Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

ESPECIFICACIONES TÉCNICAS

SERVICIO INTEGRAL DE APOYO TECNOLÓGICO A LA PLATAFORMA INFORMÁTICA

VERSIÓN JUNIO DE 2025

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: 604 44 44 144
Conmutador: 604 385 55 55 Medellín - Colombia

1. ESPECIFICACIONES TECNICAS MESA DE SERVICIO

1.1 Generalidades

1.1.1 Lugar de ejecución del servicio

La ejecución del contrato será en la Ciudad de Medellín y sus corregimientos, y tendrá como central de operaciones esencialmente para la Mesa de Servicios el Centro Administrativo Distrital CAD desde donde se deberá coordinar la atención a todas las sedes externas en las que el Alcaldía de Medellín presta servicios.

En los casos en los cuales la prestación del servicio se realice de forma remota, el contratista debe proporcionar las instalaciones para tal fin.

El costo del canal de comunicación que se requiera para servicio remoto será asumido por el contratista.

El contratista deberá disponer de un plan de contingencia para el canal de comunicación que se requiera para el servicio remoto. Se deberán realizar pruebas periódicas de esta contingencia.

1.1.2 Herramientas de trabajo

El Contratista proveerá los equipos de cómputo necesarios para cumplir con las funciones descritas y el Alcaldía de Medellín proveerá las conexiones VPN, Internet (siempre y cuando la conexión sea en las instalaciones de la Alcaldía de Medellín). El cliente debe garantizar el acceso a la red de la Alcaldía de Medellín con todas las respectivas políticas de acceso.

El Alcaldía de Medellín pondrá a disposición la Herramienta de Gestión de Servicios Tecnológicos.

La alcaldía de Medellín proporcionará algunas herramientas para realizar el monitoreo automático de hardware y software con sistema de alertas a los responsables, a nivel de infraestructura y aplicación. Sin embargo, la empresa contratista, en acuerdo con el Distrito, deberá contar con las herramientas de Monitoreo que permitan complementar el servicio y cumplir con el monitoreo en todos los niveles desde la aplicación y el servicio hasta la infraestructura. De las herramientas que provea el contratista, se capacitará y entregará credenciales de usuario al personal de la Alcaldía de Medellín, que esta considere necesario.

Las herramientas de monitoreo ofrecidas por el contratista deberán tener como mínimo las siguientes características:

- Medición de Tráfico de red de internet
- Monitoreo de servidores, switches sedes externas, Dispositivos de red
- Medición de capacidades: CPU / Memoria / Disco
- Generación de alertas al servicio
- Características limitadas de los servicios a monitorear.

1.1.3 Horarios De Prestación Del Servicio

El contratista prestará sus servicios en la jornada establecida por el Distrito. Para los horarios fuera de la jornada acordada, se contará con medios de contacto no presenciales. Los eventos que serán atendidos por fuera de la jornada establecida son aquellos eventos de urgencia o críticos sobre las diferentes plataformas que afectan la operación de los procesos de negocio y la prestación del servicio al ciudadano.

1.1.4 Indicadores de disponibilidad

Se deberá garantizar que los sistemas productivos se encuentren operativos 24x7, cumpliendo con los siguientes indicadores de disponibilidad para cada una de las plataformas y/o servicios tecnológicos.

Plataforma	Forma de cálculo	Indicador de Disponibilidad
Elementos de telecomunicaciones	Elementos activos de red de datos.	99.8%
Telefonía IP	Por servidor	99.8%
Elementos de seguridad	Por Equipo	99.8%

Plataforma de Servidores	Por servidor	99.8%
Servicio de Correo	Por Servicio	99.8%
Servicio de Internet	Por Servicio	99.8%
Servicio de Portales	Por Servicio	99.8%
Servicio de Intranet	Por Servicio	99.8%

1.1.5 Requerimientos atendidos en horario no hábil

Los requerimientos que serán atendidos en horario no hábil son:
Eventos ocurridos que afecten los siguientes servicios:

- Directorio Activo
- Correo
- Internet
- Aplicaciones
- Portales
- Servidores
- Red
- Eventos o incidentes de seguridad informática sobre cualquier plataforma.
- Plataforma de Telefonía Avaya (Si afecta a más de 20 usuarios)
- Plataformas de almacenamiento incluyendo Anywhere
- Bases de datos
- Herramientas de respaldo de información
- Plataforma sobre la que opera SAP (en sus ambientes productivos)

- problemas con el WEB Adaptor
- Plataforma Vmware – Hyperconvergencia
- Los que se requieran de acuerdo con las necesidades de la Alcaldía de Medellín.

Eventos ocurridos en la red que afectan la infraestructura del Distrito:

- Daños en los switchs de piso
- Daños en los servidores de telefonía.
- Daños en los canales de comunicación con el proveedor y/o con sedes externas críticas definidas por el Alcaldía de Medellín, las cuales se determinan de acuerdo con los procesos que allí se realicen, por tanto, estas pueden variar de acuerdo con la reorganización de las dependencias del Distrito, entre otros.

Cualquier otra clase de solicitud realizada en horario no hábil y que no se considere de carácter urgente para la entidad, será registrada y comenzará a ser atendida a primera hora del siguiente día hábil. El ANS para estas solicitudes comenzará a contar a partir de este momento, excepto aquellos requerimientos que surjan fuera del horario laboral establecido por la Alcaldía de Medellín y tengan carácter urgente o críticas para la entidad, las cuales serán costeadas mediante una bolsa de horas.

1.1.6 Requerimientos y/o solicitudes urgentes, por fuera de horario no hábil

Los requerimientos a que se refiere este numeral, están relacionados única y exclusivamente con aquellos que se presentan con un carácter urgente o crítico para la entidad; que generalmente son solicitudes o requerimientos nuevos, que no fueron programados o visualizados y además es necesario intervenirlos por fuera del horario laboral.

Para estos casos, el proveedor deberá garantizar los recursos necesarios para atender el desarrollo de las actividades correspondientes a los requerimientos de este tipo, frente a los servicios ya contratados.

Estos requerimientos serán atendidos a través de una bolsa de horas (50 horas mensuales), las cuales pueden ser prestadas por una persona o tercero que contrate el proveedor. Considerando que la ejecución de estas mismas horas se realizará acorde a las actividades de cada uno de los servicios, los planes y cronogramas establecidos así:

Las horas son acumulables entre los meses en que sean distribuidas las actividades; de no ejecutarse la totalidad de horas para el mes en curso, su saldo se acumulará para los periodos siguientes.

Las horas serán liquidadas por consumos mensuales, acorde a los informes de ejecución presentados en el informe mensual de seguimiento de actividades del contrato.

Las solicitudes de servicio deben ser realizadas por el personal autorizado como canal de comunicación entre el contratista y el Alcaldía de Medellín, a través de la herramienta o en su defecto a través del correo electrónico o herramientas colaborativas (TEAMS), y deberán ser formalizadas en la herramienta de gestión, quedando registradas como requerimientos o cambios.

En caso de que el servicio no se pueda prestar de manera remota o virtual, se contará con un tiempo de dos (2) horas para el desplazamiento a la sede que requiere la respectiva atención.

Una vez atendida y solucionada la solicitud se tendrá un plazo de (2) días hábiles para documentar el caso.

1.1.7 Consideraciones

- La bolsa de horas del soporte se podrá utilizar en el horario de lunes a viernes de 6 PM a 7 PM. Si se requiere realizar una actividad por fuera de este horario el consumo de horas será de la siguiente forma:
- Lunes a viernes después de las 7 PM, se descontarán 1.25 horas por hora laborada.
- Sábados, se descontarán 1.5 horas por hora laborada.
- Domingos o festivos se descontarán 2 horas por hora laborada.
- La duración mínima de un servicio en sitio es de 1 hora.
- La duración mínima de un servicio remoto es de 1 hora.
- El número de traslados mensuales de equipos de cómputo es de 200, si no se completan, serán acumulativos durante la ejecución del contrato.
- El número de instalaciones de equipo de cómputo por mes es de 200, si no se completan, serán acumulativos.
- El número de instalaciones y/o traslados de teléfonos por mes es de 60, si no se completan, serán acumulativos.
- Todo el personal dispuesto para la ejecución del proyecto deberá prestar el servicio de forma exclusiva para el Distrito de Ciencia y tecnología de Medellín.
- Con la finalidad de garantizar la total ejecución de los recursos del contrato, en la conciliación de facturación mensual se establecerán los saldos no ejecutados por descuentos por disponibilidad, ANS, servicio no contratado, etc. La destinación de los

mencionados saldos podrá usarse en la continuación de servicios y/o suministros del objeto del contrato previa factibilidad técnica y económica y aprobación entre las partes.

- Teniendo en cuenta que estas especificaciones técnicas están diseñadas en servicios y no se garantiza recursos dedicados al proyecto, la Alcaldía de Medellín podrá verificar en cualquier momento que el recurso humano cuenta con la idoneidad para desempeñar las actividades de los servicios.

1.1.8 Descripción de la experiencia laboral y académica

Las especificaciones técnicas están diseñada bajo el modelo de servicios operativos, por lo cual el contratista garantizará que los recursos humanos sean idóneos y estén preparados para cumplir con los requerimientos propios de la operación en cuanto a disponibilidad e indicadores de calidad para la prestación del servicio.

El personal que ejecutará las labores de nivel 1 serán como mínimo: técnicos con experiencia de 1 año.

El personal que ejecutará las labores de nivel 2 serán como mínimo: ingenieros o profesionales con carreras afines con experiencia de dos años en las plataformas que se administren u operen. Dentro de los equipos de trabajo se contará con personal capacitado en la administración de las plataformas y certificado en caso de requerirse.

La experiencia laboral y académica será verificada durante la ejecución del contrato.

Es responsabilidad del contratista la verificación de la idoneidad de los diplomas y certificaciones de todo el personal contratado. En caso de que se llegue a comprobar la contratación de personas que incumplan con algún diploma o certificación, el Distrito tomará las medidas que desde lo legal apliquen.

El contratista deberá presentar toda la estructura de servicios, que permita desarrollar sus actividades cumpliendo con los indicadores y ANS establecidos y sin detrimento de la prestación del servicio contratado. ***En todo caso, la formación profesional y experiencia laboral serán verificadas por la Alcaldía de Medellín, al igual que la estructura presentada por el contratista.***

1.2 Mesa de servicio

Concebida como una plataforma de servicio especializada que reúne un grupo de recursos, que de manera integral y a través de uno o varios medios de contacto, ofrece la posibilidad de gestionar y dar solución a las solicitudes de los usuarios que en materia de Tecnología de Información puedan presentar, con el objeto de lograr un máximo nivel de productividad de los integrantes de la entidad y el mayor grado de disponibilidad de los recursos informáticos, tecnológicos y de comunicación que éstos emplean en su gestión diaria.

