

**ACUERDO MINISTERIAL No. 032 -2017**

**ING. BORIS CÓRDOVA GONZÁLEZ**  
**MINISTRO DE TRANSPORTE Y OBRAS PÚBLICAS**

**CONSIDERANDO:**

- Que;** el artículo 154 de la Constitución de la República, a las ministras y ministros de Estado, además de las atribuciones establecidas en la Ley, les corresponde: "1. Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión".
- Que;** el artículo 227 de la Constitución de la República del Ecuador, señala que la Administración Pública constituye un servicio a la colectividad que se rige, entre otros principios por el de desconcentración eficacia, eficiencia, calidad, jerarquía, coordinación, participación, planificación, transparencia y evaluación.
- Que;** El artículo 17 del Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva, establece que: "Los Ministros de Estado son competentes para el despacho de todos los asuntos inherentes a sus ministerios sin necesidad de autorización alguna del Presidente de la República".
- Que;** el Acuerdo Ministerial 166 de 19 de septiembre de 2013 suscrito por el Secretario Nacional de la Administración Pública, dispone a las entidades de la Administración Pública Central, Institucional y que dependen de la función Ejecutiva, el uso de las Normas Técnicas Ecuatorianas para la Gestión de Seguridad de la Información, que las entidades de la Administración Pública implementarán el Esquema Gubernamental de Seguridad de la Información; y la designación al interior de las instituciones, de un Comité de Seguridad de la Información.
- Que;** el Acuerdo Ministerial No. 090 de 18 de noviembre de 2013, la Arquitecta María de los Ángeles Duarte, entonces Ministra de Transporte y Obras Públicas, dispone la implementación del Esquema Gubernamental de la Seguridad de la Información, y la conformación del



Comité de Gestión de la Seguridad de la Información del Ministerio de Transporte y Obras Públicas.

**Que;** el Acuerdo Ministerial No. 1606 de 17 de mayo de 2016, emitido por la Secretaría Nacional de la Administración Pública, en sus artículos del No. 11 al No. 15 hace referencia a la supresión del Comité de Gestión de Seguridad de la Información, y en su lugar todas las atribuciones y responsabilidades para la ejecución del Esquema de Seguridad de la Información lo asume la Coordinación General de Planificación y Gestión Estratégica.

**Que;** Mediante Decreto Ejecutivo No. 1192, de 22 de septiembre de 2016, el Presidente Constitucional de la República, Economista Rafael Correa Delgado, designó como máxima autoridad del Ministerio de Transporte y Obras Públicas al Ingeniero Boris Córdova González.

**Que;** es necesario fortalecer y reglamentar los procedimientos y mecanismos de supervisión y control que garanticen la efectividad en la gestión de la información institucional en ámbito de competencia del Ministerio de Transporte y Obras Públicas;

En ejercicio de la facultad que le confiere el artículo 154, numeral 1 de la Constitución de la República del Ecuador,

### **ACUERDA:**

## **EXPEDIR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE TRANSPORTE Y OBRAS PÚBLICAS-MTOP**

### **1. PRESENTACIÓN Y OBJETIVOS**

#### **1.1. OBJETIVO**

El objetivo de este documento es definir las Políticas internas de Seguridad de la Información del Ministerio de Transporte y Obras Públicas.

#### **1.2. ALCANCE**

El presente documento contiene las Políticas de Seguridad de la Información del Ministerio de Transporte y Obras Públicas "MTOP"; las mismas establecen lineamientos de actuación para los funcionarios (servidores y trabajadores) que

laboran en la entidad, en relación con los recursos y servicios de información. Cada Política de Seguridad de la Información es una invitación de la entidad a sus funcionarios, personal externo que tenga relación con este Ministerio y proveedores a reconocer la información como uno de sus principales activos y como un motor para el desarrollo organizacional.

Las presentes políticas deberán ser acatadas por todos los funcionarios, personal externo que tenga relación con este Ministerio y proveedores que desempeñen labores o proporcionen algún tipo de servicio al Ministerio de Transporte y Obras Públicas.

### **1.3. SEGURIDAD DE LA INFORMACIÓN**

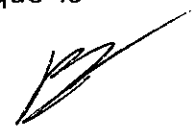
La información es un recurso que tiene un valor importante para el Ministerio de Transporte y Obras Públicas (MTO) y es esencial para las actividades de la institución, por consiguiente necesita una protección adecuada.

La información puede existir en diversas formas. Se puede imprimir o escribir en papel almacenar electrónicamente, transmitir por correo o por medios eléctricos, presentar en películas o expresarse en conversaciones. Cualquiera que sea su forma o medio por el cual se comparte o almacena, siempre debería tener protección adecuada.

La seguridad de la información es la protección de la información, contra una gran variedad de amenazas con el fin de garantizar la continuidad de la Institución, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión del Ministerio.

