

 <p><b>PERSONERIA MUNICIPAL DE DOSQUEBRADAS</b> "Por la Igualdad de tus Derechos"</p>	CODIGO	FT-GDOF-001
	FECHA	ABRIL -2009
	VERSION	01
	PAGINAS	01 DE 01



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

***VIGENCIA 2023***

ELABORO Y PROYECTO MGMN	REVISO: NICOLAS RIOS GONZALEZ	RECIBIDO POR: DIA MES AÑO -HORA
----------------------------	----------------------------------	------------------------------------

**CAM PISO 02 OFICINA 208-209 TELEFONO 3228460 FAX 3228254**  
[personeriadosquebradas@gmail.com](mailto:personeriadosquebradas@gmail.com)

 <b>PERSONERIA MUNICIPAL DE DOSQUEBRADAS</b> <i>"Por la dignidad de sus derechos"</i>	CODIGO	FT-GDOF-001
	FECHA	ABRIL -2009
	VERSION	01
	PAGINAS	01 DE 01

## **INTRODUCCION.**

Con el fin de contribuir a la preservación de la confidencialidad, integridad y disponibilidad de la información y al cumplimiento normativo, la Personería de Dosquebradas, se encuentra en proceso de implementación del Sistema de Gestión de Seguridad de la Información – SGSI, conforme a lo dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC en la política de gobierno digital, y de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI; el cual presenta un conjunto de buenas prácticas para la seguridad de la información en las entidades del Estado, y que sirve de referencia para la construcción del SGSI basado en la Norma Técnica Colombiana ISO 27001:2013, mediante un enfoque basado en la gestión del riesgo y el establecimiento de controles.


La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la entidad con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Personería y apoyan el Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Personería Municipal de Dosquebradas, para asegurar el direccionamiento estratégico de la Entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información, estos últimos correspondientes a:

- Mitigar los riesgos de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos de la entidad.
- Garantizar la continuidad del servicio frente a incidentes

El presente documento presenta las actividades y línea de tiempo a seguir por la Personería, para implementar el Sistema de Gestión de Seguridad de la Información – SGSI, en todos los procesos de la entidad durante la vigencia 2023.

**OBJETIVO GENERAL.** Describir y programar las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información – MSPI, emitido por el Ministerio de

ELABORO: MGMN 	REVISO: NICOLAS RIOS GONZALEZ	RECIBIDO. DIA ___ MES ___ AÑO ___-2 HORA _____
---	-------------------------------	---

 <b>PERSONERÍA MUNICIPAL DE DOSQUEBRADAS</b> <i>"Por la dignidad de tus derechos"</i>	CODIGO	FT-GDOF-001
	FECHA	ABRIL -2009
	VERSION	01
	PAGINAS	01 DE 01

Tecnologías de la Información y la Comunicaciones MINTIC en la Política de Gobierno Digital, y que se ejecutarán en el transcurso de la **vigencia 2023**

**ALCANCE.** Comprende la descripción y programación de las actividades a realizar por la Personería de Dosquebradas, durante la **vigencia 2023**, y aplica a toda la entidad, sus funcionarios, contratistas y terceros de acuerdo con el Modelo de Seguridad y Privacidad de la Información - MSPI emitido por el Ministerio de las Tecnologías de la Información y las Comunicaciones.

**NIVEL DE CUMPLIMIENTO.** Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política.

**RESPONSABLES.** El Sistema de Gestión de Seguridad de la Información – SGSI, se encuentra bajo la responsabilidad del contratista que está a cargo de la página de la entidad.

La alta dirección de la Personería de Dosquebradas, apoyará la ejecución del presente plan, mediante la participación y compromiso con las actividades que requieran de su apoyo y gestión y para las cuales se encuentra relacionado entre los responsables en la descripción del presente plan. Igualmente fomentará en el personal a cargo la participación en las actividades relacionadas con dicho plan.