La Mesa de Servicios y el soporte a las TIC debe operar bajo una estructura integral compuesta por un modelo operacional, organizacional y de gestión que optimice la ejecución y haga disponible el 100% del conocimiento del personal con el apoyo de una red de especialistas que ofrezcan el servicio de mesa de servicio, canalizando todas las solicitudes y atendiéndolas oportunamente, buscando el menor impacto para la operación normal del Municipio, a través de las mejores prácticas fundamentadas en ITIL en su última versión.

Entre las actividades que por la naturaleza de una Mesa de Servicios se deben cumplir, se consideran de gran importancia las siguientes:

- Gestión de Incidentes y Requerimientos
- Mantenimientos preventivos
- Gestión de Problemas

El equipo de la Mesa de Servicios no registrará datos o actualizará la configuración definida en el ERP ni en los aplicativos propios de las diferentes dependencias de la Alcaldía de Medellín, deben acoger las Políticas y lineamientos definidos para Tecnología de Información por la Subsecretaría de Servicios de Tecnologías de la Información.

NOTA: El contratista no podrá cerrar unilateralmente un caso sin que se haya resuelto o se tenga una justificación técnica para realizar dicho cierre. Deberá en todo momento prestar el servicio y no podrá negarse al mismo.

1.2 Estructura de la mesa de servicio

La siguiente es la estructura planteada para la prestación de los servicios requeridos:

NOMBRE SERVICIO
Servicio de Mesa de Ayuda nivel 1
Servicio de monitoreo del Datacenter del CAD y las plataformas tecnológicas
Servicio de mantenimiento y soporte, reemplazo de partes de equipos de cómputo
Servicio de soporte a Soluciones de Microservicios (Servicio de Implementación de Soluciones DEVOPS)
Servicio de soporte a Soluciones de Microservicios - automatización de despliegues (SRE))
Servicio de soporte a contenedores de aplicaciones de microservicios
Servicio de soporte a contenedores de aplicaciones monolíticas
Servicio de administración y soporte especializado de la plataforma de almacenamiento
Servicio de gestión de solicitudes de las plataformas de almacenamiento y de los Switch's SAN
Servicio de administración de las plataformas de backup
Servicio de administración y soporte especializado de la Plataforma de servidores
Servicio de administración y soporte básico de servidores
Servicio de administración y soporte especializado de directorio activo y DNS
Servicio de administración de la plataforma AIX
Servicio de administración de bases de datos SQL server y bases de datos no relacionales NoSQL: MongoDB y CrateDB
Servicio de administración y soporte especializado de Bases de Datos PostgreSQL, MariaDB y Oracle
Servicio de Gestión y administración de la red de datos
Servicio de gestión de Enlaces de datos
Servicio de administración de la plataforma de telefonía IP
Servicio de administración de la plataforma de datos abiertos
Servicio de gestión de seguridad informática en redes de datos y telecomunicaciones
Servicio de gestión de seguridad informática en bases de datos
Servicio de gestión de seguridad informática en servidores
Servicio de gestión de seguridad informática en aplicaciones

Servicio de gestión de seguridad informática en protección de punto final
Servicio de gestión de seguridad informática en detección y respuesta
Servicio de gestión de seguridad informática en el control de acceso de usuarios con cuentas privilegiadas
Servicio de gestión de seguridad de protección y filtrado en la Nube

Notas:
Se definirá de común acuerdo entre las partes y mediante acta la sede para prestar el servicio de manera remota

SUMINISTROS DE REPUESTOS, ACCESORIOS, DISPOSITIVOS Y SERVICIOS ESPECIALIZADOS
Suministros de repuestos de hardware y/o software para la plataforma tecnológica Servicios especializados de apoyo a la plataforma tecnológica

1.4 Suministros de repuestos, Accesorios y dispositivos de hardware y/o software para la plataforma tecnológica

Esta adquisición se ejecutará cuando se requiera repuestos, accesorios y dispositivos para las plataformas tecnológicas alojadas en el datacenter del CAD, cuya falencia impacte la disponibilidad de las plataformas tecnológicas.

La adquisición de software se realizará únicamente para adquirir software de apoyo a las plataformas tecnológicas alojada en el datacenter del CAD.

1.5 Servicios especializados de apoyo a la plataforma tecnológica

Se adquirirán servicios especializados en el caso que se requiera un servicio que no haya sido contratado dentro de estas especificaciones técnicas, pero se requiera para el cumplimiento del objeto del contrato.

1.6 Servicio de mesa de ayuda nivel 1

Gestión de incidentes y requerimientos

El objetivo de este proceso es brindar solución a los incidentes y requerimientos en el primer contacto con el usuario y gestionar la solución de estos, directamente o mediante la coordinación de varios grupos de trabajo. Esta gestión debe enmarcarse bajo las mejores prácticas de ITIL en su última versión.

Este proceso debe involucrar las actividades de seguimiento a todos los incidentes y requerimientos escalados hacia proveedores y/o fabricantes, con quienes se tiene los Acuerdos de Niveles de Servicio (ANS) definidos por el Alcaldía de Medellín.

Los principales objetivos que se deben cumplir para este proceso son:

- Detectar cualquier incidente o requerimiento en los servicios TI, bien sea por medio de la notificación que hacen los usuarios empleando los canales dispuestos para tal fin, como también de una detección temprana por medio de los instrumentos y consolas de monitoreo que debe entregar la Mesa de Servicios o presentado como propuesta por el parte del contratista.
- Registrar y clasificar los incidentes o requerimientos a través de una completa guía de categorización y de prioridades en la herramienta de gestión que posee la entidad.
- Proveer los recursos y servicios pertinentes a todos los niveles para restaurar el servicio según se define en el ANS correspondiente.

Para la gestión de incidentes y requerimientos, se tiene una clasificación por categorías al interior de los diferentes servicios soportados, con el objetivo facilitar la solución de los casos de manera homogénea, rápida y eficaz.

Otros objetivos de la categorización de incidentes y requerimientos es servir como lista de verificación, minimizar el tiempo de solución de los incidentes y requerimientos, cumplimiento de las metas de los ANS y mitigar el impacto sobre el usuario final o sobre los otros procesos generados por una inadecuada documentación, trámite, tipificación, escalamiento y posibles demoras en la búsqueda de instructivos, formatos y documentos de apoyo relacionados al incidente o requerimiento específico.

1.6.1 Gestión de versiones o gestión de entregas y despliegues

La Gestión de Versiones es la encargada de la implementación y control de calidad de todo el software y hardware instalado en el entorno de producción. Este proceso debe colaborar estrechamente con la Gestión de Cambios y de Configuraciones para asegurar que toda la información relativa a las nuevas versiones se integra adecuadamente en la Base de Datos de Gestión de Configuración (CMDB) de forma que ésta se halle correctamente actualizada y ofrezca una imagen real de la configuración de la infraestructura TI.

Las principales actividades de la Gestión de Entregas y Despliegues se resumen en:

- Implementar las nuevas versiones en el entorno de producción de hardware, software y aplicaciones.
- Llevar a cabo los planes de back-out o retirada de la nueva versión si esto fuera necesario.
- Actualizar la Biblioteca de Medios Definitivos y la CMDB.

1.6.2 Gestión de cambios

El objetivo primordial de la Gestión de Cambios es que se realicen e implementen adecuadamente todos los cambios necesarios y aprobados para la infraestructura y servicios de TI garantizando el seguimiento de procedimientos estándar. Este proceso es responsable por controlar los cambios que involucran los elementos de configuración (EC) de la Infraestructura Tecnológica y la documentación o procedimientos asociados con la operación, soporte y mantenimiento de los sistemas en producción.

De acuerdo con el diagnóstico que se realice desde el primer nivel de soporte remoto o en sitio se puede concluir que se trata de una solicitud de un cambio, modificación o instalación de uno o más elementos de la configuración (INSTALAR, MOVER, ACTUALIZAR Y/O CAMBIAR (IMAC)), por lo tanto, se debe escalar directamente al grupo responsable por el proceso de Cambios estándar.

La tipificación y documentación inicial de las solicitudes de cambios estándar desde los primeros niveles de atención telefónico permiten al responsable de ejecutar el cambio, iniciar la consecución de recursos, instructivos, soporte logístico y conociendo entre otros para el logro oportuno de las metas del Acuerdo de Niveles de Servicio, la satisfacción del usuario y eliminar el riego residual de la ejecución de un cambio.

El alcance de la Gestión de Cambios debe ir en paralelo con el de la Gestión de la Configuración: Todos los cambios de CI inventariados en la CMDB deben ser correctamente supervisados y registrados. Las principales actividades que se deben realizar en este proceso se resumen en:

- Realizar un escalamiento previo a un segundo nivel de soporte telefónico o en sitio, quienes realizarán un diagnóstico y pruebas que ayuden a soportar la decisión de realizar un cambio y por lo tanto realizar un segundo escalamiento, pero esta vez al grupo responsable del proceso de Cambios Estándar.

- Registrar, evaluar y aceptar o rechazar las Peticiones de Cambio recibidas. Esta actividad es responsabilidad de la Alcaldía de Medellín.

- Asistir y participar al Comité de Cambios con el personal relativo al cambio a realizar.
- Ejecución y/o acompañamiento del cambio.

1.6.3 Gestión de problemas

El objetivo de este proceso es determinar las causas y encontrar las posibles soluciones a los incidentes que se vuelven recurrentes o tienen un fuerte impacto en la infraestructura tecnológica.

La Gestión de Problemas tiene un estrecho vínculo con la Gestión de Incidentes, esto debido a que este proceso provee en línea y de manera confiable e íntegra una base de datos de Errores Conocidos, en la cual el personal de soporte de cualquier nivel puede extraer soluciones temporales y definitivas a los incidentes presentados.

Las principales actividades que se deben realizar en este proceso son:

- Diagnóstico de problemas de hardware sobre la infraestructura soportada.
- Control de Problemas: Identificar y clasificar los problemas para determinar sus causas y convertirlos en errores conocidos para proponer las soluciones correspondientes.

1.7 Servicio apoyo de monitoreo del datacenter del CAD y las plataformas tecnológicas

El objetivo de este proceso es monitorear y controlar las diferentes plataformas y subsistemas, haciendo uso de las diferentes herramientas dispuestas para tal fin, generar información que permita conocer el estado de los componentes, dispositivos y servicios, para detectar indisponibilidades, y poder tomar acciones preventivas y correctivas. Se deben generar también informes gerenciales sobre las plataformas monitoreadas.

La alcaldía de Medellín proporcionará algunas herramientas para tener un monitoreo automático de hardware y software con sistema de alertas a los responsables, a nivel de infraestructura y aplicación.
El contratista incluirá herramientas de Monitoreo durante la vigencia del contrato, que permitan complementar el servicio y cumplir con el monitoreo en todos los niveles desde la aplicación y el servicio hasta la infraestructura. Estas herramientas de Monitoreo del servicio complementan las herramientas propias de monitoreo que entrega el Distrito.

