PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2025-2028

PROYECTO: María Gilma Manrique Noreña Jefe Control Interno	REVISO: John Edison Parra Sánchez Secretario General	RECIBIDO POR: _____ Dia___Mes___Año_____Hora_____

Versión	Fecha de versión	Descripción	Resolución
1	2021-01	Creación del documento	003-2021
2	2022-01	Actualización vigencia 2022	006-2022
3	2023-01	Actualización vigencia 2023	006-2023
4	2024-01	Actualización vigencia 2024	020-2024
5	2025-01	Actualización vigencia 2025	004-2025

INTRODUCCION.

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.

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 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 2025-2028**.

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 Tecnologías de la Información y la Comunicaciones MINTIC en la Política de Gobierno Digital.

ALCANCE. Comprende la descripción y programación de las actividades a realizar por la Personería de Dosquebradas, durante la **vigencia 2025-2028** 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.

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 SGSI.

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

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

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

a) 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.
b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
c) 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.
d) 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.
e) Protege su información de las amenazas originadas por parte del personal.
f) Protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
g) Controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
h) Implementa controles de acceso a la información, sistemas y recursos de red.
i) Garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
j) 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.
k) Garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.
l) Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

"El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en 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 Personeria 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) **Confiabilidad 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. 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.**

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** clasificaran 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).
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
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 envié la comunicación responderá por las consecuencias que se deriven de dicho acto. La radicación de correspondencia interna y externa 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 AUTORIZACIONES	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.

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.

RESOLUCION 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"

PERSONERIA 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 les confiere la ley 909 del 2004 el decreto 1227 del 2005 y el plan nacional de capacitaciones y

PROYECTO: María Gilma Manrique Noreña Jefe Control Interno	REVISO: John Edison Parra Sánchez Secretario General	RECIBIDO POR: _____ Dia___Mes___Año_____Hora____

Anexo 01

"PROCEDIMIENTO PARA LA REALIZACION DE COPIAS DE SEGURIDAD – (BACKUP)", PERSONERIA MUNICIPAL DE DOSQUEBRADAS

POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

OBJETIVO. Garantizar el resguardo en forma segura de toda la información digital que dentro del desarrollo de las funciones se considere documental e importante y crítica, generada en cada una de las dependencias de la Personería Municipal de Dosquebradas.

ALCANCE. Este procedimiento aplica para todos los funcionarios de la Personería Municipal de Dosquebradas (de planta, contratistas y judicantes), que tienen a cargo equipos de cómputo y que manejen información importante y crítica.

Comprende desde la clasificación de los archivos en las computadoras por parte de cada uno de los usuarios, hasta el almacenamiento de las copias de seguridad.

DEFINICIONES.

COPIA DE SEGURIDAD- (BACKUP)

Se define como backup o copia de seguridad, la actividad de resguardar de forma segura la información contenida en un medio de almacenamiento de origen (disco duro) a un medio de almacenamiento de destino de diferente tipo (otro disco duro, servidor de backup, Memoria USB, CD, DVD, etc.).

CONTRASEÑA, CLAVE O PASSWORD

Una contraseña o clave (en inglés password), es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso.

INFORMACION DOCUMENTAL: Son todos aquellos archivos digitales institucionales, creados en las computadoras por cada uno de los funcionarios en sus respectivas dependencias.

PARTICIÓN: En computación, una partición de disco es una división lógica de un medio de almacenamiento

INFORMACIÓN IMPORTANTE Y CRÍTICA: Son todos aquellos archivos digitales generados por el software aplicativo con que cuenta la Personeria Municipal de Dosquebradas (MEKANO (contable), REGISTRO UNICO DE VICTIMAS (RUV), SISTEMA INTEGRAL DE AUDITORIA ((SIA), contratación, misional), BANCA VIRTUAL (Banco DAVIVIENDA Dosquebradas), COLOMBIA COMPRA EFICIENTE ((SECOP) publicación de contratación) y ASOPAGOS.

NOMBRE DE USUARIO O LOGIN NAME: Login name o nombre de usuario. Es el nombre que adquiere el usuario para acceder a un determinado servicio

MEDIOS DE ALMACENAMIENTO DE DATOS

Un dispositivo de almacenamiento de datos es un dispositivo para grabar o almacenar información (datos).

Un dispositivo de almacenamiento puede guardar la información y procesarla, o ambas. Un dispositivo que únicamente guarda la información es un dispositivo de grabación. Dispositivos que procesan la información

(equipo de almacenamiento de datos) pueden tener acceso a un medio extraíble (portable) separado o a un componente permanente para almacenar y recuperar la información.

Un sistema operativo es un software de sistema, es decir, un conjunto de programas de computadora destinado a permitir una administración eficaz de sus recursos.

SISTEMA OPERATIVO

CODIGO O NOMENCLATURA: El código, en Teoría de la comunicación, es el conjunto de caracteres que puede ser entendido tanto por el emisor y el receptor. El código que se ha usado en este texto, por ejemplo, es la lengua española o el castellano.

El DVD es un Disco de Vídeo Digital que tiene función de grabadora de videos, sonidos con una gran nitidez en el vídeo y en el sonido.

También es un dispositivo de almacenamiento masivo de datos cuyo aspecto es idéntico al de un disco compacto, aunque contiene hasta 15 veces más información y puede transmitirla a la computadora unas 20 veces más rápido que un CD-ROM. Su capacidad de almacenamiento estándar es de 4.7 GB

PUERTO USB:

Un puerto **USB** es una entrada o acceso para que el usuario pueda compartir información almacenada en diferentes dispositivos como una cámara de fotos, un pendrive, entre otros, con un computador. Las siglas **USB** quieren decir **Bus de Serie Universal** en inglés.

COMPUTADORA

Es una máquina electrónica que recibe y procesa datos para convertirlos en información útil. Una computadora es una colección de circuitos integrados y otros componentes relacionados que puede ejecutar con exactitud, rapidez y de acuerdo a lo indicado por un usuario o automáticamente por otro programa, una gran variedad de secuencias o rutinas de instrucciones que son ordenadas, organizadas y sistematizadas.

CORREO ELECTRÓNICO: Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos.

RESTAURACIÓN POR PREPRODUCCIÓN: cuando la restauración de la copia de seguridad es por pruebas en las maquinas o actualizaciones.

RESTAURACIÓN POR DAÑO: Cuando la funcionalidad del servicio y/o aplicativo se ve afectada.

CONDICIONES GENERALES. Todos los funcionarios de la Personeria Municipal de Dosquebradas que tienen a cargo equipos de cómputo y que manejen información importante y crítica, deben realizar copias de seguridad de su computadora hacia el medio de almacenamiento dispuesto por la entidad, una (01) vez por semana el día **jueves entre las 8.00 A.M hasta las 6.00 PM.**

La información de los archivos contenidos en las copias de seguridad debe ser única y exclusivamente de uso institucional y no personal.

La entidad no se hace responsable por el daño o la perdida de la información contenida en las computadoras de los funcionarios que no realicen sus copias de seguridad en los dias establecidos.

El resguardo y almacenamiento adecuado de las copias de seguridad, es responsabilidad del Área Financiera y del secretario general de la Entidad.

