1. Información General

MGGTI.G.UA - USO Y APROPIACIÓN DE TI

OAI Avanza
Oficina Asesora de Informática

2. Introducción

Desde la Oficina Asesora de Informática en el marco de MIPG y como responsables de las políticas de gestión y desempeño Gobierno Digital y Seguridad Digital, se pretende mediante la presente estrategia realizar el seguimiento y monitoreo de la implementación de la Política de Gobierno Digital y Seguridad Digital; ejercer los controles como Segunda Línea de Defensa en el cumplimiento de la política de administración del riesgo, a través de tomas o brigadas en las oficinas y dependencias para validar que todos los funcionarios y contratistas del Distrito pongan en práctica todo lo concerniente y establecido en dichas políticas.

También se busca con la implementación de "**OAI Avanza**" ser una segunda fase del Habilitador de la Política de Gobierno Digital, Cultura y Apropiación Interna, con el firme objetivo de realizar seguimiento a los conocimientos adquiridos sobre las herramientas tecnológicas por parte de funcionarios y contratistas.

De igual forma un tercer componente de la estrategia busca garantizar con el personal técnico del Nivel de Soporte 1 y 2 el correcto funcionamiento de los equipos y recursos tecnológicos utilizados por todos los funcionarios y contratistas, para el cumplimiento de las funciones y obligaciones contractuales en toda la entidad.

3. Glosario:

- **Accesibilidad:** Es una característica deseable en las páginas web e interfaces gráficas de los sistemas de información que consiste en la posibilidad que tiene un usuario de acceder a un sitio web y navegar en él, sin importar que cuente con algún tipo de discapacidad.
- **Activo:** Cualquier cosa que tenga valor para la entidad ya sea tangible o intangible. Existen diversos tipos de activos en una entidad como: información, software, hardware, tramites o servicios, recurso humano con sus aptitudes, habilidades, y experiencia, reputación o Imagen organizacional.
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Arquitectura empresarial:** práctica estratégica que consiste en analizar las entidades desde diferentes perspectivas o dimensiones, para obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria**.** El objetivo es generar valor a través de las Tecnologías de la Información para

que se ayude a materializar la visión de la entidad. Cuando se desarrolla en conjunto para grupos de instituciones públicas, permite además asegurar una coherencia global, que resulta estratégica para promover el desarrollo del país.

- **Arquitectura de TI:** De acuerdo con el Marco de referencia de Arquitectura empresarial del estado, define la estructura y las relaciones de todos los elementos de TI de una organización. se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de T. (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).
- **Arquitectura de TI sectorial:** Es el análisis integral y estratégico de un sector de la administración pública (salud, educación, tic, entre otros) basado en los dominios del Marco de Referencia de Arquitectura Empresarial, con el propósito de obtener, evaluar y diagnosticar su estado actual y planificarla transformación necesaria que le permita a un sector evolucionar hasta la arquitectura empresarial objetivo.
- **Artefacto:** Es un producto tangible resultante del proceso de diseño y desarrollo de software o arquitectura empresarial. Ejemplos de artefactos son: diagramas de casos de uso, catálogos de sistemas de información, infraestructura tecnológica, mapas de información, entre otros.
- **Capacidad Institucional:** Es una habilidad que debe tener una institución para poder cumplir con la misión y los objetivos que se propone. Se entiende que se tiene la capacidad cuando se posee procesos, infraestructura y talento humano con las competencias requeridas para prestar los servicios que debe proveer.
- **Ciudad o territorio inteligente:** Aquella que tiene una visión holística de sí misma, y en la cual sus procesos estratégicos y la provisión de servicios urbanos se basan en la promoción del desarrollo sostenible y la innovación, y en el uso y aprovechamiento de las TIC, con el propósito de aumentar la calidad de vida de los ciudadanos.
- **Confidencialidad:** Se refiere a que la información solo puede ser conocida por individuos autorizados.
- **Datos abiertos:** Son aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- **Estado abierto:** Es una modalidad de gestión pública más transparente, sujeta a rendición de cuentas, participativa y colaborativa, entre Estado y sociedad civil, donde el Estado hace posible una comunicación fluida y una interacción de doble vía entre gobierno y ciudadanía; dispone canales de diálogo e interacción, así como información para los ciudadanos con el fin de

aprovechar su potencial contribución al proceso de gestión y la ciudadanía aprovecha la apertura de esos nuevos canales participativos, podrá colaborar activamente con la gestión de gobierno, promoviendo de este modo una verdadera democracia. El Estado no solo hace referencia a la rama ejecutiva, sino a la rama legislativa, judicial y órganos de control.