Este servicio debe ser permanente, es decir un servicio en sitio 7x24 ubicado en el datacenter del CAD.

Deberá realizar las siguientes actividades:

- Monitoreo, Revisión y Detección de:
- Eventos de los subsistemas (Aire acondicionado, energía regulada, Detección y extinción de incendios, CCTV)
- Enlaces de comunicaciones.
- Plataforma de servidores o Dispositivos activos.
- Servicios de aplicaciones y bases de datos.
- Plataforma de almacenamiento.
- Activación de plan de escalamiento.
- Detectar y escalar las alertas que se generen dentro de los tiempos establecidos de acuerdo con los ANS definidos por el Alcaldía de Medellín y los procedimientos.

Formación profesional:

- Formación Técnica, Tecnológica o mínimo 6 semestres de formación profesional certificada en áreas relacionadas con la tecnología de información.
- Formación y/o conocimientos en ITIL V3 Foundation.
- Certificación y/o experiencia en Sistemas operativos Windows.
- Conocimientos en Office 2013 o superior.
- Formación en atención y/o servicio al cliente

Experiencia laboral:

Experiencia en soporte de tecnología mínima de 12 meses.

1.8 Servicio de mantenimiento, soporte, estandarización y reemplazo de partes de equipos de cómputo

Objetivo: Prestar los servicios de soporte y mantenimiento preventivo y correctivo a los diferentes elementos de la infraestructura de hardware, que no cuentan con la garantía respectiva por parte del proveedor y efectuar las actividades de reparación de equipos y elementos.

Se debe disponer del recurso humano, físico y procedimental para cumplir las funciones propias del servicio bajos las condiciones y ANS definidos por Alcaldía de Medellín. La prestación del servicio en el laboratorio se debe garantizar con un tiempo de solución ajustando a los ANS establecidos, de manera que se afecte en lo mínimo el desempeño de los usuarios que requieren el servicio.

Los principales objetivos que se deben cumplir para este proceso son:

- Tramitar las garantías para reemplazo de componentes o equipos sobre la infraestructura soportada. El Alcaldía de Medellín deberá proveer los contratos de garantía y datos de contacto requeridos para llevar a cabo este procedimiento. Para el trámite de garantías se debe registrar el requerimiento en la herramienta de gestión de incidentes y colocarlo en estado de garantía. Se debe mantener un registro de las garantías y reportarlo en los informes periódicos.
- Realizar el seguimiento a los trámites de garantías y notificar a los supervisores de manera oportuna tan pronto se detecte incumplimiento por parte de proveedores o terceros.
- Instalación del software soportado.
- Instalación de actualizaciones de Sistema Operativo sobre la infraestructura soportada, esto puede incluir diferentes sistemas.
- Mantenimiento correctivo de los equipos que ingresen a laboratorio para atención de incidentes. Esto es, limpieza física, ajuste de partes, limpieza de temporales, actualización de antivirus e instalación de actualizaciones.
- El contratista hará la gestión de soporte de reposición de elementos de la operación. Este servicio consiste en atender los casos escalados donde se requiere el suministro de elementos para solucionar los incidentes o mejorar la prestación del servicio mediante la adquisición de elementos de hardware y/o software.
- Atender las solicitudes que requieran suministro de repuestos para equipos de cómputo.

- Coordinar la salida de los repuestos desde la bodega de almacenamiento hasta la ubicación requerida por parte de analista de soporte en sitio para la reparación.
- Controlar el inventario de elementos.
- Presentar al Distrito la relación de gastos de elementos.
- Presentar los informes del proceso.

Formación profesional:

- Formación Técnica, Tecnológica o mínimo 6 semestres de formación profesional certificada en áreas relacionadas con la tecnología de información.
- Formación y/o conocimientos en ITIL V3 Foundation.
- Certificación y/o experiencia en Sistemas operativos Windows.
- Conocimientos en Office 2013 o superior.
- Formación en atención y/o servicio al cliente

Experiencia laboral:
Experiencia en soporte de tecnología mínima de 12 meses.

1.9 servicio de soporte a soluciones de microservicios (servicio de implementación de soluciones devops)

Es el encargado de trabajar con todo el equipo de TI para crear un ecosistema de despliegue de software que incremente la productividad de los equipos y la confiabilidad de las aplicaciones.

A continuación, se describen las actividades a desarrollar:

- Diseñar e implementar estrategias de automatización que agilicen el proceso de desarrollo y despliegue de aplicaciones
- Trabajar con los diferentes roles técnicos para asegurar que el desarrollo sigue los lineamientos establecidos de acuerdo con la cultura y procesos DevSecOps de la Alcaldía de Medellín
- Participar en seguimientos técnicos con los equipos de trabajo de la Alcaldía de Medellín siempre que sea requerido
- Construir extensiones, plugins y/o aceleradores para ser integrados al proceso de DevSecOps definido como puntos de apoyo y sus posteriores pruebas unitarias y/o integración.

- Entender los requerimientos técnicos de cada proyecto y/o aplicación que vaya a ser integrada al ecosistema DevSecOps con el único propósito de identi car la adherencia de estas al proceso.
- Construir y automatizar la toma de KPIs relevantes al proceso de adopción DevSecOps en la Alcaldía de Medellín.
- Automatizar la mayor cantidad de tareas siempre que sea posible dentro del proceso DevSecOps
- Seleccionar, configurar y desplegar las herramientas de CI/CD apropiadas
- Aprender nuevas tecnologías, servicios y adaptarse a las nuevas versiones de los lenguajes que domina
- Diseñar y desarrollar APIs en caso de que se requiera su adherencia al proceso DevSecOps
- Construir la documentación, lineamientos y gobierno necesarios para dar autonomía a los equipos e ir escalando el proceso de entrega continua
- Construir pipelines de integración, despliegue y entrega continua
- Construir scripts de Configuration Management.
- Implementar el estándar de aseguramiento en la calidad para la integración continua DevOps
- Gestionar y asegurar el correcto funcionamiento de las herramientas y ciclos de calidad implementados.
- Gestionar y administrar el correcto despliegue en ambientes de gestión de contenedores.
- Gestionar y administrar el correcto funcionamiento de la estructura de la gestión y orquestación de contenedores, implementada para las soluciones de software definidas por la Alcaldía de Medellín.
- Implementar soluciones DevOps para apoyar las actividades de diseño del modelo de aseguramiento de la calidad en ambientes de desarrollo, pruebas y producción en el marco del estándar DevOps.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación profesional:

Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática o afines.

Experiencia laboral:
Experiencia profesional mínima de 2 años en Implementación de Soluciones DEVOPS.

1.10 Servicio de soporte a soluciones de microservicios - automatización de despliegues (SRE)

Su función es trabajar por mantener la disponibilidad y confiabilidad de plataformas críticas y aplicaciones, construyendo y automatizando la operación de software como servicio e integrándola a un ecosistema DevSecOps.

A continuación, se describen las actividades a desarrollar Especialista SRE:

- Diseñar, implementar y mantener scripts o soluciones que permitan administrar y aprovisionar la infraestructura de las aplicaciones de una manera rápida, estándar y confiable
- Participar en seguimientos técnicos con el cliente siempre que sea requerido
- Ejecutar acciones de mejora continua sobre scripts de automatización sobre procesos operacionales (como despliegues y actualizaciones)
- Seleccionar, configurar y desplegar las herramientas de infraestructura como código apropiadas
- Aprender nuevas tecnologías, servicios y adaptarse a las nuevas versiones de los lenguajes que domina
- Construir la documentación, lineamientos y gobierno necesarios para dar autonomía a los equipos e ir escalando el proceso de operación automatizada
- Construir KPIs relevantes a la automatización de la operación
- Definir la estrategia de migración y automatizar los despliegues de aplicaciones sobre OpenShift
- Definir los estándares y especificaciones de creación, mantenimiento y configuración de los servidores o contenedores basado en infraestructura como código.

- Realizar análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones.
- Generar un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación profesional:

- Formación profesional de Ingeniería de Sistemas, Ingeniería de Computación, Ingeniería de Software, Ingeniería TI o carreras relacionadas.
- Deseables certificaciones relacionadas a tecnologías de información de preferencia.
- Conocimiento básico en diseño de arquitectura cloud y arquitectura de networking.
- Conocimiento de plataformas de contenedores (e-g., Openshift Container Plataform/ARO/ASK/EKS) y de sistemas operativos (Windows, Linux, AIX, entre otros)
- Conocimientos en plataformas en la nube (AWS, Azure).
- Capacidad para entender código desde la perspectiva de desarrollo y de operaciones.

Experiencia laboral:

Experiencia mínima de dos a cuatro (2 a 4) años en rol de especialista SRE o afines.

1.11 Servicio de soporte a contenedores de aplicaciones de microservicios

Actividades permanentes para la administración de Openshift

- Evaluar los posibles impactos a las aplicaciones ya desplegadas al actualizar la plataforma OpenShift.
- Solucionar problemas de nivel dos relacionados con la implementación publicación y despliegue de aplicaciones.
- Verificación del estado del clúster OpenShift para identificar y anticipar problemas en el funcionamiento.

- Gestionar casos de soporte nivel tres directamente con el fabricante de la plataforma (Red Hat).
- Asegurar los recursos tecnológicos adecuados para la sostenibilidad y el funcionamiento de las aplicaciones orquestadas por OpenShift.
- Realizar mediciones constantes sobre la gestión de los recursos de la plataforma OpenShift y plantear estrategias de su optimización.
- Gestionar y administrar los certificados de seguridad basados en TLS de la plataforma OpenShift.
- Dar soporte sobre la publicación y los despliegues de las aplicaciones implementadas en la plataforma OpenShift, identificando posibles oportunidades de mejora, fallas o estados críticos de funcionamiento.
- Implementar las recomendaciones de seguridad, parchado de la plataforma OpenShift y demás temas que el fabricante de la plataforma informe.
- Realizar monitoreo del estado de la plataforma, verificando el consumo de los recursos disponibles, capacidad de operación del Clúster.
- Realizar las actualizaciones menores y mayores (update y upgrades) de la plataforma OpenShift
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones.
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación profesional:

- Formación profesional en Ingeniería de Sistemas, informática, electrónica o telecomunicaciones, con mínimo 24 meses de experiencia profesional.
- Conocimientos básicos en sistemas operativos Windows y en Linux.
- Acreditar conocimientos específicos de al menos 20 horas en: Python, Yaml, Json, Java Script, entre otros.

Experiencia laboral:

Acreditar mínimo 12 meses de experiencia en administración de contenedores de aplicaciones o certificación en Docker, kubernetes y/o Openshift.