En caso de que algún funcionario necesite copias de sus archivos almacenados (backup), esta petición debe ser requerida al secretario general de la Entidad previo diligenciamiento del formato.

PROCEDIMIENTO.

No	DETALLE	RESPONSABLE
1	Solicitud del disco extraíble para realizar backup (FORMATO PMDCI01-2017)	Financiera
2	Realizar copia de seguridad en el disco extraíble, identificando en el mismo una carpeta con el nombre de la dependencia, dentro de ella se subdivide otra con la fecha en que se realiza el backup con su respectiva clave de seguridad.	Funcionario responsable del proceso con VoBo del secretario General
3	Entrega del dispositivo a la financiera de la entidad, donde se le recibe en el formato PMDCI01-2017, con fecha y hora de recibido.	Financiera y funcionario

Anexo 02

POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

DEFINICION Y ALCANCE

QUE ES LA POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS.

La presente **Política de Gestión de Documentos Electrónicos**, en adelante **"PGDE"**, de la Personería Municipal de Dosquebradas, se define y desarrolla de conformidad con la Ley 527 de 1999, la Ley 594 de 2000, el Decreto 1080 de 2015, las demás normas reglamentarias expedidas por el Archivo General de la Nación (AGN) y, en desarrollo de la Política de Gestión Documental de la Entidad, se expide con el objeto de garantizar la integridad, disponibilidad, confidencialidad y conservación de los documentos electrónicos, mediante el establecimiento de las directrices y el marco de actuación e implementación para la gestión de los mismos, y por tanto, de manera eficiente y efectiva soportar la ejecución de los procesos y procedimientos por medios electrónicos.

En el marco de la atención de los usuarios de las entidades públicas y apegándose a los principios fundamentales del Estado Social de Derecho, consagrados en la Constitución Politica de Colombia, las entidades públicas y los organismos dependientes, centralizados y descentralizados, tuvieron que hacer frente a una serie de dificultades de diversa índole, donde fundamentalmente se evidenció la falta de tecnificación y de articulación electrónica del manejo archivístico de las entidades en cuestión.

Fue allí, donde se suscitó la urgencia de realizar, dentro del marco legal vigente, un conjunto de actividades, de procesos y procedimientos que permitiera, tanto a los usuarios como a las propias entidades, manejar, de forma coordinada, eficiente, pertinente, responsable y oportuna, todo el archivo electrónico, pues la contingencia global, como bien se dijo anteriormente, obligó a las entidades a trasladar sus servicios fisicos hacia una esfera digital y electrónica en el marco del aislamiento obligatorio decretado por el Gobierno Nacional en torno a la salvaguarda de la integridad y la salud de la sociedad colombiana.

Lo anterior, ha generado la necesidad de incorporar herramientas tecnológicas en la gestión, uso y almacenamiento de información y documentación en las entidades u organizaciones. Sin embargo, más allá de los alcances técnicos y funcionales, se debe tener en cuenta que, las herramientas implementadas deben estar acorde con las exigencias de la normatividad vigente, las políticas institucionales, alineadas con los sistemas de gestión y deben obedecer a una adecuada planificación, coordinación y control de la información con el fin de garantizar su integridad, autenticidad y disponibilidad a lo largo del tiempo.

OBJETIVOS

Los principales objetivos desarrollados y contenidos dentro de la aplicación de esta política son:

a) Documentar las decisiones, acciones y operaciones de la Personería Municipal.
b) Facilitar la planificación, la toma de decisiones y apoyar la formulación de planes y programas, en materia de documento electrónico.
c) Proteger los intereses de la ciudadanía y de la entidad.
d) Preservar la memoria de la documentación electrónica de la Personería Municipal de Dosquebradas.
e) Desarrollar los instrumentos necesarios para facilitar la gestión de los documentos electrónicos que deben desarrollarse y/o adaptarse y mantenerse adecuadamente para su aplicación y gestión dentro de la entidad.
f) Estandarizar los procesos de gestión documental sobre documentos electrónicos de archivo dentro de los procesos que adelante la Personería.
g) Establecer el conjunto de criterios comunes en relación con el registro, captura, clasificación, acceso, retención, transferencia y conservación de los documentos y expedientes electrónicos producidos o custodiados por la entidad.

ALCANCE.

La presente Politica de Gestión de Documentos Electrónicos **(PGDE),** se integrará en el contexto de la entidad junto a otros procedimientos, políticas y procedimientos de gestión documental de la **PERSONERIA MUNICIPAL DE DOSQUEBRADAS**.

La mencionada política pretende establecer un conjunto de criterios, procedimientos, parámetros y criterios asumidos por la entidad, y, mediante estos como documentarlos, y de esta manera realizar la gestión de los documentos y expedientes producidos o custodiados por esta. Esta Politica pretende garantizar la disponibilidad e integridad de los metadatos mínimos obligatorios y, en su caso, los complementarios o necesarios, asegurando así la gestión, recopilación, conservación y puesta a de los documentos y expedientes electrónicos de la entidad. La presente política aplica a todos los procesos de la entidad, a todos los empleados, asesores, terceros prestadores de servicio y proveedores.

PERIODO DE VALIDEZ.

La **Política de Gestión de Documentos Electrónicos de la Personeria Municipal de Dosquebradas** se hará efectiva a partir de la fecha de su expedición, manteniendo su validez hasta que no sea sustituida o derogada por una política posterior, la cual deberá ir de la mano de la creación y actualización progresiva de los Instrumentos Archivísticos y Programas Específicos que la componen.

DEFINICIONES DE TÉRMINOS GENERALES RELACIONADOS.

ARCHIVO CENTRAL: unidad administrativa que coordina y controla el funcionamiento de los archivos de gestión y reúne los documentos transferidos por los mismos una vez finalizado su trámite y cuando su consulta es constante.

ARCHIVO DE GESTION: archivo de la oficina productora que reúne su documentación en trámite, sometida a continua utilización y consulta administrativa.

ARCHIVO ELECTRÓNICO DE DOCUMENTOS: almacenamiento electrónico de uno o varios documentos o expedientes electrónicos, producidos y tratados conforme a un proceso archivistico.

ARCHIVO HISTORICO: archivo al cual se transfiere del archivo central o del archivo de gestión, la documentación que, por decisión del correspondiente Comité de Archivo, debe conservarse permanentemente, dado el valor que adquiere para la investigación, la ciencia y la cultura. Este tipo de archivo también puede conservar documentos históricos recibidos por donación, depósito voluntario, adquisición o expropiación.

CUADRO DE CLASIFICACIÓN DOCUMENTAL: esquema que refleja la jerarquización dada a la documentación producida por una institución y en el que se registran las secciones y subsecciones y las series y subseries documentales.

DISPONIBILIDAD: característica de seguridad de la información que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran asegurando su conservación durante el tiempo exigido por ley.

DISPOSICIÓN FINAL DE DOCUMENTOS: decisión resultante de la valoración hecha en cualquier etapa del ciclo vital de los documentos, registrada en las tablas de retención y/o tablas de valoración documental, con miras a su conservación total, eliminación, selección y/o reproducción. Un sistema de reproducción debe garantizar la legalidad y la perdurabilidad de la información.

