparencia. Además, vincula los derechos intelectuales sobre desarrollos de aplicativos y el manejo de la información dentro de la entidad.

CONTROL DE CAMBIOS			
VERSIÓN	FECHA DE APROBACIÓN	FECHA DE IMPLEMENTACIÓN	DESCRIPCIÓN DEL CAMBIO
01	Octubre 04 de 2019	Octubre 04 de 2019	Emisión Inicial.