Actividades permanentes para la administración de contenedores de aplicaciones:

- Evaluar los posibles impactos a las aplicaciones ya desplegadas al actualizar la plataforma Podman.
- Solucionar problemas de nivel dos relacionados con la implementación publicación y despliegue de aplicaciones.
- Verificación del estado del servicio de Podman para identificar y anticipar problemas en el funcionamiento.
- Gestionar casos de soporte nivel tres directamente con el fabricante de la plataforma (Red Hat).
- Asegurar los recursos tecnológicos adecuados para la sostenibilidad y el funcionamiento de las aplicaciones orquestadas por Podman.
- Realizar mediciones constantes sobre la gestión de los recursos de la plataforma Podman y plantear estrategias de su optimización.
- Gestionar y administrar los certificados de seguridad basados en TLS de la plataforma Podman.
- Dar soporte sobre la publicación y los despliegues de las aplicaciones implementadas en la plataforma Podman, identificando posibles oportunidades de mejora, fallas o estados críticos de funcionamiento.
- Implementar las recomendaciones de seguridad, parchado de la plataforma Podman y demás temas que el fabricante de la plataforma informe.
- Realizar monitoreo del estado de la plataforma, verificando el consumo de los recursos disponibles, capacidad de operación del servicio.
- Realizar las actualizaciones menores y mayores (update y upgrades) de la plataforma Podman
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación profesional:

- Formación profesional en Ingeniería de Sistemas, informática, electrónica o telecomunicaciones, con mínimo 24 meses de experiencia profesional.
- Conocimientos básicos en sistemas operativos Windows y en Linux.
- Acreditar conocimientos específicos de al menos 20 horas en: Python, Yaml, Json, Java Script, entre otros.

Experiencia laboral:
Acreditar mínimo 12 meses de experiencia en administración de contenedores de aplicaciones o certificación en Docker y/o Podman.

1.12 Servicio de soporte a contenedores de aplicaciones monolíticas

Actividades permanentes para la administración de aplicaciones monolíticas

- Operar y gestionar los recursos asignados para la gestión de las aplicaciones y la publicación y despliegue de las mismas. Dentro de los recursos asignados se tienen los servidores dedicados de aplicaciones, servidores y contenedores de aplicaciones (IIS, JBoss, Tomcat, Apache, NGINX, WordPress y las nuevas tecnologías que se adquieran acorde a esta actividad).
- Apoyar la implementación de los proyectos de la Alcaldía de Medellín con la participación directa en lo que tiene que ver con la instalación, revisión, actualización y migración de las aplicaciones o instalación, publicación y soporte de los servicios web, conforme a los instructivos entregados por los proveedores o a la información técnica que aporte la Alcaldía de Medellín.
- Gestionar y dar respuesta a los requerimientos asignados a través de la herramienta de gestión.
- Reportar al Equipo de Sistemas de Información todos los cambios realizados a las diferentes aplicaciones para la respectiva actualización del Inventario.
- Monitorear y gestionar lo pertinente para que los servicios de las diferentes aplicaciones se encuentren siempre disponibles.
- Contribuir con sugerencias que ayuden en la definición de estándares para la adquisición de nuevas aplicaciones, que permitan expandir el portafolio de servicios y la prestación de

estos, así como para efectos de mejorar la plataforma donde se encuentren instaladas las aplicaciones.

- Reportar las situaciones críticas y de riesgo que puedan impactar la disponibilidad de los servicios que se prestan a través de las aplicaciones, de tal manera que se disminuyan los impactos negativos sobre la operación.
- Documentar los procedimientos realizados y reportar al administrador de la herramienta de gestión para su ingreso en la base de datos del conocimiento.
- Coordinar con los responsables del Distrito todos los cambios que se vayan a realizar en la prestación del servicio de las aplicaciones, para disminuir los impactos negativos sobre la operación.
- En caso de que se requiera para el manejo del entorno de ciertas aplicaciones es necesario tener conocimientos en programación con ciertas herramientas de desarrollo principalmente JAVA, HTML, .NET y SQL para los entornos de Bases de Datos.
- Realizar la publicación de nuevos servicios Web y soporte de los existentes que le sean asignados.
- Analizar el desempeño de los servicios de apoyo en la creación de procedimientos y métodos a nivel web.
- Realizar las actualizaciones menores y mayores (update y upgrades) de las plataformas IIS, JBoss, Tomcat, Apache, NGINX, WordPress
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación profesional:

- Formación profesional en Ingeniería de Sistemas, informática, electrónica o telecomunicaciones, con mínimo 24 meses de experiencia profesional.
- Acreditar experiencia mínima de 12 meses en sistemas operativos Windows, y conocimientos básicos en Linux.
- Acreditar conocimientos específicos de al menos 20 horas en:
- Conocimientos básicos en JAVA o Conocimientos básicos en HTML
- Conocimientos básicos en punto NET.
- Conocimientos básicos en bases de datos

Experiencia laboral:
Acreditar mínimo 12 meses de experiencia en administración de contenedores de aplicaciones (IIS, JBoss, Tomcat, Apache, NGINX, WordPress, Glassfish) y/o certificación en Jboss EAP (Red Hat Certified Specialist in Enterprise Application Server Administration).

1.13 Servicio de administración y soporte especializado de la plataforma de almacenamiento

El objetivo es apoyar los proyectos estratégicos de la entidad, realizando las actividades de tipo preventivo, correctivo y prospectivo que garanticen el correcto funcionamiento de la plataforma de almacenamiento en todos sus componentes y en caso de incidentes críticos, realizar el escalamiento respectivo para su atención por los medios adecuados, apoyándose en los contratos de soporte y mantenimiento vigentes que tenga el Alcaldía de Medellín.

Son actividades básicas permanentes para la plataforma de almacenamiento, tanto en el Datacenter principal como en el Datacenter alterno, las siguientes:

- Operar, gestionar, evaluar, analizar, diseñar y mantener operativa la plataforma de almacenamiento con la que cuenta el Distrito Medellín.
- Mantener actualizado los diseños de la arquitectura de la Plataforma de Almacenamiento
- Sugerir y diseñar planes de contingencias y mejoramiento frente a las posibles eventualidades que se puedan presentar en el almacenamiento.
- Operar y gestionar la plataforma gestión de contenido (HCP), apoyando los proyectos de la entidad que requieran de este servicio.
- Operar y gestionar la plataforma nube hibrida (HCP-ANYWHERE), apoyando los proyectos de la entidad que requieran de este servicio.
- Coordinar con los responsables del Distrito todos los cambios que se vayan a realizar en la plataforma de almacenamiento, para disminuir los impactos negativos sobre la operación
- Revisar que las máquinas (Storages, Switch FC, librerías) se encuentren con las últimas actualizaciones del firmware.
- Revisar que a nivel de almacenamiento SAN las máquinas se encuentren operativas y bien administradas; tales como: Hosts, Storages, Switch FC, librerías, Vmware, Vmware en Hiperconvergencia, Appliance de Backup, etc.

- Propender porque se mantenga operativa la alta disponibilidad de las plataformas de Almacenamiento (SAN, NAS).
- Coordinar con el equipo Datacenter, la conectividad física de los switches SAN con los servidores con tarjetas HBA y que requieran almacenamiento virtual.
- Creación de alias para cada WWN (World Wide Name) que se conecta a los puertos con el nombre asignado por el administrador de la máquina, utilizando nombres nemotécnicos.
- Creación de zonas para los distintos proyectos, asignando los alias correspondientes, siguiendo los lineamientos definidos por el Municipio.
- Realizar en forma periódica depuraciones físicas y lógicas en la plataforma, con el fin de liberar puertos en los switch y espacio en los storages.
- Realizar las conexiones y migraciones que sean solicitadas por cambios o actualizaciones en la infraestructura de switch, storages o servidores.
- Crear redundancia en los switch Fabric con protocolo ISL (Inter Switch Link Truncking), que permita un balanceo de cargas apropiado y una redundancia óptima.
- Realizar revisiones de desempeño en los puertos, analizando la carga que tiene los switches con respecto a las máquinas y al canal, teniendo en cuenta las diferentes variables como las configuraciones, la velocidad de los puertos, la hora y fecha en que se realiza según los picos para la carga.
- Coordinar con los responsables del equipo Datacenter del Distrito todos los cambios que se vayan a realizar en los switches SAN, para disminuir los impactos negativos sobre la operación.
- Apoyar en tareas operativas a los integrantes al equipo Datacenter cuando sea necesario
- Contribuir con la optimización y mejoramiento de los procesos a través del buen desempeño de las actividades de su competencia.
- Configuración de volúmenes (Raid Groups) – SAN
- Creación de host groups, con la identificación de cada máquina que se agregue a la SAN
- Configuración y verificación de failover y redundancia de las máquinas solicitadas con dicha configuración.
- Mantener actualizado el modelo gráfico de la plataforma de almacenamiento.
- Apoyo en la instalación de nuevas máquinas que requieran almacenamiento externo.
- Realizar el monitoreo y escalamiento al proveedor en caso de una falla física o problema que requiera de dicha atención
- Realizar las demás actividades que le sean asignadas y que estén directamente relacionadas con el perfil y las funciones del cargo.

- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones.
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática o afines.
- Conocimiento en Operating and Managing Hitachi Content Platform. HCP y Anywhere
- Acreditar conocimientos en ITIL.

Experiencia laboral:

- Experiencia: mínima de 4 años en administración de plataformas de almacenamiento HITACHI.
- Acreditar experiencia mínima de 36 meses en redes SAN y NAS.

1.14 Servicio de gestión de solicitudes de las plataformas de almacenamiento y de los switch’s san

Las principales actividades que se deben cumplir para este proceso son:

- Realizar conectividad física de servidores de rack o blades a los switches con HBA que requieran almacenamiento virtual, este cableado lo realiza en compañía del administrador de la máquina.
- Creación de alias para cada WWN (World Wide Name) que se conecta a los puertos con el nombre asignado por el administrador de la máquina, utilizando nombres nemotécnicos.
- Creación de zonas para los distintos proyectos, en donde se le asigna los alias correspondientes siguiendo los lineamientos definidos por el Distrito.

- Depuración física y lógica para liberar puertos y espacio en las máquinas salientes, con el fin de hacer un uso óptimo de los recursos.
- Realizar las conexiones y migraciones que sean solicitadas por cambios en la infraestructura de switch nuevos o de servidores.
- Creación de Redundancia en los switches Fabric con protocolo ISL (Inter Switch link Truncking), que permita un balanceo de cargas apropiado y una redundancia óptima.
- Monitoreo y escalamiento al proveedor en caso de una falla física y/o lógica, procurando siempre tener una contingencia mientras se realiza el cambio de la parte dañada.
    - Mantener actualizado gráficamente, el esquema de conexiones (servidores, Blades, librería, Storage).
- Realizar revisiones de desempeño en los puertos, analizando la carga que tiene los switches con respecto a las máquinas y al canal, teniendo en cuenta las diferentes variables como las configuraciones, la velocidad de los puertos, la hora y fecha en que se realiza según los picos para la carga.
- Coordinar con los responsables del Distrito todos los cambios que se vayan a realizar en los switches SAN, para disminuir los impactos negativos sobre la operación.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones.
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática o afines.
- Conocimientos básicos en almacenamiento de datos.
- Acreditar conocimientos en ITIL.