DOCUMENTO ELECTRÓNICO: es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Entramos documentos ofimáticos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, páginas WEB, entre otros.

DOCUMENTO ELECTRÓNICO DE ARCHIVO: serán de archivo cuando por su valor administrativo, fiscal, legal, científico, histórico, técnico o cultural, adquieran esa naturaleza. En cuyo caso, deberán ser tratados conforme a los principios y procesos archivísticos y permanecer almacenados electrónicamente durante todo su ciclo de vida.

EXPEDIENTE ELECTRÓNICO DE ARCHIVO: conjunto de documentos y actuaciones electrónicos producidos y recibidos durante el desarrollo de un mismo trâmite o procedimiento, acumulados por cualquier causa legal, interrelacionados y vinculados entre sí, manteniendo la integridad y orden

dado durante el desarrollo del asunto que les dio origen y que se conservan electrónicamente durante todo su ciclo de vida, con el fin de garantizar su consulta en el tiempo.

FOLIADO ELECTRÓNICO: asociación de un documento electrónico a un índice electrónico en un mismo expediente electrónico o serie documental con el fin de garantizar su integridad, orden y autenticidad, debe incluir dentro la numeración consecutiva de los documentos que conforman el expediente o la serie documental simple.

FUID - FORMATO ÚNICO DE INVENTARIO DOCUMENTAL: instrumento de recuperación de información que describe de manera exacta y precisa las series o asuntos de un fondo documental.

ÍNDICE ELECTRÓNICO: relación conformada por documentos electrónicos, foliados y de un mismo expediente para garantizar integridad, orden y autenticidad de los documentos.

INTEGRIDAD: característica técnica de seguridad de la información con la cual se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento asociados a la misma.

MEDIO ELECTRÓNICO: mecanismo tecnológico, óptico, telemático, informático o similar, conocido o por conocerse que permite producir, almacenar o transmitir documentos, datos o información.

MODELO DE REQUISITOS PARA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS: instrumento de planeación, el cual formula los requisitos funcionales y no funcionales de la gestión de documentos electrónicos de las entidades.

PRESERVACIÓN A LARGO PLAZO: Conjunto de principios, políticas, medidas, planes y estrategias de orden administrativo y operativo orientadas a asegurar la estabilidad física, tecnológica y de protección del contenido intelectual y de la integridad del objeto documental, independiente de su medio y forma de registro o almacenamiento.

PROGRAMA DE GESTIÓN DOCUMENTAL: instrumento estratégico para la gestión documental, pues con él se establecen las estrategias que permitan a corto mediano y largo plazo, la implementación y el mejoramiento de la prestación de servicios, desarrollo de los procedimientos, la implementación de programas específicos del proceso de gestión documental.

RETENCIÓN DOCUMENTAL: plazo que los documentos deben permanecer en el archivo de gestión o en el archivo central, tal como se consigna en la tabla de retención documental.

SISTEMA DE GESTIÓN DE DOCUMENTOS ELECTRONICOS – SGDE: es una aplicación para la gestión de documentos electrónicos.

SISTEMA DE GESTIÓN DE DOCUMENTOS ELECTRONICOS DE ARCHIVO –SGDEA. es el software o programa destinado a gestionar los documentos electrónicos que desean preservarse a mediano y largo plazo. Puede consistir en un módulo especializado, en varios módulos integrados o en la combinación de varios tipos de programas informáticos.

SISTEMA INTEGRADO DE GESTIÓN: conjunto de orientaciones, procesos, políticas, metodologías, instancias e instrumentos enfocados en garantizar un desempeño institucional articulado y armónico que busque de manera constatable la satisfacción de los grupos de interés.

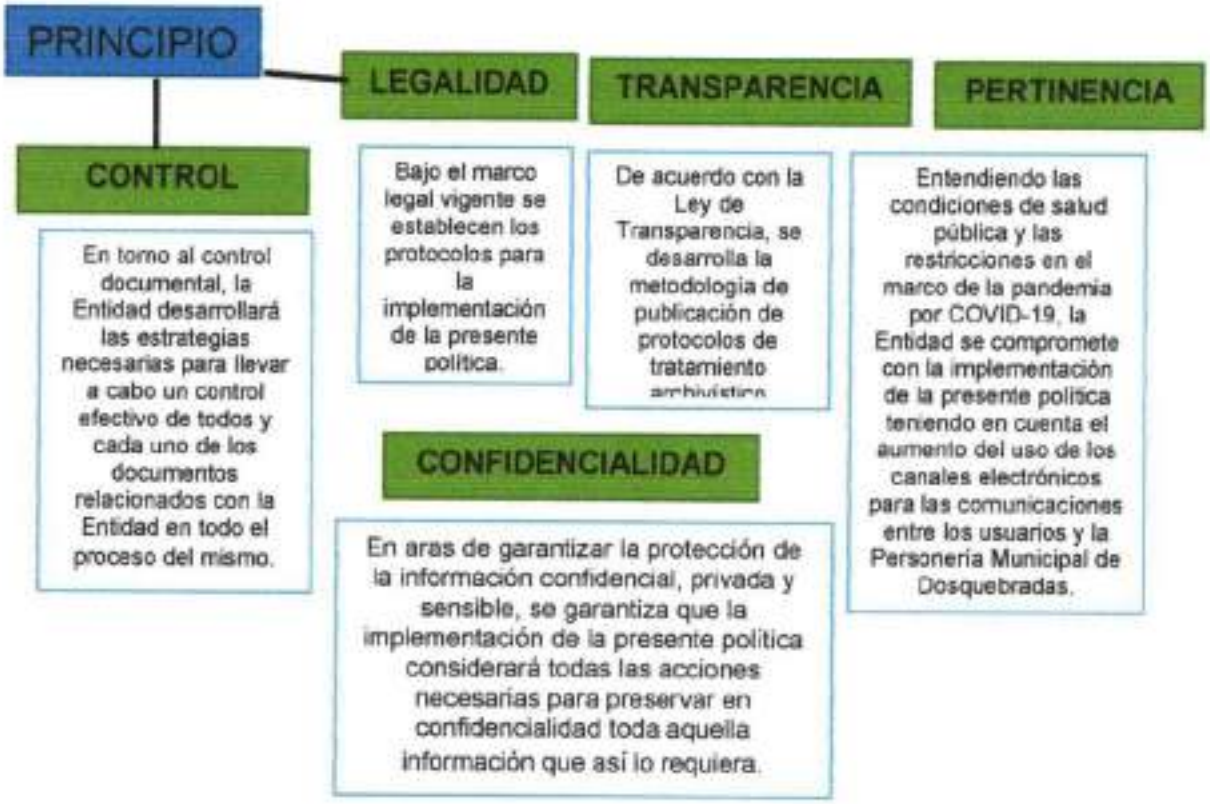
SISTEMA NACIONAL DE ARCHIVOS ELECTRONICOS – SINAE: busca implementar los lineamientos sobre documentos electrónicos, un modelo estándar y un sistema de información unificado que permita la homogenización y estandarización de los procesos de conservación, preservación y divulgación del patrimonio documental en formato electrónico.