- **Gestión de T.I.:** Es una práctica, que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI). A través de la gestión de TI, se opera e implementa todo lo definido por el gobierno de TI. La gestión de T.I. permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas.
- **Gobierno Digital:** Consiste en el uso de las tecnologías digitales como parte integral de las estrategias de modernización de los gobiernos para crear valor público. Esto depende de un ecosistema de actores gubernamentales, ONG, empresas, asociaciones ciudadanas e individuos que dan soporte a la producción de y acceso a datos, servicios y contenido a través de interacciones con el gobierno. En Colombia, Gobierno Digital es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones -Ministerio TIC, que tiene como objetivo "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".
- **Integridad:** Se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. · Lineamiento: Es una directriz o disposición obligatoria para efecto de este manual que debe ser implementada por las entidades públicas para el desarrollo de la política de gobierno digital. Los lineamientos pueden ser a través de estándares, guías, recomendaciones o buenas prácticas.
- **Manual de Gobierno Digital:** Documento que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de la Política de Gobierno Digital en Colombia, el cual es elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de Planeación.
- **OAI:** Oficina Asesora de Informática
- **Sede Electrónica:** Es una dirección electrónica que permite identificar la entidad y la información o servicios que provee en la web, a través de la cual se puede acceder de forma segura y realizar con todas las garantías legales, los procedimientos, servicios y trámites electrónicos que requieran autenticación de sus usuarios. (Decreto 1078 de 2015, articulo 2.2.17.7.1).
- **TIC:** Tecnologías de la información y Comunicación

4. Responsabilidad y Autoridad

Jefe Oficina Asesora de Informática

5. Política de Operación

- El presente documento se rige por lo establecido en las políticas institucionales de gestión y desempeño gobierno y seguridad digitales.
- La Oficina Asesora de Informática verificara el correcto uso de herramientas tecnológicas institucionales como el sistema de transparencia y gestión documental Transdoc – Sigob, Microsoft Teams, One Drive, SharePoint, SIC entre otras.
- La Oficina Asesora de Informática como miembro de la segunda línea de defensa en la Política de Administración de riesgos, debe garantizar el cumplimiento de los controles establecidos.
- Todas las intervenciones de soporte técnico de nivel 1 y 2 deben ser registradas en el gestor de Servicios de TI – SAUS
- Cada Intervención debe finalizar con informe, plan de mejoramiento y actas de compromisos pactados.
- La estrategia de Agentes de Soporte estará enmarcada por lo establecido en los procedimientos e instructivos del subproceso de Mesa de Servicios.
- En todas las intervenciones se debe promover la política de cero papel.

6. Definición de la Estrategia

La presente estrategia aborda las políticas de gobierno digital, seguridad digital y su puesta en práctica en cada una de las oficinas y dependencias del Distrito de Cartagena.

A continuación, se detalla la estrategia **OAI AVANZA** en cada uno de sus componentes.

La estrategia consiste en conformar un Equipo interdisciplinario de la Oficina Asesora de Informática para realizar unas jornadas presenciales a la oficinas y dependencias adscritas a la Alcaldía de Cartagena. Con esto se busca identificar de primera mano cómo los funcionarios y contratistas utilizan las herramientas tecnológicas disponibles en distrito con el fin de validar los conocimientos adquiridos en los procesos de capacitación e inducción en el uso de las herramientas. De igual forma se busca validar que los funcionarios y contratistas pongan en práctica todos los lineamientos establecidos en las Políticas de Gobierno Digital y Seguridad Digital. Un aspecto importante que

busca la estrategia es validar el cumplimiento de todos los controles de seguridad establecidos en el mapa riesgos además de realizar un seguimiento como segunda línea de defensa de acuerdo con la política de administración de riesgos de la Alcaldía Mayor de Cartagena.

Las jornadas presenciales se realizarán según un cronograma donde previamente se le notificará mediante oficio a la oficina o dependencia, con el fin de evitar interferir en cualquier actividad critica que esté adelantando para la fecha establecida, y a su vez estén presente todos los funcionarios y contratistas que la conforman.