La seguridad de la información pretende preservar las siguientes características:

- a) **Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- b) **Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- c) **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.



#### **1.4. VIGENCIA**

Las políticas contenidas en el presente documento estarán vigentes desde la fecha de su aprobación y mientras no exista una modificación posterior de las mismas.

#### **1.5. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo que tenga relación con esta Institución y proveedores de MTOP, por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerarse desde acciones administrativas, civiles y hasta penal, de acuerdo con las circunstancias, si así lo ameriten.

### **2. POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN**

La información es uno de los principales activos para el desarrollo de las operaciones y cumplimiento de los objetivos del Ministerio de Transporte y Obras Públicas "MTOP". En consecuencia, la información debe ser protegida de riesgos que afecten su confidencialidad, integridad y disponibilidad.

Los funcionarios, personal externo que tenga relación con este Ministerio, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información del MTOP, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política Global de Seguridad de la Información del Ministerio de Transporte y Obras Públicas "MTOP" se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la entidad. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2005

La Dirección de Tecnologías de la Información tendrá la potestad de modificar la Política Global o las Políticas Específicas de Seguridad de la Información de

acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

## **2.1. POLÍTICA DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

### **2.1.1. Política de Organización Interna**

El Ministerio de Transporte y Obras Públicas, establecerá a los funcionarios un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

### **2.1.2. Política que Rige la Relación con Terceras Partes**

El Ministerio de Transporte y Obras Públicas establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de garantizar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

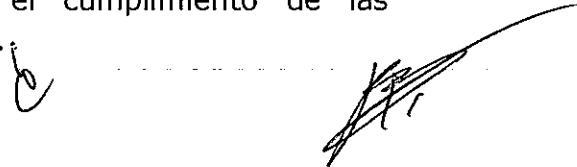
La Coordinación General de Asesoría Jurídica, ha implementado la cláusula de confidencialidad en todos los contratos para terceros cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Institución.

Los funcionarios responsables de la realización y/o firma de contratos o convenios con terceras partes garantizarán la divulgación de las políticas, normas y procedimientos de seguridad de la información.

## **2.2. POLÍTICAS PARA GESTIÓN DE ACTIVOS DE LA INFORMACIÓN**

### **2.2.1. Política de Responsabilidad por los Activos**

El Ministerio de Transporte y Obras Públicas como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.



### **2.2.2. Política de Clasificación, Administración y Protección de la Información**

El Ministerio de Transporte y Obras Públicas definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad e importancia, y generará Guías de Clasificación de la Información para que los propietarios de la misma puedan catalogarla y se puedan determinar controles específicos para su protección.

Una vez clasificada la información el MTOP proveerá los recursos necesarios en la aplicación de controles para preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de funcionarios de la entidad y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

## **2.3. POLÍTICAS DE SEGURIDAD DEL PERSONAL**

### **2.3.1. Política Relacionada con la Vinculación de Funcionarios**

El Ministerio de Transporte y Obras Públicas reconociendo la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las actividades y roles que deben desempeñar los funcionarios en sus cargos.

Todo funcionario que se vincule a la Institución deberá suscribir el ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN otorgado por el Ministerio a través de la Dirección de Administración de Recursos Humanos, quienes a su vez son los encargados de dar a conocer las políticas, normas y procedimientos de seguridad de la información.

### **2.3.2. Política de Concienciación a los Usuarios**

El Ministerio de Transporte y Obras Públicas en su interés por garantizar que el personal cuente con un nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información, diseñará y ejecutará de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

### **2.3.3. Política de Desvinculación o Cambio de Labores de los Funcionarios**

El Ministerio de Transporte y Obras Públicas asegurará que sus funcionarios serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

## **2.4. POLÍTICAS DE SEGURIDAD FÍSICA Y DE ENTORNO**

### **2.4.1. Política de Áreas Seguras**

La Dirección de Tecnologías de la Información, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos del Ministerio de Transporte y Obras Públicas, asignará actividades específicas a sus funcionarios, quienes deben garantizar la adecuada operación y administración de los recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de dichas actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de garantizar la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

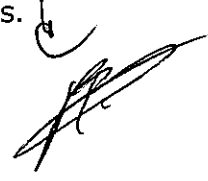
### **2.4.2. Política de Seguridad para los Equipos Institucionales**

El Ministerio de Transporte y Obras Públicas, para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

## **2.5. POLÍTICAS DE GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES**

### **2.5.1. Política de Asignación de Responsabilidades Operativas**

El Ministerio de Transporte y Obras Públicas realizará su mayor esfuerzo para facilitar la implantación y garantizar la efectividad de los mecanismos de seguridad física y control de acceso que aseguren las áreas de procesamiento de información sensible. Del mismo modo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus instalaciones.