TRD - TABLA DE RETENCIÓN DOCUMENTAL: instrumento que describe el listado de series, con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos.

TVD - TABLA DE VALORACIÓN DOCUMENTAL: instrumento que describe el listado de asuntos o series documentales a los cuales se asigna un tiempo de permanencia en el archivo central, así como una disposición final.

MARCO NORMATIVO	
Ley 527, del 18 de agosto de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
Ley 594 de 2000, Ley General de Archivos	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Art 19 Incorporación de tecnologías en la administración y conservación de sus archivos
Ley 1437, 18 de enero de 2011	Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, Capitulo IV- Utilización de medios electrónicos.
Acuerdo 04 del 15 de marzo de 2013	Por el cual se reglamentan parcialmente los Decretos 2578 y 2609 de 2012 y se modifica el procedimiento para la elaboración, presentación, evaluación, aprobación e implementación de las Tablas de Retención Documental y las Tablas de Valoración Documental
Acuerdo 03, del 17 de febrero de 2015	Por el cual se establecen lineamientos para la gestión de documentos electrónicos, conforme al capítulo IV de la ley 1437/11, y reglamenta capítulo IV del Decreto 2609 de 2012. AGN
Decreto 1287 de 2020	Por el cual se reglamenta el Decreto Legislativo 491 de 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria
Decreto 419 de 2020	Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica
Ley 1755 de 2015	Regula el derecho fundamental de petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
Decreto 1080 de 2015	Artículo 2.8.2.5.8 Instrumentos archivísticos para la Gestión documental.

Ley 1712 de 2014	Crea la Ley de Transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. El objeto de la ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.
Decreto 2609 de 2012	Por el cual se reglamenta el Titulo V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Ley 1581 de 2012	Dictan disposiciones generales para la protección de datos personales.
Ley 594 de 2000	Ley General de Archivos



DEFINICION DE DOCUMENTOS ELECTRONICOS.

Se define documento electrónico como "toda la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares" y para el caso específico, en el caso de la **PERSONERIA MUNICIPAL DE DOSQUEBRADAS**, en desarrollo de sus actividades o en virtud de sus obligaciones legales. Estos documentos, formaran parte de la evidencia oficial de las acciones y decisiones de la entidad, y por tanto formaran parte de su patrimonio documental y archivístico.

Por tanto, se definen los requisitos que estos deben cumplir para que se consideren documentos electrónicos válidos:

a) Contener información de cualquier naturaleza o índole, archivada en un soporte electrónico según un formato determinado, de fácil identificación y tratamiento.

b) Contener los datos de identificación que permitan la individualización del mismo, y que de tal manera sea posible la incorporación, anexo y conservación dentro de un expediente electrónico

c) Incluirá los metadatos mínimos obligatorios, definidos de acuerdo a la normativa nacional e internacional vigente para el documento electrónico y Expediente electrónico.

d) De ser necesario, de acuerdo al caso, incluirá otros metadatos complementarios toda vez que cumplan la política de gestión y conservación de documentos electrónicos.

e) Incorporar las firmas electrónicas que correspondan.

POLÍTICAS PARA SERVIDORES PÚBLICOS Y CONTRATISTAS EXTERNOS

Estas políticas aplican tanto a los procesos realizados directamente por la Personería Municipal de Dosquebradas, como a los ejecutados a través de contratos o acuerdos con terceros. Deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externos de la entidad y de las sedes externas de la entidad que hagan uso de la información institucional y de sus recursos tecnológicos.

Comprende desde la explicación de los riesgos a los que están expuestos los activos de información, hasta la ejecución y seguimiento al cumplimiento de las normas y/o políticas informáticas.

Las políticas de seguridad de la información también aplican para los servidores públicos en modalidad de teletrabajo.

1.1. POLÍTICAS DE IDENTIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

Los activos de información dentro del alcance del Sistema de Gestión de Seguridad de la Información SGSI de la Personería deben ser identificados, clasificados y definidos los responsables de cada uno de ellos. Busca asegurar que la información recibe el nivel de protección apropiado de acuerdo a la clasificación establecida. 1.1.1. Identificación y clasificación de la información.

1.1.1.1 Los activos de información deben ser identificados y registrados en un inventario.
1.1.1.2 Los activos de información deben tener propietario designado.
1.1.1.3 El Propietario de un activo de información es responsable de:

- Definir los usuarios autorizados que pueden tener acceso al activo y sus privilegios de acceso.
- Determinar las clasificaciones correspondientes a la sensibilidad del activo.

- Asegurar que se gestione el riesgo de seguridad del activo.
- Establecer las reglas de uso del activo, cuando sea necesario.
- Solicitar la aplicación de controles para la protección del activo de información.

1.1.1.4 Cada activo de información debe tener un custodio designado, quien ha de protegerlo mediante la aplicación y el mantenimiento de los controles de seguridad autorizados por el propietario.
1.1.1.5 La información de la Personería Municipal se clasifica en:

- **Información pública**. Es toda información que la Personería Municipal genere, obtenga, adquiera, o controle en su calidad de obligado.

- **Información clasificada**. Es aquella información que estando en poder o custodia de la Personería Municipal en su calidad de obligado, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

- **Información reservada**. Es aquella información que estando en poder o custodia de la Personería Municipal en su calidad de obligado, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional). 1.1.1.6 El manejo de la información de la Personería Municipal debe seguir los lineamientos del Manual de Protección de la Información.
1.1.1.7 Sólo se permite la transferencia de información Clasificada o Reservada cuando exista un acuerdo de confidencialidad o compromiso contractual que lo regule.
1.1.1.8 La Personería Municipal tiene control total sobre la información que se almacene en la infraestructura de tecnología de la información de la entidad; por lo tanto, se reserva el derecho de mover, borrar, monitorear o tomar custodia de dicha información
1.1.1.9 Los servidores públicos y contratistas son responsables de proteger la información de su trabajo.

1.2. POLÍTICA DE GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

En la Personería Municipal de Dosquebradas la gestión de los riesgos fundamenta la toma de decisiones de seguridad de la información. Busca establecer la gestión del riesgo como eje principal de las actuaciones institucionales relacionadas con la seguridad de la información.
1.2.1. Lineamientos generales de la gestión del riesgo de seguridad informática
1.2.1.1 Servidores públicos y contratistas de la Personería Municipal, deben identificar y reportar condiciones que podrían indicar la existencia de riesgos de seguridad informática.

1.3. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

En la Personería Municipal de Dosquebradas los eventos e incidentes de seguridad de la información son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad.

Busca establecer las líneas de actuación de los servidores públicos frente a la ocurrencia (confirmada o sospechada) de situaciones que afecten la seguridad de la información.

1.3.1. Reporte de eventos, incidentes y debilidades de la seguridad informática.
1.3.1.1. Los servidores públicos y contratistas deben reportar inmediatamente todas las situaciones que puedan afectar la seguridad de la información.
1.3.1.2. Los servidores públicos y contratistas deben abstenerse de crear, acceder, almacenar o transmitir material ilegal, pornográfico, que promueva la violación de los derechos humanos o que atente contra la integridad moral de las personas o de las instituciones.
1.3.1.3. Está prohibida la realización de pruebas a los controles de seguridad de la información.
1.3.1.4. Los programas informáticos desarrollados o adquiridos por Personería Municipal son para el uso exclusivo de la entidad.