EL día de la intervención el líder de cultura y apropiación de la OAI debe hacer la presentación ante el jefe de las dependencias, funcionarios y contratistas explicando en qué consiste la actividad a desarrollar y cuáles son los temas a tratar.

6.1 Componentes de las Estrategias

OAI AVANZA se divide en tres componentes, la cual se darán los conceptos y cómo se debe validar cada uno de ellos.

- **Guardianes Digitales**
- **Inspectores TIC**
- **Agentes de Soporte**

6.1.1 Guardianes Digitales

Esta estrategia busca garantizar la puesta en práctica de los lineamientos emitidos por la Oficina Asesora de Informática, previamente ya aprobados por el Comité de Gestión y Desempeño Institucional en las políticas de gobierno y seguridad digitales. El personal de la OAI para esta estrategia debe enfatizar y validar la importancia del tratamiento de los datos, seguridad digital y los controles que se deben tener.

Además, se busca mitigar los riesgos asociados al uso de la tecnología desde el usuario final garantizando que se cumplan las Políticas Institucionales y sus riesgos asociados. En todo riesgo detectado se debe levantar un acta de compromiso y seguimiento.

Al iniciar el cuestionario se le debe preguntar al usuario si ha recibido información, capacitación de la Política de Gobierno Digital y Seguridad Digital, luego se

procede con las preguntas de acuerdo con el documento de diagnóstico, las preguntas van enfocadas hacia los siguientes temas:

- **Conocimiento de políticas:** Preguntar a los funcionarios si conocen la política Digital, Política de seguridad digital, Política de cero papel.

- **Credenciales de Acceso:** Se debe resaltar sobre la importancia de no revelar las credenciales personales a otra persona. Cómo establecer una contraseña segura, autenticación de dos factores y demás buenas prácticas de credenciales seguras. incentivar el uso adecuado de contraseñas, las cuales deben cumplir con unos criterios mínimos de seguridad (más de 8 caracteres, combinación de letras mayúsculas y minúsculas, caracteres especiales, números)

- **Uso de redes sociales:** Insistir e incentivar el uso correcto de redes sociales donde no se publiquen contenidos que expongan datos personales que atenten contra la integridad de los dueños del dato.
- **Correo Institucional:** Verificación de credenciales, que las contraseñas cumplan con los requisitos mínimos de seguridad, verificar que no se utilice el correo institucional para el envío de información personal, resaltar en que toda la información que aquí reposa es de propiedad de la Alcaldía de Cartagena, informar que terminada la vinculación laboral el correo se restringirá para el actual responsable.

- **Uso adecuado de los medios de almacenamiento:** Se debe verificar que la información o datos institucionales se esté guardando de manera adecuada en los repositorios que brinda la Entidad (SharePoint, OneDrive)

- **Uso de Herramientas de Colaboración:** Incentivar el uso de las herramientas de colaboración (Microsoft Teams) para que usted y su equipo estén informados, organizados y conectados

6.1.2 Inspectores TIC

Esta estrategia está orientada a garantizar el correcto uso de las herramientas tecnológicas institucionales utilizadas por funcionarios y contratistas, este mecanismo es un segundo momento después del proceso de capacitación interna que busca afianzar el correcto uso de herramientas como SIGOB, Microsoft Teams, SIC entre otras herramientas disponibles en el Distrito.

Los Inspectores TIC harán uso del formato Excel checklist: Diagnostico de Seguridad Digital.

Sistemas de Transparencia de Gestión Documental Transdoc – Sigob: Transdoc-Sigob es la herramienta de comunicación oficial del Distrito de Cartagena de Indias D.T y C., en este sistema se genera gran cantidad de documentación en todas las dependencias y es la herramienta de mayor uso, por ende, es fundamental el correcto uso durante todo el flujo de la correspondencia.

Basadas en las estadísticas de los últimos años existe un mal procedimiento en la utilización de este sistema lo que ha llevado a errores, correspondencias perdidas entre otros problemas derivados del mal uso. De ahí la importancia y especial interés en la sensibilización y correcta apropiación de este sistema.

Antes de comenzar una brigada en una dependencia se le debe solicitar un informe de gestión de dicha dependencia para el estado general de todos los funcionarios y contratitas adscritos a esta, para abordar inicialmente aquellas personas identificadas con mayores falencias en el uso de Transdoc. Toda vez que se cuente con este informe se deben abordar a las personas con los siguientes temas.