**DEFINICIONES.** A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes definiciones:

**INFORMACIÓN:** se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

**SISTEMA DE INFORMACIÓN:** se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

**TECNOLOGÍA DE LA INFORMACIÓN:** se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

**GUÍA:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

ELABORO: MGMN	REVISO: NICOLAS RIOS GONZALEZ	RECIBIDO. DIA ___ MES ___ AÑO ___3 HORA
---------------	-------------------------------	--

CAM PISO 02 OFICINA 208-209 TELEFONO 606-3401165

 <p><b>PERSONERÍA MUNICIPAL DE DOSQUEBRADAS</b> "Por la Igualdad de sus Derechos"</p>	CODIGO	FT-GDOF-001
	FECHA	ABRIL -2009
	VERSION	01
	PAGINAS	01 DE 01

**MEJOR PRÁCTICA:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad en la entidad.

**MSPI:** Modelo de Seguridad y Privacidad de la Información; herramienta diseñada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia - MINTIC, con el fin de guiar a las Entidades en la implementación del Sistema de Gestión de Seguridad GSI.

**POLÍTICA:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico

**PROCEDIMIENTO:** Los procedimientos definen específicamente como las políticas, estándares, mejores prácticas y guías serán implementadas en una situación dada. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico.

Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca cómo les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.


## DESARROLLO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios(as), contratistas y terceros que tengan interacción con la Entidad.

La Personería protegerá la información creada, procesada, transmitida o resguardada por los procesos propios de la actividad, con el fin de minimizar impactos económicos, operativos o legales debido a un uso incorrecto de esta

*Principios de seguridad que soportan el Plan de Seguridad de la Información*

La Personería protegerá la información generada, procesada o resguardada por cada una de las actividades definidas en el mapa de procesos, así como su infraestructura tecnológica y activa del riesgo que se genera de los accesos otorgados a la información digital o electrónica

ELABORO: MGMN 	REVISÓ: NICOLAS RIOS GONZALEZ	RECIBIDO. DIA ___ MES ___ AÑO ___ HORA
---	-------------------------------	---



CODIGO	FT-GDCF-001
FECHA	ABRIL -2009
VERSION	01
PAGINAS	01 DE 01

### CONTROLES DE ACUERDO CON LA CLASIFICACIÓN DE LA INFORMACIÓN DE SU PROPIEDAD O EN CUSTODIA.

- Proteger su información de las amenazas originadas por parte del personal.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar control de acceso a la información, sistemas y recursos de red.
- Implementar la seguridad como parte integral del ciclo de vida de los sistemas de información.
- Realizar a través de una adecuada gestión de los eventos de seguridad y las debilidades identificadas en los sistemas de información, una mejora efectiva de su modelo de seguridad.
- Garantizar la disponibilidad de sus procesos y la continuidad de su operación, acorde a los impactos que pueden generar los eventos que puedan afectarlos.
- Exigir el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en las políticas de seguridad y privacidad de la información a funcionarios(as), contratistas, proveedores y en general a quienes interactúen con la información de la Entidad.

### POLITICAS TRATAMIENTO DE LA INFORMACION Y DATOS

- La Personería ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- La entidad protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.
- La Personería protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos 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 o en custodia.
- Protege su información de las amenazas originadas por parte del personal.
- Protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementa controles de acceso a la información, sistemas y recursos de red.
- Garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- 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.
- Garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en

ELABORO: MGMN

REVISÓ: NICOLAS RIOS GONZALEZ

RECIBIDO. DIA \_\_\_ MES \_\_\_ AÑO \_\_\_ 5  
HORA

CAM PISO 02 OFICINA 208-209 TELEFONO 606-3401165

 <b>PERSONERÍA MUNICIPAL DE DOSQUEBRADAS</b> "Por la Dignidad de tus Derechos"	CODIGO	FT-GDOF-001
	FECHA	ABRIL -2009
	VERSION	01
	PAGINAS	01 DE 01

las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

## IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

**Justificación.** La Personería Municipal de Dosquebradas con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de 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.