1.3.2. Uso adecuado del correo electrónico
1.3.2.1. No está autorizado el envío de correos electrónicos con contenido que atente contra la integridad y la dignidad de las personas, así como con el buen nombre de la entidad.
1.3.2.2. Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico se retire de la Personería Municipal, su cuenta de correo será desactivada.
1.3.2.3. Las cuentas de correo electrónico son propiedad de la Personería Municipal, son asignadas para la realización tareas propias de las funciones laborales y no deben utilizarse para ningún otro fin.
1.3.2.4. Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Entidad.
1.3.2.5. Cuando se detecte un correo fraudulento, con fines maliciosos o con contenido sospechoso se debe informar esta situación

1.3.3. Uso adecuado de equipos de cómputo asignados
1.3.3.1. No está permitida la instalación, ejecución y/o utilización de software diferente al preinstalado en los equipos de cómputo o al instalado por integrantes de los equipos de trabajo de informática.
1.3.3.2. Los parámetros de configuración del sistema operativo solo deben ser modificados por integrantes de los equipos de trabajo de informática.
1.3.4. Uso adecuado de los servicios de red
1.3.4.1. No deben almacenarse archivos personales en carpetas de la red y demás servicios de almacenamiento en internet suministrados por la Personería Municipal 1.3.4.2. No se permite el uso de servicios de descarga o intercambio de archivos que funcionan bajo el esquema P2P (person to person). Por ejemplo: Torrent, Ares, eMule, Limewire, GNUnet, entre otros.
1.3.4.3. No está permitida la descarga de archivos de audio y/o video a menos que lo requieran en virtud de sus responsabilidades laborales.
1.3.4.4. La Personería Municipal podrá controlar y limitar la navegación a ciertos sitios, recursos o servicios de internet con el fin de proteger la seguridad y la disponibilidad del servicio de internet.
1.3.4.5. No está permitido deshabilitar o evadir los controles de navegación en internet.

1.3.4.6. En horarios laborales, está prohibido el uso del servicio de internet de la entidad para acceder a páginas de transmisión de películas, programas de televisión y eventos deportivos.
1.3.4.7. El acceso remoto a los equipos y dispositivos de la plataforma de T.I. solo está permitido para labores de soporte técnico autorizado.
1.3.4.8. El acceso remoto a equipos de cómputo debe contar con la aprobación del servidor público o contratista responsable de dicho equipo.
1.3.4.9. Solo se permite el acceso remoto a estaciones de trabajo de la entidad si el servidor público o contratista responsable del equipo de cómputo lo aprueba. 1.3.4.10. Solo está permitido el uso de servicios de almacenamiento de información suministrados por la entidad.
1.3.4.11. No se permite la inclusión de equipos de cómputo personales (tales como PCs, computadores portátiles, celulares, tabletas, impresoras, cámaras, y wearables) en la red institucional.
1.3.4.12. Todo equipo Tecnológico debe ser revisado, registrado antes de conectarse a cualquier nodo de la Red. Aquellos dispositivos que no estén aprobados deben ser desconectados de la red, eventos de conexión de equipos no autorizados a la red institucional se deben reportar como eventos/incidentes de seguridad.

1.3.5. Uso de material protegido por derechos de autor

1.3.5.1. Se prohíbe el almacenamiento de archivos multimedia (videos, música, imágenes o libros electrónicos) y cualquier otro tipo de contenido que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en las carpetas de red y demás servicios de almacenamiento en internet suministrados por la entidad.
1.3.5.2. Se prohíbe el almacenamiento, uso, instalación y/o ejecución de software que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) y/o licenciamiento en la plataforma tecnológica de la entidad.

1.4. POLÍTICA DE PERSONAS Y CULTURA FRENTE A LA SEGURIDAD INFORMÁTICA

Se deben aplicar medidas de control antes, durante y después de finalizada la relación laboral, con el fin de mitigar los riesgos de seguridad de la información asociados al factor humano. Procura que los servidores públicos y contratistas, entiendan sus responsabilidades y las funciones de sus roles como usuarios de la información con el fin de reducir el riesgo de hurto, fraude o filtraciones.

1.4.1. Antes del empleo

1.4.1.1. Toda persona a ser contratada como servidor público, debe aceptar formalmente el cumplimiento de las políticas del presente manual.

1.4.2. Durante el empleo o la vigencia del contrato

1.4.2.1. Los servidores públicos y contratistas de la Personeria Municipal son responsables por desempeñar sus funciones cumpliendo las políticas definidas en el presente manual.

1.4.2.2. Los servidores públicos y contratistas de la Personería Municipal son responsables por desempeñar sus funciones sin descuidar, ignorar o desestimar los controles de seguridad establecidos.
1.4.2.3. Los servidores públicos y contratistas que tengan acceso a la información de la Personería Municipal deben participar en las actividades o iniciativas de concientización en materia de seguridad de la información a las que sea convocado. 1.4.2.4. El incumplimiento de las políticas consignadas en el presente manual podrá generar sanciones disciplinarias.
1.4.2.5. Las políticas de seguridad informática forman parte integral de los contratos de trabajo de los servidores públicos.

1.4.3. Terminación del contrato o cambio de cargo.

1.4.3.1. Servidores públicos y contratistas que finalicen su relación laboral con la Personería Municipal deben entregar a su superior inmediato o responsable, la información de la entidad que se encuentre bajo su responsabilidad y/o manejo. Debe quedar registro de lo anterior en el formato **"PLAN DE ENTREGA DEL CARGO" del Sistema Integrado de Gestión.**
1.4.3.2. La información y el conocimiento desarrollado por los servidores públicos de la Personería Municipal durante el horario laboral y dentro de la vigencia del contrato laboral es propiedad de la entidad, por lo tanto, se prohibe el borrado o la copia de dicha información por parte de servidores públicos y contratistas en proceso de retiro o por personal retirado.
1.4.3.3. Ante la finalización de la relación laboral o contractual de un servidor público o contratista con la Personería Municipal, se deben suspender inmediatamente los permisos de acceso a la plataforma de la entidad.
1.4.3.4. La Dirección de Personal debe informar inmediatamente los retiros o traslados de los servidores públicos, trabajadores oficiales y practicantes, con el fin de revocar o modificar los privilegios de acceso asignados a dicho personal.
1.4.3.5. El superior inmediato de servidores públicos y contratistas es el responsable de gestionar el retiro o modificación de los derechos de acceso ante novedades laborales como la terminación o cambio del contrato.
1.4.3.6. El superior inmediato es el responsable de gestionar el respaldo de la información de los equipos de cómputo de los servidores públicos y contratistas en proceso de retiro.

1.5. POLÍTICA DE SEGURIDAD INFORMÁTICA PARA CONTRATACIÓN.

La información de la Personería Municipal debe ser protegida en el proceso de contratación. Busca proteger los procesos de contratación frente a situaciones que comprometan la disponibilidad, la integridad y la confidencialidad de la información de dichos procesos; resguardando así su legalidad y transparencia.