Utilizar el formato Excel checklist: Diagnostico de uso de Transdoc para evaluar los siguientes aspectos.

- **Credenciales de Acceso:** se debe garantizar que el usuario de SIGOB que este usando el funcionario o contratista es el asignado. Recalcar la importancia de que los usuarios son únicos e intransferibles y los riesgos asociados a la transferencia o préstamo de este usuario y contraseña.

- **Bandeja Interna:** Se debe validar que se le esté dando respuesta a través de derivadas de toda la correspondencia interna y su posterior gestión para mantener esta bandeja al día.

- **Bandeja Externa:** Se debe validar se le esté dando respuesta a través de derivadas de toda la correspondencia externa y su posterior gestión para mantener esta bandeja al día. Esta correspondencia es de especial atención pues es la correspondencia PQRSD (Peticiones, Quejas, Reclamos, Sugerencias y Denuncias) de la ciudadanía y entes de control (Fiscalía, Contraloría, procuraduría, etc)

- **Bandeja en elaboración:** Se debe validar el estado de esta bandeja, como se redactan derivadas y oficios para dar respuesta o hacer solicitudes. Hacer énfasis que esta es una bandeja temporal que no debe tener mayor correspondencia salvo aquella relacionada que se le está dando respuesta por derivada o elaboración de una nueva correspondencia.

- **Tramitada a Revisar:** se debe validar esta bandeja de especial atención pues se tienden a confundir pues algunas personas asumen que la correspondencia ya se encuentra tramitada porque ya cuenta con un consecutivo, Ejemplo “AMC-OFI-0000425-2025”, se debe hacer énfasis que cuando esté en este estado, la correspondencia aún está en estado de borrador, sujeta a cualquier modificación hasta tanto no se tramite.

- **Para Firmar:** se debe validar el estado de esta bandeja donde reposan los oficios en espera de firma del emisor, se debe aclarar que solo les aparecerá correspondencia a quienes tengan opción de firmar documentos y sean remitidos a esta opción por él o por sus subalternos si es el caso de un usuario jefe de dependencia o líder de programa.

- **Firmar Correspondencia:** Se debe validar con el usuario la importancia de esta opción haciendo énfasis que este es el punto donde la correspondencia es tramitada y se deja la trazabilidad de esta. Se le debe recalcar al usuario que este es el punto donde la correspondencia se convierte en PDF y se remite el destinario interno o externo.

- **Derivadas y Precedentes:** Retroalimentación de la importancia de las derivadas para establecer una respuesta a un oficio interno o externo y de esta forma garantizar que no se pierda la trazabilidad o el fujo de la correspondencia desde la solicitud hasta la respuesta. Se debe enfatizar en la importancia de responder oficios a sus precedentes para responder por el mismo medio en que llego el oficio. Se le debe recortar como enlazar un oficio con un precedente con una derivada si por omisión u olvido no estableció al momento de redactar una respuesta.

- **Transferencias:** Se debe resaltar esta opción de transferencia dado que se tiende a confundir con tramitar correspondencia. Se le debe recordar al usuario no es recomendable solo transferir correspondencia sin tramitar entre usuarios de la misma área. Las transferencias a otras dependencias se deben realizar siempre y cuando el oficio se encuentre tramitado y sea de usuario de jefe a jefe.

- **Búsquedas Internas y Externas:** son dos de las tres opciones que maneja la búsqueda en archivo, la otra opción es Todo, donde están inmerso lo externo y lo interno. Cabe anotar que en el archivo solo se encuentran las correspondencias que se han finalizado. En lo externo, todo lo codificado con el Codificador EXT y lo Interno todo lo codificado con AMC.

- **Numero de Correspondencias por Bandejas**: esta opción, permite al jefe de la oficina o secretario mirar el estado de las bandejas de su personal a cargo.

- **Verificación de Codificadores y Formatos:** Se debe validar con el usuario que tenga habilitados todos los codificadores y formatos necesarios para el cumplimiento de sus actividades y funciones diarias.

- **Malas Prácticas:** El funcionario no debe prestar sus credenciales de SIGOB para el desarrollo de sus funciones y obligaciones (salvo la delegación del jefe a una persona de su entera confianza), no se debe trabajar o tramitar correspondencias con varias sesiones, es decir, un despacho no lo puede estar manejando varias personas, pues no va a haber un responsable en caso de error en un trámite.