Experiencia laboral:

Mínima de 1 año en plataformas de almacenamiento.

1.15 Servicio de administración de las plataformas de backup

El objetivo de este proceso es operar y gestionar, mantener disponible y gestionar de forma eficiente la plataforma de backup de la Alcaldía de Medellín.

Actividades permanentes backup de la información:

- Realizar la copia de seguridad de la información corporativa en las diferentes herramientas y sistemas de almacenamiento provistos por el Alcaldía de Medellín
- Operar y gestionar la plataforma de backup.
- Operar y gestionar las políticas de backup, utilizando las herramientas de administración suministradas por el Distrito, que para este caso es: "Veritas Netbackup", implica la creación, modificación y eliminación de políticas de acuerdo con los requerimientos de la Alcaldía de Medellín.
- Velar por mantener la plataforma de backup en las últimas versiones liberadas.
- Monitorear la ejecución de las copias de seguridad y tomar acciones cuando no se ejecutan correctamente.
- Realizar las actividades pertinentes para la recuperación de información cuando sea solicitada por los usuarios.
- Coordinar con el responsable en sitio para mantener la librería de backup con el número de cintas adecuadas. Esta actividad contempla etiquetar cintas nuevas, cargarlas y retirar de la librería de acuerdo con la demanda.
- Operar y gestionar los medios (cintas), manteniendo inventario con el respectivo estado de cada una.
- Revisión semestral de las políticas de backup, realizando la revisión de su configuración, frecuencias, cuales se están usando, cuales no se están usando y cumplimiento de los estándares de nombramiento definidos por el Alcaldía de Medellín.
- Reportar cada inconveniente técnico que se presente en la plataforma de respaldo, como son: la librería, la solución de respaldo a disco (Appliance).
- Generar reportes periódicos a los líderes, para el análisis pertinente y toma de decisiones.
- Investigar y proponer mejoras para las estrategias de backup.
- Realizar periódicamente las pruebas de restauración de backups, según las políticas del Distrito.
- Realizar las respectivas remediaciones a Backup, de acuerdo con las recomendaciones de seguridad informática que se indiquen, en los tiempos establecidos dentro de los ANS contemplados para estas actividades.

- Coordinar con los responsables del Distrito todos los cambios significativos que se vayan a realizar en la plataforma de backup, para disminuir los impactos negativos sobre la operación.
- Cumplir con los procedimientos, instructivos y formatos publicados en la herramienta de gestión de la calidad de la Alcaldía de Medellín.
- Participar en la elaboración y modificación de la documentación de los procedimientos, instructivos y formatos que serán publicados en la herramienta de gestión de la calidad de la Alcaldía de Medellín.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones basadas en estadísticas de consumo, ratas de crecimiento, tendencias de consumo y análisis de obsolescencia.
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento

Formación profesional:

- Formación profesional en Ingeniería de Sistemas, Electrónica Telecomunicaciones o carreras afines con 48 meses de experiencia.
- Acreditar certificación en plataformas de backup.

Experiencia laboral:

- Acreditar 36 meses de experiencia en la administración y manejo de plataformas de backup.
- Acreditar experiencia mínima de 12 meses en utilización de herramientas Veritas Netbackup.

1.16 Administración y soporte especializado de la plataforma de servidores

Actividades permanentes para la administración y soporte especializado de servidores:

- Operar y gestionar la plataforma de virtualización en sus ambientes de producción y de pruebas, lo cual incluye la instalación, administración y el soporte de la plataforma virtual con VMware, software suministrado por el Alcaldía de Medellín.
- Operar y gestionar la plataforma de hiperconvergencia donde reside el ambiente de virtualización con VMware
- Proporcionar desde VMware, los recursos requeridos para el buen funcionamiento del ambiente de microservicios
- Implementar las políticas de seguridad en los servidores físicos y virtuales de acuerdo con los estándares definidos por el Alcaldía de Medellín y por el fabricante según el Sistema Operativo y servicios instalados en el servidor.
- Entregar recomendaciones de mejoramiento y apoyo en la implementación de nuevos servidores, teniendo en cuenta el diseño de la contingencia y alta disponibilidad de los servidores críticos o de alto impacto definidos por el Alcaldía de Medellín.
- Gestionar y administrar el mantenimiento correctivo y preventivo del hardware de servidores, previa información entregada por el Alcaldía de Medellín, teniendo en cuenta las garantías y contratos de mantenimiento vigentes.
- Garantizar el funcionamiento de los snapshots de los servicios que se encuentran clusterizados en ambientes Vimware.
- Realizar las respectivas correcciones a las vulnerabilidades que se encuentren en la plataforma de servidores, de acuerdo con las recomendaciones de seguridad informática que se indiquen, en los tiempos establecidos dentro de los ANS contemplados para estas actividades.
- Gestionar lo pertinente para que los servidores estén siempre cubiertos dentro de las políticas de backup.
- Operar y gestionar los diferentes Dominios que posea el Alcaldía de Medellín contemplados en la propuesta.
- Administrar, gestionar y operar las herramientas de software y dispositivos hardware, tal como los servicios objeto de la propuesta (directorio activo, WSUS, Exchange Server, office365, OWA IIS (internet information server, solo la instalación y puesta en funcionamiento del servicio, no incluye publicación de sitios Web) y las nuevas tecnologías que se adquieran acorde a esta actividad.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones.
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.

- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación académica:

- Formación: Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática o afines.
- Certificaciones o constancias de capacitación o entrenamiento en administración de VMware, que demuestren o prueben que es profesional calificado para la administración de esta plataforma.
- Constancia de capacitación o entrenamiento en administración de plataforma de Hiperconvergencia.
- Acreditar conocimientos en ITIL.

Experiencia laboral:

- Experiencia mínima de 4 años en administración de plataformas de virtualización con VMware.

1.17 Servicio de administración y soporte básico de servidores

Actividades permanentes para la administración y soporte básico de servidores:

- Instalar nuevos servidores, operar y gestionar recursos compartidos, monitorear servidores.
- Escalamiento a proveedores cuando el requerimiento lo amerite
- Operar y gestionar los logs de auditoría del sistema operativo y de servicios contemplados en la propuesta.
- Operar y gestionar los servicios DHCP, DNS, WINS, IIS, así como las relaciones de confianza.
- Aplicar políticas centralizadas de seguridad sobre el directorio activo, suministradas por el Alcaldía de Medellín.
- Operar, gestionar y dar soporte a los servidores corporativos y del dominio.
- Operar, gestionar y configurar los servidores de correo electrónico y de comunicaciones unificadas y telefonía.

- Mantener la operatividad y disponibilidad de la plataforma de servidores.
- Realizar la administración, actualización, aplicación de parches de seguridad, detección temprana de eventos y demás situaciones que permitan asegurar la disponibilidad de la plataforma de servidores, correo electrónico, y disponibilidad y el dominio entre otras.
- Garantizar el cumplimiento de los ANS definidos por el Alcaldía de Medellín y de las responsabilidades según el rol de los procesos que sean asignados.
- Manejar garantías, incluye trámite de reparaciones de hardware con otros proveedores de acuerdo con los niveles de servicio (ANS) establecidos con terceros.
- Administración y soporte de la plataforma de los servidores Windows, Linux y AIX.
- Planear, administrar, gestionar, operar y acompañar las instalaciones de los servidores que tenga en su inventario el Alcaldía de Medellín.
- Operar y gestionar el inventario de equipos de servidores
- Coordinar con los responsables del Distrito todos los cambios que se vayan a realizar en los servidores y servicios, para disminuir los impactos negativos sobre la operación.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones.
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación profesional:

- Formación Profesional: Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática o afines.
- Certificaciones o constancias de capacitación o entrenamiento en administración de servidores con sistemas operativos Windows y Linux.
- Acreditar conocimientos en ITIL.

Experiencia laboral:

- Experiencia mínima de 1 año en administración de servidores Windows y servidores Linux.

1.18 Servicio de administración y soporte especializado de directorio activo y dns

Responsable de la administración y gestión de la infraestructura y servicios de Directorio Activo y DNS, garantizando la correcta operación y disponibilidad de los servicios.

Actividades permanentes para la administración y soporte especializado del directorio activo:

- Mantener los criterios tecnológicos y procedimentales para todas las implementaciones relacionadas con el directorio activo y correo electrónico, estructurando documentación de la infraestructura a cargo, basados en la mejores prácticas y lineamientos o requerimientos de la Alcaldía.
- Soportar tecnológicamente la infraestructura y servicios de Directorio Activo y DNS, dando gestión y solución a incidentes, requerimientos y problemas de alta complejidad, dentro de los acuerdos de niveles de servicio pactados.
- Establecer planes de trabajo, que garanticen el mejoramiento continuo de los servicios de directorio activo y correo electrónico
- Velar, gestionar y asegurar que los tiempos de respuesta cumplan con los acuerdos de niveles de servicio contratados para todo lo relacionado con el soporte del área de servidores
- Gestionar los escalamientos con terceros y proveedores cuando se requiera y velar el cumplimiento de los tiempos de atención definidos.
- Velar por la aplicación de las directivas, los procesos y los controles adecuados para proteger las partes clave de la infraestructura de TI asociada al directorio activo y la plataforma de correo, frente a riesgos, asegurando los puntos de entrada, monitoreo del proceso de cuentas con privilegios permanentes, cuentas VIP, cuentas de Active Directory conectadas con privilegios, controladores de dominios y otros servicios de infraestructura que afectan a la administración de identidades, del acceso y de la configuración, como servidores de administración de sistemas o servidores de infraestructura de clave pública (PKI).
- Detectar signos de ataques malintencionados o riesgos de seguridad en el directorio activo
- Trabajar estrechamente con los equipos de la Unidad de Infraestructura de TI y de la Unidad de Seguridad Informática para identificar los componentes más críticos del directorio activo, controladores de dominio, plataforma de correo y proteger los que

tienen el máximo valor. Debe proponer los niveles de control y supervisión de la seguridad en función de la importancia crítica del recurso.

- Administrar eficazmente el directorio activo y plataforma de correo electrónico para asegurarse de que dispone de procesos eficaces de administración del ciclo de vida de los usuarios, datos, aplicaciones y sistemas administrados por la instalación de Active Directory, de tal forma que exista una cadena clara de responsabilidad para el aprovisionamiento, administración, supervisión, actualización y, en última instancia, retirada del sistema de usuarios, datos, aplicaciones y sistemas administrados.

Formación profesional:

- Formación profesional en Ingeniería de Sistemas, informática, electrónica o telecomunicaciones, con 24 meses de experiencia profesional.