1.5.1. Disposiciones generales

1.5.1.1. Los servidores públicos y contratistas responsables por los servicios de contratistas o proveedores, son responsables de identificar y valorar los riesgos de la información asociados al acceso de éstos.
1.5.1.2. Los contratos celebrados entre la Personería Municipal y contratistas o proveedores con acceso a la información de la entidad, deben incluir cláusulas para mitigar riesgos de seguridad de la información.

1.5.1.3. Con el fin de proteger la información de ambas partes, se debe formalizar un acuerdo de confidencialidad. El acuerdo deberá definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir.
1.5.1.4. Siempre que haya un proceso de selección que implique la entrega de información Clasificada o Reservada de la entidad, los proponentes participantes deben firmar previamente un acuerdo de confidencialidad.

1.6. POLÍTICA DE SEGURIDAD FÍSICA DE LA INFORMACIÓN Y LOS EQUIPOS DE CÓMPUTO.

Se debe brindar seguridad fisica a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión.

Se pretende proteger la información, así como las tecnologías de información y la comunicación de la entidad frente a incidentes de seguridad causados por condiciones inadecuadas protección fisica, sean estas ambientales o que faciliten el acceso indebido a los activos de información.

1.6.1. Seguridad en las instalaciones

1.6.1.1. Fuera del horario laboral normal o cuando se alejen de sus estaciones de trabajo, los Servidores públicos y contratistas deben despejar sus pantallas, escritorios y áreas de trabajo, de tal manera que los datos, bien sean físicos (como documentos impresos y carpetas) o electrónicos (como memorias USB, Discos Duros Externos, CDs y DVDs), estén resguardados adecuadamente.
1.6.1.2. Cuando un servidor público se percate de la presencia de personas sospechosas en las instalaciones de entidad, debe reportar dicha situación.
1.6.1.3. No se deben prestar ni descuidar los elementos de identificación y acceso a las instalaciones de la Personería Municipal (tales como tarjetas de acceso, camets, llaves y tokens).
1.6.1.4. Cuando se imprima información clasificada o reservada, las impresiones deben ser retiradas inmediatamente.
1.6.1.5. Siempre que sea posible, las impresiones deben ser protegidas por medio de una clave de seguridad.
1.6.1.6. Las reuniones y sesiones de videoconferencias de la Personería Municipal no deben ser grabadas en audio o video a menos que todos los participantes estén al tanto de dicha grabación. En el acta de la reunión debe registrarse que la sesión fue grabada.
1.6.1.7. No está permitido fumar, ingerir alimentos o bebidas en las aulas con equipos de cómputo.

1.6.2. Seguridad de los equipos

1.6.2.1. Los servidores públicos y contratistas de la Personería Municipal son responsables de garantizar la debida protección de los equipos asignados (computadores de escritorio y dispositivos móviles) dentro y fuera de la entidad, lo que contempla su vigilancia, el debido cuidado en su transporte y el uso de cualquier otra medida de seguridad física necesaria.

1.6.2.2. Los equipos suministrados por la Personeria Municipal, como computadores de escritorio y dispositivos móviles (incluye computadores portátiles), no deben ser objeto de alteraciones en su hardware. Toda modificación a los equipos debe ser autorizada y realizada por personal de soporte técnico de los equipos de trabajo de informática.
1.6.2.3. Se debe bloquear la sesión cuando el usuario se aleje del computador. 1.6.2.4. La salida de los computadores (de escritorio o portátiles) de la entidad debe ser autorizada por el secretario general.
1.6.2.5. Toda pérdida de equipos de cómputo o de alguno de sus componentes, debe ser informada.
1.6.2.6. Los equipos de cómputo externos (no entregados por la Personeria Municipal) no deben conectarse a la red de datos de la entidad, a menos que cumplan con los requisitos. (Requisitos por definir).

1.7. POLÍTICA DE CUMPLIMIENTO

La Personería Municipal de Dosquebradas cumple la regulación y legislación vigente aplicable en materia de seguridad de la información. Busca identificar y asegurar el cumplimiento de los requisitos regulatorios y legales aplicables a la entidad en cuanto a la seguridad de la información.

1.7.1. Cumplimiento legal y normativo

1.7.1.1. Será sancionado con las acciones disciplinarias y legales correspondientes, al que utilizare registros informáticos, software u otro medio para ocultar, alterar o distorsionar información requerida para una actividad de la entidad, para el cumplimiento de una obligación respecto al Estado o para ocultar los estados contables o la situación de un proceso, área o persona física o jurídica.
1.7.1.2. Toda la información de ciudadanos o servidores públicos y contratistas que incluya cédulas de identidad, datos de contacto o información financiera debe ser sólo accesible al personal de la entidad que necesite ese acceso en virtud de su trabajo.
1.7.1.3. La realización de auditorías (verificaciones o pruebas de seguridad) no deben afectar la normal operación de los sistemas de información o plataformas.

1.8. POLÍTICA DE SEGURIDAD PARA REDES SOCIALES INSTITUCIONALES

Las redes sociales institucionales deben ser protegidas de situaciones de acceso indebido y publicaciones no autorizadas.
1.8.1. Asegurar el manejo seguro de las redes sociales institucionales, evitando situaciones que puedan afectar la reputación de la entidad derivadas del su uso no autorizado.
1.8.2. Las credenciales de acceso (usuario y contraseña) de una cuenta institucional de redes sociales, solo pueden ser conocidas por un único responsable designado. 1.8.3. Las contraseñas de acceso a las redes sociales institucionales deben cumplir los lineamientos para contraseñas establecidos en el presente documento.
1.8.4. Las contraseñas de redes sociales institucionales deben ser cambiadas cada tres meses como mínimo.

1.8.5. No debe establecerse la misma contraseña a más de una cuenta de redes sociales institucionales.
1.8.6. Se deben cambiar las contraseñas de acceso cada vez que se cambien los responsables del manejo de las redes sociales institucionales.
1.8.7. Copias de las credenciales de acceso a las redes sociales institucionales (usuarios y contraseñas) deben ser puestas en sobres firmados y sellados (un sobre por cada cuenta de redes sociales) estos sobres deben permanecer en un sitio seguro, como una caja de seguridad; de modo que puedan ser utilizados en caso de contingencias con el (los) responsable(s) de las redes sociales.

COMPONENTES DE LA GESTIÓN DOCUMENTAL

Procesos

- Planeación de tratamiento de correspondencia electrónica
- Producción de correspondencia electrónica
- Gestión y Trámite de correspondencia electrónica
- Organización de correspondencia electrónica
- Transferencia de correspondencia electrónica
- Disposición de documentos electrónicos
- Preservación a largo plazo de documentos electrónicos

Instrumentos Archivísticos

- Plan institucional de Archivos
- Programa de Gestión Documental
- Tabla de Retención Documental
- Mapas de procesos
- Cuadro de clasificación documental
- Inventario Documental
- Modelo de requisitos para la Gestión Documental

Clasificación

Todos y cada uno de los documentos electrónicos allegados a la Entidad corresponden a una clasificación puntual que permite dar trámite a los mismos, en este orden de ideas, identificar el tipo de documento de forma oportuna, agiliza los trámites y hace que la Entidad trabaje de forma más eficiente en el marco de una óptima atención a los usuarios.