Adicionalmente, debe considerarse los conceptos de:

- a) **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- b) **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- c) **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- d) **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- e) **Confianza de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

**CUMPLIMIENTO.** El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio.

ELABORO: MGMN	REVISÓ: NICOLAS RIOS GONZALEZ	RECIBIDO. DIA ___ MES ___ AÑO ___-6 HORA
---------------	-------------------------------	---

 <b>PERSONERIA MUNICIPAL DE DOSQUEBRADAS</b> "Por la Igualdad de sus Derechos"	CODIGO	FT-GDOF-001
	FECHA	ABRIL -2009
	VERSION	01
	PAGINAS	01 DE 01

Si los funcionarios de la entidad o terceros violan este plan, **LA PERSONERIA MUNICIPAL DE DOSQUEBRADAS** se reserva el derecho de tomar las medidas correspondientes.

**COMUNICACIÓN.** Mediante socialización a todos los funcionarios de la **PERSONERIA MUNICIPAL DE DOSQUEBRADAS**, se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad [www.personeriadosquebradas.gov.co](http://www.personeriadosquebradas.gov.co).

**MONITOREO.** Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

**DESCRIPCIÓN DE LAS POLÍTICAS.** La entidad en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad.

**DERECHOS  
MORALES  
Y  
PATRIMONIALES**

Los usuarios son responsables de la custodia y la confidencialidad de los datos y la información a la cual tengan acceso en forma directa e indirecta. La entidad es propietaria de todos los datos e información que circule o se genere al interior de la misma o que esté disponible a través de sus sistemas de información y/o computadores. En este sentido, el **PERSONERO** y **SERVIDORES PÚBLICOS DE NIVEL DIRECTIVO** clasificarán los datos y la información generados o utilizados solicitando a sus colaboradores y contratistas seguir los procedimientos establecidos para el resguardo de los mismos a través de copias de seguridad (Backup).

ELABORO: MGMN	REVISO: NICOLAS RIOS GONZALEZ	RECIBIDO. DIA ___ MES ___ AÑO ___7 HORA
---------------	-------------------------------	--

**CAM PISO 02 OFICINA 208-209 TELEFONO 608-3401165**

**DIVULGACION DE LA INFORMACION**

La información entregada a los medios de comunicación debe hacerse a través del funcionario encargado del manejo de la comunicación de la entidad. La Personería no se hace responsable por las consecuencias que se deriven de la utilización inadecuada por parte de terceros. Igualmente, se abstiene de suministrar la información que haya recibido de terceros para su uso interno y confidencial.

**INFORMACIÓN CONFIDENCIAL**

Exigir a los usuarios la protección de la información clasificada como confidencial o de uso restringido. Incluir una cláusula de confidencialidad en los contratos u órdenes, cuando el contratista requiera acceder de manera directa o indirecta a los datos o información de la Entidad. Todo empleado que participe en proyectos o tenga acceso a su información, debe guardar confidencialidad sobre la misma. El responsable del proyecto debe solicitar a los participantes, como parte de los términos, compromiso y condiciones iniciales de su participación, que firmen un acuerdo de confidencialidad de la información

**RECURSOS INFORMÁTICOS**

Establecer el cambio periódico de los recursos informáticos, dependiendo de la obsolescencia, la vida útil, el estado de los mismos y las necesidades de la Entidad. Se dará de baja a los equipos teniendo en cuenta el procedimiento establecido para tal fin. Exigir a los usuarios la utilización responsable y razonable de los recursos informáticos. Igualmente, el acatamiento de las medidas de control establecidas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde con la importancia de los datos y la naturaleza de los riesgos

**DERECHOS DE AUTOR LICENCIAS DE SOFTWARE**

Proteger el Derecho de Autor y Derechos Conexos, de acuerdo con lo consagrado en la constitución política, los ordenamientos legales y acuerdos. Emplear, en lo posible, las últimas versiones del software disponible en el mercado, para disminuir los problemas ocasionados por las diferencias de versiones. Todos los programas utilizados en los computadores de la entidad deben contar con sus respectivas licencias de uso vigentes y condiciones exigidas

**ADMINISTRACION Y CONTROL**

La conexión a la red debe ser autorizada por el Personero o profesional delegado con las directrices emitidas por el representante legal. No pueden conectarse computadores, servidores, hubs, switches, routers, o cualquier otro hardware a la red sin la autorización correspondiente.