Experiencia laboral:

- Experiencia laboral de 24 meses, de los cuales debe acreditar experiencia específica:
- Acreditar 24 meses de experiencia profesional en administración de plataformas Windows y Linux, servicios de DA, DHCP, DNS, File server, FTP, Terminal server Mínimo 24 meses de experiencia en Administración de Sistemas Operativos Microsoft Windows Server 2008 R2 , 2012 o superior.

1.19 Servicio de administración de la plataforma AIX

Objetivo: Operar y gestionar la plataforma de servidores Power Series de IBM Referenciadas en la línea base.

Esta administración comprende:

- Gestión sobre el mantenimiento preventivo y correctivo de daños en sitio relacionado con las máquinas administradas.
- Gestión y administración del Sistema Operativo.
- Documentar todos los procedimientos realizados generando una base de datos de conocimiento.

- La administración de la plataforma debe cubrir las actualizaciones de software y firmware que durante el tiempo contractual hayan sido liberadas por el fabricante.
- Durante el tiempo de la administración de la plataforma, el administrador de la plataforma AIX deberá cumplir con las siguientes actividades relacionadas con la gestión:
- Instalar, configurar y poner en funcionamiento la Infraestructura Informática directamente relacionada con los servidores Power Series de IBM en Sistema Operativo AIX. (Por demanda).
- Planear la disponibilidad y capacidad de los Power Series de IBM. (Permanente).
- Actualizar y aplicación de parches al sistema operativo de los servidores Power Series de IBM. (Permanente).
- Actualización y aplicación de microcódigo de los servidores Power Series de IBM y los recursos asociados, consola de monitoreo (HMC). (De acuerdo con los ANS y Garantía de los equipos).
- Instalar, configurar y mantener los sistemas de respaldos que posea el Alcaldía de Medellín, en los equipos Power Series de IBM. (Permanente).
- Gestionar los eventos y verificar las garantías con el proveedor IBM. (Permanente).
- Elaborar informes mensuales de comportamiento de la plataforma y notificar eventos relevantes que afecten el desempeño de los servicios asociados a ella, enviar al responsable de la plataforma de servidores del equipo Datacenter de la Alcaldía de Medellín.
- Crear cintas imagen de los sistemas operativos de todas las particiones configuradas en los servidores Power Series de IBM. (Diario).
- Notificar todos los eventos relacionados con la plataforma, al responsable por parte de TI (Líder de Datacenter o Líder de Infraestructura) de la Alcaldía de Medellín. (Por ocurrencia).
- Gestionar la garantía que cubre todas sus partes tanto de software como de hardware, ante IBM.
- Verificar la disponibilidad y correcto funcionamiento de los servidores Power Series de IBM y las particiones asociadas. (Diario).
- Verificar el correcto funcionamiento de la infraestructura de Alta disponibilidad de SAP R/3, Portales y Replicación remota (HACMP, TRUE COPY). (Diario).
- Verificar y administrar los espacios de almacenamiento asignados a los servidores Power Series de IBM. (Diario).
- Verificar el log del sistema operativo y el log de errores el cual registra e informa fallas en el funcionamiento de todos los dispositivos lógicos y físicos, y ejecutar diagnósticos de los servidores Power Series de IBM. (Diario)

- Asegurar la Disponibilidad para la administración y soporte de la Plataforma, durante las actividades adicionales programadas o no programadas por el Alcaldía de Medellín, por fuera de los horarios habituales.
- Verificar la correcta ejecución de los backups hechos por los sistemas de respaldos que posea el Alcaldía de Medellín, en los equipos Power Series de IBM. (Diario).
- Coordinar la restauración de la información solicitada por los administradores de las aplicaciones que se encuentran en los equipos Power Series de IBM. (Por petición)
- Redistribuir recursos entre las particiones de acuerdo con necesidades específicas de las bases de datos y aplicaciones. (Por petición)
- Prender, apagar y reiniciar tanto las particiones como los servidores Power Series de IBM. (por petición)
- Hacer aseguramiento básico de la Plataforma Power Series de IBM y ejecutar las recomendaciones de TI.
- Verificar la conectividad de la plataforma e informar cualquier evento que comprometa el acceso de los usuarios a la misma. (por ocurrencia)
- Mantener documentados y actualizados los procedimientos relacionados con la administración de la Plataforma Power Series de IBM, basados en normas de calidad.
- Realizar las respectivas remediaciones a las vulnerabilidades que se encuentren en la plataforma de servidores con sistema operativo AIX, de acuerdo con las recomendaciones de seguridad informática que se indiquen, en los tiempos establecidos dentro de los ANS contemplados para estas actividades.
- Coordinar con los responsables de la Alcaldía de Medellín todos los cambios que se vayan a realizar en la Administración de la plataforma AIX, para disminuir los impactos negativos sobre la operación.
- Implementaciones, administración y soporte de características avanzadas en la plataforma Power IBM tales como: Cluster de alta disponibilidad, características avanzadas e implementación de ambientes virtualizados en la plataforma haciendo uso de herramientas Power VM Enterprise entre otras.
- Solución de problemas de interacción entre Sistema Operativo y aplicaciones Oracle y SAP.
- Realizar actualizaciones de software (Firmware y Sistema Operativo) con el fin de garantizar el soporte.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.

- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento

Formación profesional:

- Formación profesional en Ingeniería de Sistemas, informática, electrónica o telecomunicaciones, con 24 meses de experiencia profesional.
- Certificación de IBM en administración de sistemas operativos AIX.

Experiencia laboral:

- Acreditar mínimo 24 meses de experiencia en administración de plataformas AIX.

1.20 Servicio de administración de bases de datos sql server y bases de datos no relacionales nosql: mongodb y cratedb

El objetivo es operar, gestionar, mantener disponible y gestionar de forma eficiente, las bases de datos SQL de la Alcaldía de Medellín.

- Incluye todas las tareas administrativas que debe realizar, utilizando el software de administración de base de datos, proporcionado por el Alcaldía de Medellín.
- La administración de estas bases de datos contempla a nivel general, la creación, modificación, actualización, respaldo, recuperación, análisis de rendimiento, optimización y apoyo en la implementación de bases de datos, bajo los principios de confiabilidad, seguridad, disponibilidad e Integridad.
- Crear las instancias de bases de datos que sean requeridas por el Alcaldía de Medellín
- Realizar la migración de las bases de datos a las nuevas versiones liberadas, de acuerdo a los planes aprobados por el Alcaldía de Medellín.
- Crear las tareas administrativas para nuevos requerimientos de gestión, de las Bases de Datos.
- Operar y gestionar los servicios de bases de datos.
- Actividades permanentes DBA SQL Server:
- Operar y gestionar las estructuras de las bases de datos
- Operar y gestionar la actividad de los datos

- Operar y gestionar los usuarios de las bases de datos
- Operar y gestionar la memoria
- Operar y gestionar el I/O
- Operar y gestionar el espacio en disco asignado a las BD
- Revisar permanentemente las alertas y logs de la BD, para evitar indisponibilidad de estas o del servicio.
- Realizar el análisis de rendimiento de las BD
- Realizar el análisis de costos de instrucciones sobre la Base de Datos
- Aplicar permanentemente procedimientos de afinamiento a las bases de datos, con revisión de parámetros y configuración de estas.
- Aplicar los Parches de la Base de datos que corrijan Bugs y errores
- Mantener documentados los cambios realizados en las bases de datos.
- Instalar, actualizar o eliminar el software del motor de base de datos en los diferentes servidores, de acuerdo con el licenciamiento proporcionado por el Alcaldía de Medellín.
- Generar los reportes periódicos a los líderes respectivos, para el análisis pertinente.
- Generar informes actualizados relativos a la plataforma.
- Realizar las respectivas remediaciones a las vulnerabilidades que se encuentren en la plataforma de Bases de Datos SQL Server de acuerdo con las recomendaciones de seguridad informática que se indiquen, en los tiempos establecidos dentro de los ANS contemplados para estas actividades.
- Coordinar con los responsables del Distrito todos los cambios significativos que se vayan a realizar en la Administración de las Bases de datos, para disminuir los impactos negativos sobre la operación.
- Realizar la migración de las bases de datos a las nuevas versiones liberadas, de acuerdo con los planes aprobados por el Alcaldía de Medellín.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento

Administración de bases de datos no relacionales NoSQL: MongoDB y CrateDB:

- Crear las instancias de bases de datos que sean requeridas por el Alcaldía de Medellín

- Realizar la migración de las bases de datos a las nuevas versiones liberadas, de acuerdo con los planes aprobados por el Alcaldía de Medellín.
- Crear las tareas administrativas para nuevos requerimientos de gestión, de las Bases de Datos no relacionales.
- Operar y gestionar los servicios de bases de datos no relacionales.

Actividades permanentes DBA de bases de datos no relacionales NoSQL:

- Operar y gestionar las estructuras de las bases de datos
- Operar y gestionar la actividad de los datos
- Operar y gestionar los roles y permisos de los usuarios en las bases de datos
- Operar y gestionar la memoria
- Operar y gestionar el I/O
- Operar y gestionar el espacio en disco asignado a las BD
- Revisar permanentemente las alertas y logs de la BD, para evitar indisponibilidad de estas o del servicio.
- Realizar el análisis de rendimiento de las BD
- Realizar el análisis de costos de instrucciones sobre la Base de Datos
- Aplicar permanentemente procedimientos de afinamiento a las bases de datos, con revisión de parámetros y configuración de estas.
- Aplicar los Parches de la Base de datos que corrijan Bugs y errores
- Mantener documentados los cambios realizados en las bases de datos.
- Instalar, actualizar o eliminar el software del motor de base de datos en los diferentes servidores, de acuerdo con el licenciamiento proporcionado por el Alcaldía de Medellín.
- Generar los reportes periódicos a los líderes respectivos, para el análisis pertinente.
- Generar informes actualizados relativos a la plataforma.
- Realizar las respectivas remediaciones a las vulnerabilidades que se encuentren en la plataforma de acuerdo con las recomendaciones de seguridad informática y del proveedor que se indiquen, en los tiempos establecidos dentro de los ANS contemplados para estas actividades.
- Coordinar con los responsables del Distrito todos los cambios significativos que se vayan a realizar en la Administración de las Bases de datos, para disminuir los impactos negativos sobre la operación.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones

- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento

Formación profesional:

- Formación profesional en Ingeniería de Sistemas, Electrónica Telecomunicaciones con 48 meses de experiencia laboral.
- Acreditar certificación en bases de datos SQL Server.

Experiencia laboral:

- Acreditar 36 meses de experiencia en la administración y manejo de bases de datos SQL Server.
- Experiencia mínima de 12 meses en la administración de Bases de datos No relacionales NoSQL.