Microsoft Teams

Es una potente herramienta cuyo principal objetivo es la colaboración en equipo, siendo su principal función la mensajería empresarial u organizacional para comunicarnos y colaborar no solo con miembros de nuestra propia organización, sino también de fuera de ella.

- **Reunión de equipos**: donde se reúnen o agrupan los funcionarios o contratistas de un mismo proyecto o área. De esta manera la app les permite comunicarse entre ellos en tiempo real. Se debe verificar que los funcionarios sepan programar reuniones.

- **Chat**: fácil y sencillo. Como bien indica el nombre, la función del chat sirve para comunicarse con otros miembros del grupo de trabajo sin que el resto se entere. Se debe verificar que los funcionarios usen y se apropien de esta herramienta que es de mucha utilidad.

- **Llamadas**: Con esta opción podemos llamar tanto a otros miembros del grupo como clientes externos, ya sea por voz o por videollamada. Se debe verificar que sepamos y podamos hacer llamadas.

- **Reuniones en línea**: una de las funciones estrella de Teams es la de poder hacer reuniones en línea entre los miembros de un mismo grupo, e incluso añadir personas terceras. Verificar que los funcionarios usen y se apropien de esta opción que brinda la herramienta.

- **Archivos**: con Microsoft Teams compartir archivos entre los diferentes miembros es realmente sencillo. Además, se pueden borrar, cargar nuevos archivos, editarlos e incluso compartirlos con otros miembros. Todo ello desde la propia interfaz sin necesidad de herramientas externas. Verificar que usen y se apropien de esta opción que brinda la herramienta.

Correo institucional

Outlook es un gestor de información personal desarrollado por Microsoft, disponible como parte de la suite **Microsoft 365** (antes **Office 365**).

Microsoft Outlook puede usarse como aplicación independiente para trabajar día y noche, para dar servicios a múltiples usuarios en una organización, como buzones compartidos, calendarios comunes, etc.

- **Direcciones de correo personalizadas:** Las cuentas empresariales o corporativas del correo Microsoft 365, Outlook, son claves para brindarle personalización a sus mensajes. De esta forma evita que los correos terminen en la bandeja de spam o sean difíciles de identificar. Verificar que los funcionarios estén familiarizados e incitar la apropiación con esta opción.

- **Movilidad:** ha motivado un esquema laboral multiplataforma, desde revisar la bandeja del correo electrónico en una cafetería hasta responder a los mensajes importantes desde la Tablet o celular mientras está en casa. Verificar que los funcionarios estén familiarizados e incitar la apropiación con esta opción.

- **Orden:** Con una solución inteligente como el correo Institucional usted y sus equipos pueden organizar mejor su bandeja de entrada**,** así como marcar las conversaciones más importantes y tener a mano los mensajes claves para no invertir más tiempo en búsquedas de emails. Verificar que los funcionarios estén familiarizados e incentivar la apropiación con esta opción.

- **Cero filtraciones y pérdidas de datos:** Con las cuentas de correo electrónico corporativo usted, tiene la confianza de respaldar los datos, gracias a opciones personalizadas es posible recibir notificaciones cuando haya riesgo de filtración de información confidencial o sensible como números de tarjetas de créditos y estrategias. Verificar que este tipo de opciones también estén al alcance de los funcionarios y se apropien de ella.

- **Escalabilidad en el almacenamiento**: Con el uso y apropiación de nuestro correo institucional se acabaron las quejas por la poca capacidad de almacenamiento que se presenta en los correos gratuitos. Se debe exponer a los funcionarios y contratistas esta bondad que ofrece la herramienta.

SAUS

Es una herramienta tecnológica en la cual se realiza la trazabilidad de incidencias y requerimientos provenientes de los funcionarios y contratistas de las diferentes dependencias de la Alcaldía Mayor de Cartagena. Esto significa que todos los datos importantes, como incidentes, problemas, cambios, solicitudes y soporte técnico se registran y documentan en un solo lugar.

- **Estadísticas y reportes:** La generación de los datos proporciona informes y análisis que ayudan a la alta dirección a tomar decisiones con mayor rapidez y precisión basadas en el análisis de los datos almacenados.