### **2.5.2. Política para la Planeación y Aceptación de Sistemas**

El Ministerio de Transporte y Obras Públicas garantizará la capacidad de procesamiento adecuada en sus recursos tecnológicos y sistemas de información, estableciendo proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida; así mismo, velará porque la puesta en marcha de recursos tecnológicos o sistemas de información cuente con controles orientados a la aceptación.

### **2.5.3. Política de Protección frente a Software Malicioso**

El Ministerio de Transporte y Obras Públicas proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de procesamiento de la misma adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios frente a los ataques de software malicioso.

### **2.5.4. Política de Respaldo y Almacenamiento de la Información**

El Ministerio de Transporte y Obras Públicas garantizará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Los Procesos o Unidades del MTOP propietarias de la información, con el apoyo de la Dirección de Tecnologías de la Información encargada de la generación de copias de respaldo, definirán la estrategia a seguir para el respaldo y almacenamiento de la información.

### **2.5.5. Política de Seguridad en las Redes de Datos**

El Ministerio de Transporte y Obras Públicas proveerá a través de la Dirección de Tecnologías de la Información, los mecanismos de control necesarios para garantizar la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

### **2.5.6. Política de Uso de Periféricos y Medios de Almacenamiento**

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica del Ministerio de Transporte y Obras Públicas, será



reglamentado por la Dirección de Tecnologías de la Información, considerando las labores realizadas por los funcionarios y su necesidad de uso.

#### **2.5.7. Política de Uso del Correo Electrónico y la Mensajería Instantánea**

El Ministerio de Transporte y Obras Públicas, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará y garantizará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

#### **2.5.8. Política de Uso Adecuado de Internet**

El Ministerio de Transporte y Obras Públicas consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para garantizar la disponibilidad de Internet como herramienta laboral a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

#### **2.5.9. Política de Intercambio de Información**

El Ministerio de Transporte y Obras Públicas garantizará la protección de la información en el momento de ser transferida o intercambiada con otras entidades, acogiendo y aplicando los procedimientos de transferencia de información de acuerdo con su nivel de clasificación; así mismo, se establecerán Acuerdos de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio.

#### **2.5.10. Política de Auditoría y Monitoreo de los Recursos Tecnológicos y los Sistemas de Información**

La Unidad de Seguridad de la Información y la Unidad de Infraestructura y Operaciones realizará monitoreo permanente del uso que dan los funcionarios y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información del Ministerio de Transporte y Obras Públicas. Además, velará por la custodia de los registros de auditoría y cumpliendo con los periodos de retención establecidos para dichos registros.



## **2.6. POLÍTICAS DE CONTROL DE ACCESO**

### **2.6.1. Política de Administración de Cuentas de Usuario y Contraseñas**

El Ministerio de Transporte y Obras Públicas garantizará el establecimiento de lineamientos y derechos para el control de acceso lógico de cada usuario o grupo de usuarios a los recursos tecnológicos y los sistemas de información de la Institución.

### **2.6.2. Política de Verificación y Mantenimiento de los Derechos de Acceso**

El Ministerio de Transporte y Obras Públicas, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores. De igual manera, garantizará que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

### **2.6.3. Política de Control de Acceso a Sistemas Operativos, Redes de Datos y Sistemas de Información**

La Dirección de Tecnologías de la Información, responsable de la plataforma tecnológica del Ministerio de Transporte y Obras Públicas, garantizará que los sistemas operativos, las redes de datos y los sistemas de información que apoyan los procesos de la misma, sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

## **2.7. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**

### **2.7.1. Política para el Establecimiento de Requisitos de Seguridad**

El Ministerio de Transporte y Obras Públicas asegurará que el software adquirido y desarrollado tanto al interior, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por la Institución. Las áreas propietarias de sistemas de información incluirán requisitos de seguridad y calidad en la definición de requerimientos y se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos de software.

### **2.7.2. Política de Control al Procesamiento de los Sistemas de Información**

Los propietarios de sistemas de información del Ministerio de Transporte y Obras Públicas, velarán por el correcto procesamiento, calidad y veracidad de la información ingresada, así como generada por los sistemas de información. Los funcionarios que operan los sistemas de información realizarán validaciones periódicas de la información contenida en dichos sistemas.

### **2.7.3. Política para el Manejo de Información Cifrada**

El Ministerio de Transporte y Obras Públicas garantizará que la información de la entidad clasificada como sensible, será cifrada al momento de almacenarse y transmitirse por cualquier medio.

### **2.7.4. Política de Seguridad de los Archivos del Sistema**

El Ministerio de Transporte y Obras Públicas proveerá ambientes separados de desarrollo, pruebas y producción para sus sistemas de información, con los controles de acceso establecidos para cada ambiente y una adecuada segregación de funciones, con el fin de evitar accesos no autorizados a los ambientes productivos. De igual manera, proporcionará protección a los archivos fuente, configuración y ejecutables de los sistemas de información o software adquirido y/o desarrollado al interior de la entidad.