1.21 servicio de administración y soporte especializado de bases de datos Postgresql, mariadb y oracle

Para este servicio se desarrollan las siguientes actividades:

- Crear las instancias de bases de datos que sean requeridas por el Alcaldía de Medellín en cualquiera de los sistemas operativos dispuestos para tal fin.
- Mantener actualizado los diseños de las arquitecturas de los ambientes de las bases de datos PostgreSQL - MariaDB - Oracle.
- Sugerir y diseñar planes de contingencias y mejoramiento frente a las posibles eventualidades que se puedan presentar en las bases de datos PostgreSQL - MariaDB - Oracle.
- Instalar y configurar los motores de bases de datos que sean requeridos por el Alcaldía de Medellín en cualquiera de los sistemas operativos dispuestos para tal fin.

- Instalar, configurar, operar y gestionar las herramientas gráficas de monitoreo para los motores de bases de datos requeridos.
- Operar y gestionar las bases de datos a través de herramientas gráficas o mediante comandos a través de los sistemas operativos en los cuales se encuentren instaladas las BD.
- Operar y gestionar, mantener disponible y gestionar de forma eficiente, las bases de datos Oracle, Postgresql y MariaDB de la Alcaldía de Medellín.
- Realizar la migración de las bases de datos a las nuevas versiones liberadas, de acuerdo con los planes aprobados por el Alcaldía de Medellín.
- Crear las tareas administrativas para nuevos requerimientos de gestión, de las Bases de Datos.
- Aplicar los Parches a la Base de datos que corrijan Bugs y errores de vulnerabilidades.
- Mantener documentados los cambios realizados en las bases de datos.
- Realizar las respectivas remediaciones a las vulnerabilidades que se encuentren en las Bases de Datos Oracle, Postgresql y MariaDB, de acuerdo con las recomendaciones de seguridad informática que se indiquen, en los tiempos establecidos dentro de los ANS contemplados para estas actividades.
- Operar y gestionar las actividades de recuperación de las Bases de Datos.
- Operar y gestionar la tecnología de alta disponibilidad en Bases de Datos para los ambientes en los cuales exista la plataforma proporcionada por el Municipio.
- Analizar e identificar aquellas instrucciones o sentencias creadas en las bases de datos por los desarrolladores que afectan el rendimiento o la estabilidad en los servidores.
- Crear script de optimización y ejecución de tareas que permitan mejorar la administración de las Bases de Datos.
- Coordinar con los responsables del Distrito todos los cambios significativos que se vayan a realizar en la Administración de las Bases en los diferentes motores, para disminuir los impactos negativos sobre la operación.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento

Formación profesional:

- Formación profesional en Ingeniería de Sistemas, Electrónica Telecomunicaciones y/o afines con 48 meses de experiencia laboral.
- Acreditar 36 meses de experiencia en la administración y manejo de bases de datos Oracle.
- Acreditar conocimientos en SQL, PL/PgSQL y PL/SQL y afinamiento de bases de datos.

Experiencia laboral:

- Acreditar 12 meses de experiencia en la administración y manejo de bases de datos PostgreSQL.
- Acreditar 12 meses de experiencia en la administración y manejo de bases de datos MariaDB.

1.22 Servicio de gestión de solicitudes de la administración y soporte de bases de datos postgresql, mariadb y oracle

Para este servicio se desarrollan las siguientes actividades:

- Operar y gestionar los servicios de bases de datos.
- Operar y gestionar las estructuras de las bases de datos.
- Operar y gestionar la actividad de la base de datos.
- Operar y gestionar los usuarios de las bases de datos.
- Operar y gestionar la memoria.
- Operar y gestionar el I/O (Input Output).
- Administrar el espacio en disco asignado a las BD. Si las bases de datos tienen un espacio mayor al 85% del asignado, los DBAs deben recibir notificaciones e incrementar el espacio, para evitar caídas de los servicios.
- Operar y gestionar las BD en sistemas operativos Windows, Linux, AIX.
- Monitorear las BD en los servidores AIX.
- Generar reportes de las estructuras y parámetros de las BD.
- Revisar permanentemente las alertas y logs de la BD, para evitar indisponibilidad de estas o del servicio.
- Realizar el análisis de rendimiento de las BD.
- Realizar el análisis de costos de instrucciones sobre la Base de Datos (BD).

- Aplicar permanentemente procedimientos de afinamiento a las bases de datos, con revisión de parámetros y configuración de estas.
- Realizar particionamiento de tablas en los casos que sea requerido siempre y cuando se cuente con el respectivo licenciamiento.
- Monitorear y ajustar los parámetros de la base de datos.
- Operar y gestionar los control files, tablespace, archivos redolog, achivos dump.
- Realizar la administración de los usuarios a nivel de base de datos.
- Mantener la integridad de identidad, semántica y referencial.
- Administración y mantenimiento de los diferentes elementos de la base de datos (instancias, vistas, vistas versionadas, esquemas).
- Generar y analizar las estadísticas relativas al rendimiento de base de datos con el fin de identificar áreas potenciales del problema y buscar las opciones de mejoramiento que mejoren el performance de la Base de datos. Se deben generar reportes por demanda, el cual debe incluir las acciones que se tomaron para mejorar los indicadores de desempeño del servicio.
- Realizar o documentar las hojas de vida de las BD significativas y críticas.
- Documentar los procedimientos realizados generando los archivos respectivos, e informar al administrador de la plataforma ARCGIS para que alimente la base de datos del conocimiento.
- Realizar el apoyo técnico en la migración de datos de la Base de datos.
- Aplicación y apoyo técnico en PL/SQL y PGSQL

NOTA: El Servicio de administración de bases de datos Oracle, pPstgreSQL y Maria DB, incluye:
Todas las tareas administrativas que deba realizar, utilizando el software de administración de base de datos proporcionado por el Alcaldía de Medellín o mediante comandos través de los sistemas operativos.

La administración de estas bases de datos contempla a nivel general, la creación, modificación, actualización, respaldo, recuperación, análisis de rendimiento, optimización y apoyo en la implementación de bases de datos, bajo los principios de confiabilidad, seguridad, disponibilidad e Integridad.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en:
- Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática o afines.

- Conocimientos básicos en bases de datos.
- Acreditar conocimientos en ITIL.
- Acreditar conocimientos en SQL.

Experiencia laboral:

- Acreditar 12 meses de experiencia en la administración y manejo de bases de datos

1.23 Servicio de gestión y administración de la red de datos

Se solicita administración de la red de datos con servicios calificados para operar infraestructuras de red complejas como la de la Alcaldía de Medellín, cumpliendo con las funciones solicitadas.

La administración de la red de datos también incluye la gestión de los enlaces de telecomunicaciones, entre la sede principal de la Alcaldía de Medellín y las demás sedes de la administración, distribuidas en toda la ciudad y sus corregimientos; en sus diferentes tecnologías, incluyendo enlaces propios y enlaces proporcionados por empresas de telecomunicaciones.

Las siguientes son las actividades permanentes que deben ser atendidas:

- Realizar la administración y Operación del Backbone y Red Ethernet (elementos activos y pasivos) que permitan mantener la operatividad de la infraestructura de red de la Alcaldía de Medellín.
- Realizar la Administración y Operación de la Red LAN.
- Brindar soporte técnico en sedes externas cuando sea solicitado
- Realizar las configuraciones necesarias para que la red opere con protocolo IPV6, de acuerdo con las necesidades de la Alcaldía de Medellín.
- Gestión e implementación de soluciones en IPV6.
- Brindar soporte en IPV6
- Gestionar y configurar los equipos de acuerdo con las políticas definidas y entregadas por Alcaldía de Medellín.
- Realizar el análisis de Tráfico de Red con herramientas de software especializadas para tal fin. De acuerdo con los resultados proponer las soluciones posibles e implementarlas en apoyo con el Alcaldía de Medellín.

- Escalar hasta los fabricantes previa aprobación de la administración y/o el supervisor para la solución de problemas de alto nivel, de acuerdo con los niveles de servicio (ANS) establecidos por el Alcaldía de Medellín con terceros.
- Acompañar y monitorear, el mantenimiento preventivo, correctivo y actualizaciones del hardware y software de red involucrado en la plataforma a nivel de LAN, WAN y telefonía, manteniéndolo vigente a través de nuevos drivers o funcionalidades liberadas; dentro de los horarios que no afecten la operación y acorde con los contratos de soporte y mantenimiento que posea el Alcaldía de Medellín.
- Realizar los reportes mensuales de equipos en stock, traslados, ubicación, cambios, estado, versión de software y lo que sea requerido para tener un control sobre la gestión de operación de la red de datos de la Alcaldía de Medellín.
- Tramitar la garantía de partes de equipos con los fabricantes o empresa con los cuales se tenga contratado el servicio de soporte mantenimiento, de acuerdo con los niveles de servicio (ANS) establecidos con terceros e informar al Alcaldía de Medellín sobre el estado del trámite y el cumplimiento de ANS.
- Operar y gestionar el backup de configuraciones de los elementos activos de red, manteniéndolo actualizado y disponible.
- Generar los informes mensualmente de disponibilidad y recursos de la red de la Alcaldía de Medellín.
- Generar programas y procedimientos de mantenimiento preventivo de todos los elementos activos y pasivos contemplados en la propuesta en las redes de la Alcaldía de Medellín y sus sedes externas.
- Realizar las respectivas remediaciones a las vulnerabilidades que se encuentren en la plataforma de telecomunicaciones y telefonía IP, de acuerdo con las recomendaciones de seguridad informática que se indiquen, en los tiempos establecidos dentro de los ANS contemplados para estas actividades.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento
- Aplicar Líneas base de instalación de dispositivos de redes y telecomunicaciones
- Aplicar Hardening de dispositivos de redes y telecomunicaciones por tipo de fabricante

- Actualizar, documentar y elaborar los diagramas lógicos y físicos de los dispositivos de telecomunicaciones, se hará verificación mensual de esta información.
- Realizar la Gestión de Logs de Servidores de dispositivos de redes y telecomunicaciones
- Monitoreo del tráfico de red entre estaciones de usuario y entre servidores
- Realizar análisis y solución de problemas de conectividad
- Desempeñar las demás funciones que le sean asignadas por el jefe inmediato, de acuerdo con la naturaleza del empleo y el área de desempeño
- Realizar PROYECTOS DE TECNOLOGIA BASADOS EN LOS ESQUEMAS DE INNOVACION redes y telecomunicaciones a la medida del rol
- Participar en la implementación, mantenimiento y mejora continua de las plataformas de telecomunicaciones.
- Recomendar mejoras y diseños a nivel de redes LAN.

Formación profesional (1 y 2):

- Formación profesional en ingeniería de sistemas, informática, electrónica, telecomunicaciones o telemática.
- A nivel de certificaciones se solicita que al menos dentro de los perfiles anteriores se posean las siguientes certificaciones:
- IPv6 Forum Certified Course & Network Engineer (Silver).
- CCNA de Cisco.
- IPv6 Forum Course Silver – CS6 (Transversal).
- CCNP de Cisco vigente o vencido.