- **Derecho de petición**: Son todas aquellas peticiones que son remitidas a la entidad, tanto por usuarios particulares como por entidades privadas o públicas, centralizadas o descentralizadas. ***El tratamiento que se le da a esta correspondencia está delimitado según el tipo de petición, el área de la petición y la delegación de la Entidad que debe hacer frente a las solicitudes de los peticionarios.***

- **Requerimiento**: Es la petición de una cosa que se considera necesaria, especialmente el que hace una autoridad, Acto judicial por el que se intima que se haga o se deje de ejecutar algo

- **Informaciones**: Es toda aquella información que es allegada a la Entidad pero que no corresponde una petición y que no obliga a otorgar una respuesta por parte de la Personeria Municipal de Dosquebradas.

- **Invitaciones**: Son las correspondencias que tienen como finalidad, invitar a la Entidad o a sus funcionarios a ser partícipes de procesos de capacitación, de conmemoración, de acciones judiciales o de cualquier otra eventualidad que pueda ser motivo de invitación para la Entidad por parte de usuarios o de entidades tanto públicas como privadas.

- **Otros:** Son todos los documentos que son recibidos por la entidad y que no se clasifican en ninguno de los rótulos anteriores, para este caso, la entidad deberá definir un funcionario que se encargue de cada documento según sus competencias.

Obtención y registro de documentos

La obtención de los documentos es diversa, pues las fuentes pueden ser tanto internas como externas.

Se consideran **internas**, todas aquellas comunicaciones que sean recibidas por la Entidad y que hayan sido creadas por los funcionarios de la misma, éstas pueden ser complemento o parte adicional y fundamental de una comunicación externa, lo anterior no implica que se les deba otorgar un tratamiento especial, sino que, por el contrario, deben seguir el lineamiento que se expondrá más tarde en la presente política.

Ahora bien, se consideran **externas**, todas las comunicaciones que son recibidas por la entidad y cuyo origen son externo a la misma, por ejemplo, correos electrónicos de peticionarios o entidades ajenas a la Personería Municipal de Dosquebradas. En cualquiera de los dos casos mencionados, toda documentación debe ser identificada, clasificada y rotulada con un consecutivo de identificación que permitirá, en etapas posteriores, determinar, no solo la ruta a seguir, sino también, la ubicación de los documentos en el archivo electrónico general de la Entidad.

Identificación documental

Todo documento que sea recibido o emitido por la Entidad debe identificarse, clasificarse y rotularse. Dicho lo anterior, este asunto es fundamental para que la organización documental sea eficiente y el archivo electrónico se encuentre siempre ordenado y cumplimiento con los requisitos planteados y formulados en la presente Política de Gestión de Documentos Electrónicos.

Para lo anterior, la Entidad, de acuerdo con su Plan Institucional de archivos y teniendo en cuenta la metodología de identificación y rotulación con números consecutivos, deberá establecer los lineamientos que permitan unificar los códigos a fin de establecer una secuencia única para documentos electrónicos.

Búsqueda y recuperación documental

Cuando se habla de documentos electrónicos, existe una gran ventaja frente a los documentos fisicos y tradicionales, toda vez que existe una sistematización práctica que facilita la búsqueda, el entendimiento documental y la eficiencia de las entidades que incorporan un archivo electrónico.

La búsqueda y la recuperación documental hace referencia a la capacidad que tiene la Entidad para encontrar, en el universo de datos propios, un documento particular, un expediente o cualquier otro archivo de carácter documental, todo, respaldado por una ruta electrónica dada a partir del conjunto de datos y e ubicaciones para dar con el sitio final donde se encuentra alojado el documento en cuestión.

Metodología de implementación

La **PERONERIA MUNICIPAL DE DOSQUEBRADAS**, reconociendo la importancia de la implementación de la Política de Gestión de Documentos Electrónicos y de integrar los procesos y procedimientos archivísticos, articulará éstos con las normas técnicas respectivas, los programas específicos de la Política de Gestión de Documentos Electrónicos.

Para la implementación del **Sistema de Gestión de Documentos Electrónicos de Archivo - SGDEA,** es necesario trazar metas a corto, mediano y largo plazo que permitan alcanzar el logro de los objetivos planteados en el proyecto para lo cual se deben definir estrategias alineadas con las políticas globales de la entidad y sus necesidades.

Por consiguiente, tanto en los planes estratégicos de la organización como:

Plan institucional de Archivos – PINAR
Programa de Gestión Documental - PGD

Se debe contemplar, incluir y priorizar el desarrollo e implementación del **SGDEA**, sus objetivos y metas definiendo un plan de acción que comprenda cada una de las actividades a desarrollar.

A continuación, se plantean cinco (5) fases que pueden definirse como una ruta de acción que comprende las actividades a desarrollar en un proyecto SGDEA, a nivel estratégico y gerencial, y que involucra actores, responsables y actividades.

1. PLANEACION. En esta fase se debe definir la estructura de desglose de trabajo a alto nivel, el alcance de la implementación del SGDEA, establecer sus objetivos, productos o entregables esperados, los riesgos y cuantificar el tiempo y los recursos que abarcara a partir del análisis de las necesidades de una entidad, hasta la finalización de los procesos implementados.

1.1 ALCANCE	Comprende las actividades orientadas a: establecer las etapas de desarrollo del proyecto de implementación del SGDEA como proyecto y no como solución tecnológica y describir claramente la definición y el control de lo que se va a hacer, hasta dónde; de lo que está y no estará incluido, conforme a la misión; estrategias y metas de la entidad.
1.2 OBJETIVOS	Comprende la formulación de los objetivos a corto, mediano y largo plazo que la entidad pretenda lograr con la implementación del SGDEA, por lo que deben ser

3.1 ESTRATEGIA DE LA IMPLEMENTACION	Todo proceso requiere de la definición de una dirección estratégica clara, concreta y medible, que facilite el cumplimiento de los objetivos planteados.
3.2 ALTERNATIVAS	Todo proceso requiere de la definición de una dirección estratégica clara, concreta y medible, que facilite el cumplimiento de los objetivos planteados.
3.3 ANALISIS DEL MERCADO ACTUAL	se requiere conocer las soluciones existentes en cuanto a gestión documental electrónica y que tanto cumplen con las necesidades requeridas por la organización
3.4 REQUISITOS FUNCIONALES	determinar el nivel de cumplimiento y adaptación respecto de los requerimientos funcionales y no funcionales
3.5 CUMPLIMIENTO NORMATIVO	se requiere verificar el cumplimiento normativo y el nivel de adaptación de la herramienta tecnológica a los requerimientos archivísticos

4. FASE DE IMPLEMENTACION. Una vez se tiene claridad sobre qué procesos o procedimientos se van a automatizar dentro del SGDEA, y se han identificado las necesidades que se pretenden cubrir, se da inicio a la fase de implementación