### **2.7.5. Política de Seguridad en los Procesos de Desarrollo y Soporte**

El Ministerio de Transporte y Obras Públicas velará porque el desarrollo interno o externo de los sistemas de información cumpla con el ciclo de vida de desarrollo de software, requerimientos de funcionalidad y seguridad esperados, así como con metodologías para la definición de requerimientos de software y para la realización de pruebas al software desarrollado. Además, se garantizará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Institución.

### **2.7.6. Política de Gestión de Vulnerabilidades**

La Unidad de Seguridad de la Información del Ministerio de Transporte y Obras Públicas, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica a través de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

b



## **2.8. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD**

### **2.8.1. Política para el Reporte y Tratamiento de Incidentes de Seguridad**

El Ministerio de Transporte y Obras Públicas promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de **información**, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas. De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando el incidente de acuerdo con su criticidad.

## **2.9. POLÍTICAS DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**

### **2.9.1. Política de Continuidad, Contingencia, Recuperación y Retorno a la Normalidad**

**El Ministerio de Transporte y Obras Públicas** proporcionará los recursos suficientes para garantizar una respuesta efectiva de funciones y procesos en caso de contingencia o eventos catastróficos que se presenten en la Institución y que afecten la continuidad de su operación.

Además, **el Ministerio de Transporte y Obras Públicas** responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; así mismo, se restablecerán las operaciones con el menor costo y pérdidas posibles, y se mantendrán canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

## **2.10. POLÍTICAS DE CUMPLIMIENTO**

### **2.10.1. Política de Cumplimiento de Requerimientos de Licenciamiento y Propiedad Intelectual**

El Ministerio de Transporte y Obras Públicas teniendo en cuenta la legislación referente a derechos de autor y propiedad intelectual, velará porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables; así mismo, el Ministerio

de Transporte y Obras Públicas propenderá por el cumplimiento de esta legislación por parte de los funcionarios de la entidad.

### **2.10.2. Política de Privacidad de la Información**

El Ministerio de Transporte y Obras Públicas establecerá los controles necesarios para preservar la información que la entidad conozca y almacene de sus funcionarios, clientes, proveedores y terceros, y velará para que dicha información sea utilizada únicamente para funciones propias del Ministerio y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización. Además, garantizará el derecho de Habeas Data de sus funcionarios y terceros.

### **3. SANCIONES**

La infracción a las obligaciones establecidas en la presente política, podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley pertinente. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

La Dirección de Tecnologías de la Información velará por el cumplimiento de estas políticas, resguardando los intereses de la Institución.

La Dirección de Tecnologías de la Información no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

### **DISPOSICIONES GENERALES**

**PRIMERA.-** Las disposiciones contenidas en la presente Política de Seguridad de la Información son de carácter obligatorio para las y los servidores y las y los trabajadores del MTOP.

**SEGUNDA.-** Encargar la ejecución y seguimiento del presente Acuerdo a la Coordinación General de Planificación y Gestión Estratégica, a través de la unidad especializada de Gestión de Seguridad de la Información de la Dirección de Tecnologías de la Información.

### **DISPOSICIÓN FINAL**

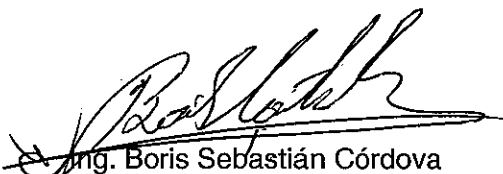


La Coordinación General de Planificación y Gestión Estratégica y la Coordinación General Administrativa Financiera, deberán disponer la generación del instructivo para la aplicación de las Políticas de Seguridad de la Información, en un plazo de 75 días laborables, dentro de este plazo la Coordinación General de Planificación y Gestión Estratégica será la encargada de la aprobación del instructivo y puesta en vigencia, cuyo seguimiento de la aplicación y cumplimiento del mismo estará a cargo de la Dirección de Tecnologías de la Información a través de su Unidad de Gestión de Seguridad de la Información.

Encárguese de la socialización y difusión de este Acuerdo a la Dirección de Tecnologías de la Información del Ministerio de Transporte y Obras Públicas.

El presente acuerdo prevalece sobre cualquier norma o disposición de igual o inferior jerarquía, y entrará en vigencia a partir de la fecha de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Comuníquese y Publíquese. -Dado en la ciudad de San Francisco de Quito,  
Distrito Metropolitano, a        23 MAY 2017



Ing. Boris Sebastián Córdova  
**MINISTRO DE TRANSPORTE Y OBRAS PÚBLICAS**