**CORREO ELECTRONICO**

La Personería suministrara el acceso al correo electrónico y a internet, como herramientas para la realización de las labores, dependiendo de las responsabilidades y naturaleza del trabajo contratado, conforme a lo previsto en el manual de funciones. El uso inadecuado de internet constituirá una falta grave, que se clasificará como tal por la magnitud del hecho o por no atender los requerimientos de la empresa para que se cese la utilización indebida. La comprobación y las sanciones disciplinarias se realizarán conforme lo establecido en la legislación aplicable

ELABORO: MGMN

REVISO: NICOLAS RIOS GONZALEZ

RECIBIDO. DIA \_\_\_ MES \_\_\_ AÑO \_\_\_  
HORA \_\_\_





**PERSONERÍA MUNICIPAL DE  
DOSQUEBRADAS**  
"Por la Igualdad de tus Derechos"

CODIGO FT-GDOF-001

FECHA ABRIL -2009

VERSION 01

PAGINAS 01 DE 01

### GESTIÓN DOCUMENTAL

Propender porque las circulares y en general comunicaciones informáticas enviadas entre los servidores públicos, se realice por medios electrónicos. Cualquier comunicación registrada por otro medio, no será considerada como oficial y el funcionario responderá por las consecuencias derivadas de ello, todo documento será reconocido una vez haya sido enviado a su destinatario, el radicado implica oficialización del documento y se entenderá que debe ser tramitado, el funcionario que a sabiendas radique y no envíe la comunicación responderá por las consecuencias que se deriven de dicho acto. La radicación de correspondencia interna y externa que requiera imprimirse es responsabilidad de cada funcionario y ventanilla única.

### COMPUTADORES, SERVIDORES Y REDES

Prohibir a los usuarios la modificación de la configuración de hardware y software establecida en cada uno de los computadores. La financiera será responsable que los equipos se protejan para disminuir el riesgo de hurto, destrucción, fluctuaciones de energía, incendio y medio ambiente (por ejemplo: agua), utilizando instalaciones en condiciones adecuadas, cerraduras, vigilantes, protectores contra transitorios de energía eléctrica y, para los servidores. Prohibir el uso de módems en computadores que tengan conexión a la red local, para prevenir la intrusión de hackers.

### CUENTAS DE LOS USUARIOS

Cuando la entidad vincula a un respectivo funcionario o contratista este debe firmar un documento donde declara conocer las políticas informáticas y de seguridad de la información y acepta las responsabilidades. No debe concederse una cuenta a personas que no sean funcionarios adscritos a la Personería a menos que estén debidamente autorizados. En este caso, la persona debe firmar un documento donde declare conocer las políticas informáticas y de seguridad de la información y acepta sus responsabilidades.

### IDENTIFICACION, CONTRASEÑAS Y AUTORIZACIONE

Las funcionarios o contratistas que acceden a los sistemas de información requieren de un identificador, el cual será proporcionado como parte del proceso de autorización. Los identificadores concedidos deberán eliminarse o deshabilitarse, por solicitud de la financiera, cuando cese la vinculación del usuario con la empresa en forma permanente o temporal, o cuando se presente un uso indebido. De esta manera, todas las acciones realizadas con un identificador de usuario son responsabilidad del titular del mismo.

### SEGURIDAD FISICA Y DEL ENTORNO

Implantar los controles de seguridad apropiados para el ingreso a las instalaciones de la entidad de funcionarios, contratistas y terceros. El acceso de personal contratista, se debe autorizar una vez se haya formalizado el contrato y de acuerdo con los controles de seguridad definidos. Se debe exigir al personal contratista, cumplir igualmente con las políticas, procesos procedimientos establecidos en la entidad.