5. FASE DE EVALUACION Y MONITOREO. monitoreo sobre las actividades de cada una de las fases del proyecto, y su avance según su planificación. Esta fase es de vital importancia porque permite identificar y gestionar los riesgos, enumerar y evaluar los hitos importantes del proyecto SGDEA y documentar los cambios o ajustes que hayan surtido durante su implementación. Dentro de las actividades a contemplar se encuentran actividades que contribuyen a hacerle seguimiento al proyecto SGDEA como a la solución tecnológica que apoya su implementación dentro de las que se encuentran:

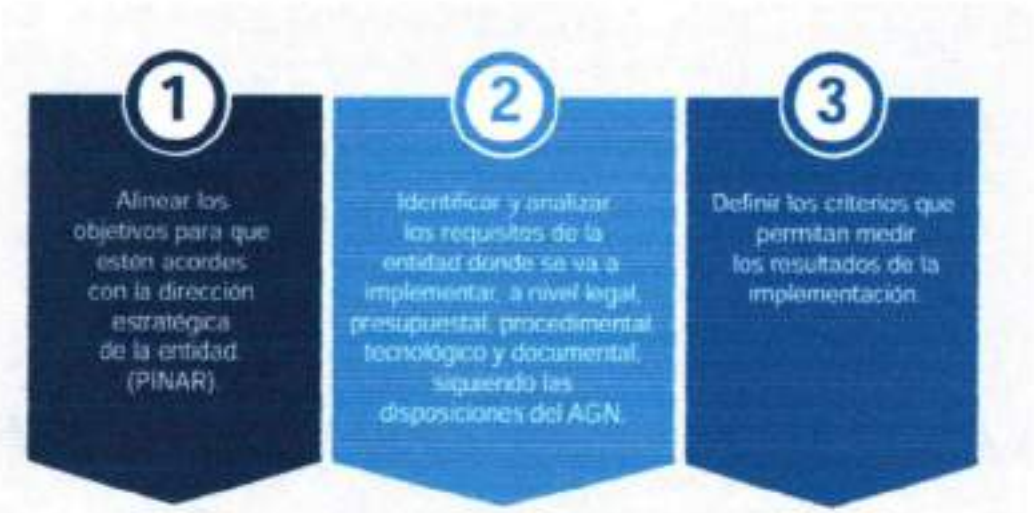
- **Gestión de calidad**
- **Gestión del cambio**
- **Estrategias de mejora**

Teniendo en cuenta que la **PERSONERIA MUNICIPAL DE DOSQUEBRADAS**, recibe con frecuencia en sus canales electrónicos diferentes tipos de comunicaciones, es necesario clasificar tales en diferentes segmentos, toda vez que, a cada uno de esos tipos, se les da un tratamiento particular y diferenciador, factor clave en la estructuración metodológica de la implementación de la presente política.

Así mismo, todos y cada uno de los tipos de comunicaciones recibidas por parte de la Entidad por parte de cualquiera de los tipos de peticionarios, ya sean usuarios o entidades, deben tener un conducto regular que permite, no solo ejecutar satisfactoriamente la política en cuestión, sino también, atender de forma oportuna, eficiente y ágil, las comunicaciones electrónicas recibidas por la Entidad, pues éste es, en síntesis, el objetivo final de la Política de Gestión de Documentos Electrónicos.

Establecimiento de objetivos del SGDEA Comprende la formulación de los objetivos a corto, mediano y largo plazo que la entidad y/o la organización pretendan lograr con la implementación del SGDEA, por lo que deben ser específicos, medibles, alcanzables y con tiempos definidos. Tenga en cuenta que al establecer los objetivos se debe:

	especificos, medibles, alcanzables y con tiempos definidos.
	Identificar y analizar los requisitos de la entidad donde se va a implementar, a nivel legal, presupuestal, procedimental, tecnológico y documental.
1.3 ENTORNO NORMATIVO	es necesario que la entidad analice los estándares internacionales y/o nacionales como las leyes, decretos y políticas existentes en materia de gestión de documentos, seguridad de la información, interoperabilidad, gestión de la calidad, gestión ambiental, entre otros, los cuales en últimas son los que reflejarán una correcta gestión electrónica de documentos.
1.4 ROLES Y RESPONSABLES	Identificar y establecer roles y responsabilidades tanto de la Dirección como responsabilidades operacionales y técnicas enfocadas a un cargo especifico, teniendo en cuenta que el personal que realizará estas actividades sea competente para llevarlas a cabo
1.5 ELABORACION DEL PLAN	Realizar un desglose donde se definan fases o etapas de implementación entregables, tiempos y responsables, esto con el fin de tener un mayor control y/o seguimiento durante la ejecución y de esta forma garantizar que se cumplan los objetivos planteados
1.6 GESTION DEL RIESGO	Tiene como finalidad panificar la gestión de riesgos, es decir, identificar y analizar cada riesgo asociados a la implementación del SGDEA, así como definir las estrategias de monitoreo y control, con el fin de evaluar la probabilidad de ocurrencia, su impacto y la estrategia de mitigación.
2. FASE DE ANALISIS. Comprende las actividades orientadas a conocer la estructura general de la entidad y a determinar la necesidad de información desde cuatro perspectivas: organizacional, normativo, tecnológico y documental. Cada uno de estos análisis se puede desarrollar en paralelo porque uno no influye sobre el otro, sin embargo, si se complementan.	
2.1 ANALISIS ORGANIZACIONAL	identifica la estructura organizativa de la entidad, sus relaciones y la definición de funciones y responsabilidades
2.2 ANALISIS TECNICOS	Comprende las actividades orientadas a identificar los aspectos técnicos y tecnológicos de la entidad. El resultado de esta fase permitirá determinar si la infraestructura actual soporta la implementación del SGDEA en el caso contrario la entidad deberá definir las acciones y aspectos requeridos para garantizar la ejecución y puesta en marcha del proyecto
2.3 ANALISIS DOCUMENTAL	Consiste en determinar el estado actual de cada uno de los procesos de la gestión documental, incluyendo la identificación de los documentos su estructura y formatos, así como la verificación del nivel de aplicación de los instrumentos archivísticos
2.4 DIAGNOSTICO DOCUMENTAL	Para realizar el diagnóstico de la gestión documental se deben tener en cuenta los siguientes elementos y herramientas, verificando si este paso ya se llevó a cabo durante las etapas previas y necesarias para la construcción de los instrumentos archivísticos como el PINAR y el PGD
2.5 IDENTIFICACION DE LOS DOCUMMENTOS	Los documentos vitales y/o esenciales de una organización, constituyen uno de los activos de información más valiosos que permiten la reconstrucción sus actividades aun después de su desaparición, por lo cual su identificación resulta un factor importante y necesario a tener en cuenta para la gestión de su ciclo vital dentro del SGDEA
3. FASE DE DISEÑO. se define la estrategia de implementación del SGDEA, se hace el desglose de fases y se realiza una proyección generando un análisis de alternativas y soluciones garantizando la adquisición de una solución escalable, interoperable, segura, funcional y sostenible financiera y técnicamente.	



JOHN EDISON PARRA SANCHEZ
Secretario General

PROYECTO: Maria Gilma Manrique Noreña Jefe Control Interno	REVISO: John Edison Parra Sánchez Secretario General	RECIBIDO POR: _____ Dia___Mes___Año_____Hora____