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 especifico, 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 archivistico.

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

a) Contener información de cualquier naturaleza o indole, 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 politicas 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 Personería 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 de Itagüí 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 prohíbe 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 física 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 física, 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, carnets, 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 Personería 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 Personería 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 Personería 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 físicos 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.