- **Automatización en los procesos de TI**: Ofrece una serie de herramientas que pueden optimizar significativamente los procesos de gestión de servicios de TI. Desde la creación automática de los tickets hasta la asignación de los casos a los ingenieros de soporte técnico, también ayuda a agilizar los flujos de trabajo y contribuye a reducir los errores humanos y a mejorar la eficiencia general del equipo de TI.

- **Incidencia:** Se define como cualquier tipo de interrupción en los servicios de TI. Para el caso de la Alcaldía Mayor de Cartagena y la Oficina Asesora de Informática se toma como todos los casos impliquen la no operatividad funcional que involucren a los usuarios finales y los procesos administrados por dicha dependencia.

- **Requerimiento:** Este proceso según ITIL se refiere a todas las solicitudes que generan los usuarios y que no están asociados a un incidente. En este sentido para la Alcaldía Distrital de Cartagena y la Oficina Asesora de Informática hace referencia a las solicitudes de creación, consultas, peticiones técnicas, y funcionales, administrar, crear y gestionar proyectos asociados a los procesos de Tecnología de la Información y comunicaciones mejorando la satisfacción del usuario al brindarles una solución rápida y accesible.

- **Credenciales de Acceso** La seguridad de los datos y la información confidencial de SAUS, permiten controlar el acceso a la plataforma y restringir ciertas funciones según los roles y privilegios asignados por la Oficina Asesora de Informática - OAI a cada usuario que se crea y conecta a la herramienta. Garantizando que solo las personas autorizadas tengan acceso a información sensible.
- **Integración con Otras Herramientas:** es altamente compatible y se integra fácilmente con la herramienta Fusion Inventory para gestionar el inventario de todos los equipos de cómputo y dispositivos tecnológico, de la Alcaldía Distrital de Cartagena.

Sede Electrónica

La Sede Electrónica de la Alcaldía distrital de Cartagena de Indias representa una herramienta invaluable para los ciudadanos y las empresas, ofreciendo opciones, entre ellas acceso a tramites, servicios, consultas de documentos y estado de procesos. Siendo accesible desde la comodidad de sus hogares o lugares de trabajo, desde cualquier dispositivo conectado a Internet.

- **Agilidad y eficiencia en trámites y servicios**:
    - Permite realizar diversos trámites y solicitudes de manera virtual, sin necesidad de desplazarse presencialmente a las oficinas de la Alcaldía.
    - Reduce tiempos de espera y agiliza el acceso a servicios.
    - Brinda la posibilidad de realizar consultas y seguimiento de trámites en línea.

- **Accesibilidad y transparencia**:
    - Facilita el acceso a la información y servicios de la Alcaldía desde cualquier lugar y en cualquier momento con conexión a internet.
    - Promueve la transparencia en la gestión pública al hacer accesible la información sobre trámites, contratos, procesos y demás actuaciones de la entidad.
    - Permite la participación ciudadana en la toma de decisiones y la veeduría de la gestión pública a través de mecanismos de participación.
    - Personas con discapacidad visual o auditiva pueden acceder a la información.

- **Comodidad y seguridad:**
    - Evita desplazamientos innecesarios y ahorra tiempo.
    - Ofrece un canal de atención seguro y confiable para interactuar con la Alcaldía.
    - Permite realizar pagos en línea de manera segura.

- **Modernización y sostenibilidad**:
    - Contribuye a la modernización del Estado y la prestación de servicios públicos más eficientes.
    - Promueve la sostenibilidad ambiental al reducir el uso de papel y otros recursos físicos.

6.1.3 Agentes de soporte:

Esta estrategia está orientada a garantizar el óptimo funcionamiento de los equipos tecnológicos dispuestos para los usuarios final tales como equipos de cómputo, impresoras, teléfonos IP, conectividad alámbrica e inalámbrica, credenciales de acceso. El equipo de la estrategia validará el estado de los recursos tecnológicos y problemas presentados con el uso de estos, con la finalidad de que sean solucionados en el momento de la intervención y de manera oportuna en el tiempo.

En esta estrategia se garantiza la correcta funcionalidad de los siguientes dispositivos y/o componentes:

Al iniciar la verificación se debe utilizar el documento de diagnóstico condiciones

- **Equipo de Cómputo tipo escritorio:** verificar y hacer un checklist de todos los programas y herramientas que estos deben tener instalados para el uso correcto de sus funciones.