ELABORO: MGMN

REVISO: NICOLAS RIOS GONZALEZ

RECIBIDO. DIA \_\_\_ MES \_\_\_ AÑO \_\_\_ 9  
HORA

 <b>PERSONERÍA MUNICIPAL DE DOSQUEBRADAS</b> <i>"Por la defensa de sus derechos"</i>	<b>CODIGO</b>	<b>FT-GDOF-001</b>
	<b>FECHA</b>	<b>ABRIL -2009</b>
	<b>VERSION</b>	<b>01</b>
	<b>PAGINAS</b>	<b>01 DE 01</b>

La Personería Municipal de Dosquebradas, por medio de resolución 098 del 2019 aprueba y adopta el manual de políticas y procedimientos para la protección de los datos personales.

**RESOLUCIÓN No 098-2019**  
**Agosto 28-2019**

"Por medio de la cual se adopta el manual de políticas y procedimientos para la protección de datos personales"

**PERSONERÍA MUNICIPAL DE DOSQUEBRADAS – RISARALDA**, en uso de sus facultades legales, especialmente las contenidas en el artículo 168 de la ley 136 de 1994 y las que le confiere la ley 909 del 2004, el decreto 1227 del 2005 y el plan nacional de capacitaciones y:

**CONSIDERANDO**

Que la Constitución Política dispone en el artículo 15 que toda persona tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos y en archivos de entidades públicas y privadas.

Que a su vez el artículo 20 de la Carta Magna garantiza a toda persona el derecho fundamental de informar y recibir información veraz e imparcial.

Que en desarrollo de los preceptos constitucionales antes citados, el Congreso de la República expidió la Ley 1250 de 2008, por medio de la cual se dictaron disposiciones generales frente al manejo de datos y reguló el manejo de la información contenida en bases de datos personales.

Que así mismo el Congreso de la República expidió la Ley Estatutaria 1581 de 2012, a través de la cual dictó disposiciones generales para la protección de datos personales y dispuso como deberes de los sujetos obligados, entre otros, el contenido en el artículo 17, literal ki que expresamente señala "Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos".

Que con el fin de regular el derecho de acceso a la información pública y regularizar las excepciones a la publicidad de la información, el Congreso de la República expidió la Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

ELABORÓ:  / REVISÓ:  / APROBÓ: 

 <b>PERSONERÍA MUNICIPAL DE DOSQUEBRADAS</b> <i>"Por la defensa de sus derechos"</i>	<b>TÍTULO</b>	<b>MANUAL</b>
	<b>VERSIÓN</b>	<b>01</b>
	<b>PÁGINAS</b>	<b>01 DE 01</b>

Que con el fin de dar cumplimiento a la normativa antes señalada, La Personería Municipal de Dosquebradas adopta el manual de Políticas y Procedimientos para la Protección de Datos Personales, documento que establece la forma como se recolectan, manejan y conservan los datos personales de los sujetos que la entidad en desarrollo de sus funciones constitucionales y legales requiere de su uso, y señala el procedimiento por el cual el interesado puede acudir ante la administración para solicitar el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de sus datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales que allí mismo se señalan.

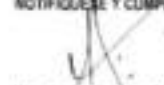
Por lo antes considerado, el Personero Municipal de Dosquebradas Risaralda:

**RESUELVE:**

**ARTÍCULO PRIMERO.** ADOPTAR el Manual de Políticas y Procedimientos para la Protección de Datos Personales, el cual hace parte integral del presente acto.

**ARTÍCULO SEGUNDO.** La Presente Resolución rige a partir de su expedición y publicación.

**NOTIFIQUESE Y CUMPLASE**

  
**MAURICIO GARCÉS OBANDO**  
 Personero Municipal (encargado)

ELABORO: <b>MGMN</b>	REVISÓ: <b>NICOLAS RIOS GONZALEZ</b>	RECIBIDO. DIA ___ MES ___ AÑO <b>10</b>
		HORA

**CAM PISO 02 OFICINA 208-209 TELEFONO 606-3401165**