- **Equipo de Cómputo tipo todo en uno:** verificar y hacer un checklist de todos los programas y herramientas que estos deben tener instalados para el uso correcto de sus funciones, además verificar si la conexión es por cable o por wifi.

- **Equipo de Cómputo tipo Workstation:** verificar y hacer un checklist de todos los programas y herramientas que estos deben tener instalados para el uso correcto de sus funciones.

- **Periféricos:** Teclados, Mouse y Parlantes: Verificar que estos estén y funcionen correctamente.

- **Impresoras:** Verificar su funcionamiento, carga de papel en bandeja indicada, sensores, ip, verificar su configuración.

- **Telefonía IP**: Verificar que entren y salgan llamadas, además verificar si conocen la opción de transferir una llamada cuando no sea de su resorte.

- **Conectividad Alámbrica:** Verificar su conexión, verificar navegación, verificar estado del Patch Cord.

- **Conectividad Inalámbrica:** Verificar su conexión, verificar navegación, verificar a que red están conectados.

- **Credenciales de Acceso:** Hacer una verificación con el permiso y autorización del funcionario de sus credenciales, es decir, indicarles que su usuario y contraseña es intransferible, que su contraseña debe cumplir con unos criterios mínimos de seguridad (más de 8 caracteres, combinación de letras mayúsculas y minúsculas, caracteres especiales, números)

- **Conexión energía regulada:** Verificar que los computadores estén conectados en la energía regulada (Faceplate naranja).

Verificar que si tienen regletas, estabilizadores o reguladores de voltajes no estén sobrecargadas. Verificar que en la energía regulada solo estén conectados computadores y/o sus componentes (no planchas, no hornos, no calentadores, etc.)

7. Roles y Responsabilidades

- **Líder de Proceso:** Es el gestor líder de proceso de la Oficina Asesora de Informática que debe articular con el líder de estrategia todas las acciones y temas a tratar durante la intervención, debe suministrar todos los insumos al líder de estrategia para garantizar el cumplimiento de la brigada.

- **Líder de Estrategia:** El líder de estrategia es la persona encargada de liderar el personal de la OAI dispuesto durante la brigada, debe coordinar al equipo de apoyo y velar por la ejecución de la intervención y garantizar que se cumplan todos los objetivos. Además, es la persona encargada de hacer el preámbulo ante el jefe de la oficina atendida o quien se le asigne para atender la brigada.

- **Guardianes, Agentes e Inspectores:** Son los funcionarios y contratistas de la Oficina Asesora de Informática que verificaran el uso de los recursos tecnológicos y el cumplimiento de las políticas objeto de este documento. Además, son los encargados que se dé cumplimiento con la intervención y/o atención del 100% al personal de la dependencia visitada.

- **Enlaces TIC:** funcionarios y/o contratistas al interior de cada Oficina y dependencia del distrito, quienes actúan en calidad de enlace con la Oficina Asesora de Informática, los cuales tienen la función durante la brigada de brindar la información requerida por parte de la OAI y ser facilitadores con el personal de su dependencia.

- **Funcionarios y Contratistas:** Son las personas pertenecientes a la dependencia intervenida quienes deben estar prestos y con disposición de atender y dar información a los agentes y lideres de estrategia a fin de garantizar una correcta apropiación y uso de las herramientas TIC.

8. Documentos de validación

Para la validación de cada componente se cuenta con los siguientes documentos para realizar seguimiento, evaluación, compromisos y acciones de mejora.

- Memorando de Socialización de la estrategia

- Checklist de Evaluación
- Acta de Compromisos
- Formulario de encuesta de satisfacción

9. Plan de incentivos

Como una manera de promover la estrategia e incentivar a todos los funcionarios y contratistas, se reconocerá a dos (02) personas de cada dependencia intervenida, que se caractericen por las buenas prácticas en el uso y apropiación de los recursos digitales a través de una evaluación de apropiación del conocimiento.

- ✓ Preguntas por parte del Equipo OAI

10. Identificación del personal

Todo el personal de la Oficina Asesora de Informática que participe de **OAI AVANZA** debe estar identificado con el chaleco diseñado y gorra, para que todas las dependencias los identifique durante la brigada.

10. Apoyo gráfico

Se contará con elementos visuales "Habladores" los cuales serán ayudas para comprender e incentivar los temas a tratar en la estrategia:

- Utilizo Transdoc-Sigob y adopto sus mejores prácticas
- Conozco la Política de Gobierno Digital
- Soy un funcionario seguro, mis credenciales de acceso son exclusivas
- Solo utilizo correos institucionales en mi trabajo
- Hago mis solicitudes tecnológicas por SAUS
- Utilizo EVA para solucionar mis problemas tecnológicos
- Servicios Tecnológicos ágiles y seguros
- Funcionario digital de éxito
- Mantente siempre conectado y en movimiento

11. Cronograma de Intervención

Ver Documento Anexo del Cronograma de intervención

12. Medición e Indicadores

Para poder medir la planeación, ejecución e impacto de la estrategia se plantearon los siguientes indicadores para retroalimentar la estrategia y realizar acciones de mejora.

Indicadores para medir la Implementación:

- Nivel de Satisfacción de Usuario: Mide el porcentaje de aceptación de la estrategia
- Nivel de Participación: Mide el porcentaje de funcionarios y contratistas que participan en las brigadas.
- Nivel de ejecución de las Actividades: Mide el porcentaje de ejecución de todas las actividades y Temas a tratar en las brigadas
- Nivel de conocimiento del equipo OAI: Mide el nivel de conocimiento que puede recibir el funcionario o contratista.

Indicadores para medir el grado de Conocimiento:

- Nivel de Compresión y Conocimiento: Mide el porcentaje de conocimiento y comprensión de las herramientas de software institucionales.
- Nivel de Uso: Mide la cantidad de sistemas y aplicaciones utilizadas por funcionarios y contratistas.

Indicadores para medir el grado de implementación de las políticas y lineamientos de la Oficina Asesora de Informática:

13. Seguimiento y control de compromisos

En las dependencias donde se evidencie malas prácticas y fallas en controles en los riesgos se debe suscribir un plan de mejoramiento con seguimiento quincenal por espacio de dos meses, pasado este periodo y persisten los problemas se debe remitir el caso al comité institucional de coordinación de control interno para evaluar el caso.

14. Evidencias

En cada intervención realizada se debe realizar toda la evidencia del total de las actividades desarrolladas: Oficio de comunicación a la dependencia, registro fotográfico, Informe general de la actividad, Checklist de validación, actas de compromiso, etc.

Toda la evidencia se debe guardar en el repositorio de Proyecto 2025 Actividad 2.3 Elemento Cultura y Apropiación – OAI Avanza 2025.

15. Conformación de Equipos

Componente Guardianes Digital		
No	**Nombres y Apellidos**	**Rol**
1	Sebastián Hernández	Líder
2	Lucas Pedrozo	Guardian de apoyo
3	Esteban de Jesús Barrios Arroyo	Guardian de apoyo
4	Oscar Vergara	Guardian de apoyo
5	Álvaro Enrique Camargo Vitola	Guardian de apoyo
6		

Componente Inspectores TIC		
No	**Nombres y Apellidos**	**Rol**
1	Claudia Patricia Leottau Sanmiguel	Líder
2	Jair José Sánchez Pérez	Inspector de Apoyo
3	Álvaro Yesid Mouthon Pineda	Inspector de Apoyo

Componente Agentes de Soporte		
No	**Nombres y Apellidos**	**Rol**
1	Silfredo Enrique Godoy Chávez	Líder
2	Alan Flórez	Agente Soporte Nivel 1
3	Kevin David Cuello Niño	Agente Soporte Nivel 1
4	Álvaro Rivas Caballero	Agente Soporte Nivel 1
5	Enrique Luis Giraldo Jaramillo	Agente Soporte Nivel 1

16. Documentos de Referencia

- Política de Gobierno Digital

- Políticas de Seguridad Digital
- Manual de Política de Seguridad Digital
- Política de Cero Papel

17. Control de cambios

FECHA	DESCRIPCION DE CAMBIOS	VERSIÓN
##/##/##	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	1.0

18. Validación del Documento

ELABORADO POR	REVISADO POR:	APROBADO POR:
Nombre: Michael Jack Cohen Arteaga **Cargo: Profesional Universitario Código 219 Grado 33** **Fecha: 16/03/2024**	Nombre: **Edgar Eduardo Hernández Sierra** Cargo: **Asesor Externo** Fecha:	Nombre**: Ernesto José Robles Gómez** Cargo: **Jefe Oficina Asesora de Informática** Fecha: ##/##/####