Experiencia laboral (1 y 2):

- Acreditar como mínimo, 24 meses de experiencia en administración de redes de comunicaciones de datos, equipos de red multicapa y Switches de CORE.

Formación profesional (3):

- Profesional en ingeniería de sistemas, informática, electrónica, telecomunicaciones o telemática.

- Acreditar las siguientes certificaciones:
- SmartZone SE and Partner Assessment - Accreditation Exam (Ruckus).
- IPv6 Forum Course Silver – CS6 (Transversal).
- IPV6 Forum Course Network Engineer (CNE6)

- FCSS - SD-WAN 7.2 Self-Paced
- FCA - FortiGate 7.4 Operator Self-Paced
- Fortinet Secure Wireless LAN

Experiencia laboral (3):

- Experiencia laboral de 24 meses, de los cuales debe acreditar experiencia específica: Acreditar 24 meses de experiencia profesional en, Mínimo 24 meses de experiencia en gestión, soporte y administración de redes de datos, wifi y switchs core.

1.24 Servicio de gestión de enlaces de datos

El objetivo de este servicio es la administración, operación y monitoreo de los enlaces de datos que comunican el CAD con las diferentes sedes de la Alcaldía de Medellín y escalar si es necesario al proveedor de servicios en caso de problema, mal funcionamiento o poco rendimiento.

A continuación, se describen las actividades que debe ejecutar este servicio:

- Realizar la administración, operación y monitoreo de los enlaces de datos que comunican las diferentes sedes de la Alcaldía de Medellín y escalar si es necesario al proveedor de servicios en caso de problema, mal funcionamiento o poco rendimiento.
- Mantener actualizados y disponibles los mapas de arquitectura en formato digital de los enlaces de datos propios y terceros, que sean necesarios para mantener documentada la topología de telecomunicaciones de las sedes de la Alcaldía de Medellín, en las carpetas digitales que se designen para dicho fin. Se realizará verificación mensual de esra información.
- Realizar el análisis de Tráfico de los enlaces de datos con herramientas de software especializadas para tal fin. De acuerdo con los resultados, proponer las soluciones posibles e implementarlas en apoyo con el Alcaldía de Medellín.
- Realizar las respectivas remediaciones a las vulnerabilidades que se encuentren en la plataforma telecomunicaciones de las sedes externas, de acuerdo con las recomendaciones de seguridad informática que se indiquen, en los tiempos establecidos dentro de los ANS contemplados para estas actividades.

- Acompañar y monitorear, el mantenimiento preventivo, correctivo y actualizaciones del hardware y software de los enlaces de datos, manteniéndolos vigente a través de nuevos drivers o funcionalidades liberadas; dentro de los horarios que no afecten la operación y acorde con los contratos de soporte y mantenimiento que posea el Alcaldía de Medellín.
- Proponer mejoras para la optimización del uso del ancho de banda de las sedes conectadas al Alcaldía de Medellín.
- Realizar los reportes mensuales de equipos en stock, traslados, ubicación, cambios, estado, versión de software y lo que sea requerido para tener un control sobre la gestión de operación de la red de datos de la Alcaldía de Medellín.
- Tramitar la garantía de partes de equipos con los fabricantes o empresa con los cuales se tenga contratado el servicio de soporte mantenimiento, de acuerdo con los niveles de servicio (ANS) establecidos con terceros e informar al Alcaldía de Medellín sobre el estado del trámite y el cumplimiento de ANS.
- Operar y gestionar el Backup de configuraciones de los elementos activos de los enlaces de datos, manteniéndolo actualizado y disponible.
- Generar los informes mensualmente de disponibilidad y recursos de los enlaces de datos de la Alcaldía de Medellín.
- Generar programas y procedimientos de mantenimiento preventivo de todos los elementos activos y pasivos contemplados en la propuesta en las redes de la Alcaldía de Medellín y sus sedes externas.
- Presentar planes y proyectos tendientes a mejorar la infraestructura tecnológica de los enlaces de datos de la Alcaldía de Medellín con sus sedes externas.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.
- Gestión de usuarios y dispositivos, esto incluye la creación de cuentas de usuario, la asignación de permisos a los usuarios y la administración de los dispositivos conectados a la plataforma.
- Seguridad de la plataforma WiFi, esto incluye la implementación de medidas de seguridad para proteger la plataforma de ataques externos.
- Monitoreo y mantenimiento de la plataforma WiFi, esto incluye la supervisión del rendimiento de la plataforma y la implementación de las actualizaciones necesarias.

Formación profesional:

- Formación profesional en ingeniería de sistemas, informática, electrónica, telecomunicaciones o telemática.

- A nivel de certificación dentro del perfil anterior se debe tener:
- Certified Wireless Technology Specialist
- SmartZone SE and Partner Assessment - Accreditation Exam (Ruckus).
- CCNA vigente o vencido.
- IPv6 Forum Course Silver – CS6 (Transversal).
- Trabajo en alturas.

Experiencia laboral:

- Acreditar experiencia de mínimo, 24 meses en soporte y mantenimiento en soluciones de enlaces inalámbricos y/o redes inalámbricas WI- FI.

1.25 Servicio de administración de la plataforma de telefonía ip

Para la plataforma de telefonía se solicita administración remota desde el NOC del proveedor, con servicio calificado para operar plataformas de telefonía con más de 4500 extensiones IP, en tecnología AVAYA como la de la Alcaldía de Medellín, cumpliendo con las funciones solicitadas.

Las siguientes son las actividades permanentes que deben ser atendidas:

- Monitorear, operar y gestionar los servidores de comunicaciones de la red de voz.
- Creación de extensiones IP.
- Creación de coberturas.
- Administración de códigos de llamadas nacionales, celulares o Internacionales previa autorización de la Alcaldía de Medellín y conforme a las políticas vigentes.
- Creación y gestión de troncales digitales.
- Actualización de firmware para los teléfonos IP y la plataforma de telefonía.
- Tramitar la garantía de partes de equipos con los fabricantes o empresa con los cuales se tenga contratado el servicio de soporte mantenimiento, de acuerdo con los niveles de

servicio (ANS) establecidos con terceros e informar al Alcaldía de Medellín sobre el estado del trámite y el cumplimiento de ANS.

- Operar y gestionar el Backup de configuraciones de los elementos activos de la plataforma de telefonía, manteniéndola actualizada y disponible.
- Generar los informes mensualmente de disponibilidad y recursos de plataforma de telefonía de la Alcaldía de Medellín.
- Generar programas y procedimientos de mantenimiento preventivo de todos los elementos activos y pasivos contemplados en la propuesta en las redes de la Alcaldía de Medellín y sus sedes externas.
- Presentar planes y proyectos tendientes a mejorar la infraestructura tecnológica de la plataforma de telefonía de la Alcaldía de Medellín.
- Acompañar y monitorear el mantenimiento preventivo, correctivo y actualizaciones del hardware y software de la plataforma de telefonía, manteniéndola vigente a través de nuevos drivers o funcionalidades liberadas; dentro de los horarios que no afecten la operación y acorde con los contratos de soporte y mantenimiento que posea el Alcaldía de Medellín.
- Realizar las respectivas remediaciones a las vulnerabilidades que se encuentren en la plataforma de telefonía IP, de acuerdo con las recomendaciones de seguridad informática que se indiquen, en los tiempos establecidos dentro de los ANS contemplados para estas actividades.
- Actualización de base de datos de usuarios y extensiones.
- Administración de los recursos operacionales de la plataforma de voz como son números de extensión, equipos telefónicos y troncales.
- Control de inventarios de los equipos de telefonía.
- Estadísticas de llamadas y reportes de consumo a través de software de tarificación.
- Administración del servicio de correo de voz, incluyendo la creación y eliminación de buzones de voz.
- Capacitaciones e implementación de servicios de telefonía IP.
- Gestión de enlaces de troncales primarios.
- Operar y gestionar la herramienta de gestión ASA de las plantas Avaya, suministrada por el Alcaldía de Medellín.
- Configuración de VLANs.
- Configuración de rutas estáticas según se requiera.
- Configuración de protocolos de enrutamiento dinámicos según se requiera.
- Configuración de protocolos de redundancia.

- Aplicación de listas de acceso si es del caso.
- Aplicación de protocolos de calidad de servicio (audio y prioridades).
- Revisión y lectura continúa de log y alarmas, que permitan realizar detección temprana de problemas y eventos.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento

Formación profesional:

- Formación profesional en ingeniería de sistemas, informática, electrónica, telecomunicaciones o telemática.
- Experiencia profesional mínima de 18 meses, en soporte de telefonía IP en plataformas AVAYA.
- Formación tecnológica en sistemas, informática, electrónica, telecomunicaciones o telemática.
- A nivel de certificación dentro del perfil se debe tener:
- IPv6 Forum Course Silver – CS6 (Transversal)
- certificación Avaya AIPS

Experiencia laboral:

- Experiencia profesional mínima de 12 meses, en soporte de telefonía IP en plataformas AVAYA.

1.26 Servicio de administración de la plataforma de datos abiertos

Dentro de las actividades de este servicio se encuentran:

- Instalar y configurar los nodos de datos de la plataforma Cloudera.
- Configurar y balancear la carga de los componentes para lograr el mejor aprovechamiento de los recursos y mantenimiento de la calidad de servicio de la plataforma.

- Proponer y ejecutar planes de expansión de la infraestructura que se requieran, previa concertación y aprobación de la Alcaldía de Medellín.
- Actualizar los diagramas de arquitectura de la plataforma Hadoop Cloudera; y elaborar la documentación de las diferentes conexiones, y los procedimientos para restablecimiento de los servicios que se cataloguen como de nivel crítico.
- Realizar el restablecimiento de los servicios que se cataloguen como de nivel crítico en la plataforma Cloudera.
- Monitoreo de la plataforma y manejo de alertas con su correspondiente solución
- (troubleshooting).
- Acompañamiento técnico para la identificación las fuentes de conexión y la estructura de los datos a Integrar en las plataformas Cloudera del Distrito Medellín.
- Aplicar las recomendaciones que se emitan para la plataforma desde las entidades de Auditoría y de manera concertada con el Alcaldía de Medellín.
- Acompañar al proveedor a realizar la actualizar la plataforma Cloudera de acuerdo con los releases de versionamiento periódicos que afecta el fabricante, para mantener su funcionalidad y aprovechar las nuevas características y parches de seguridad.
- Actualizar el sistema operativo de los nodos que componen la plataforma Cloudera, de acuerdo con los requerimientos necesarios para garantizar la compatibilidad con los releases de versionamiento que efectúe el fabricante.
- Mantener Operativo los Host de Vmware en los cuales se encuentra configurada la plataforma de Cloudera.
- Realizar los diagnósticos correspondientes, para prevenir Fallas en las diferentes plataformas que conforma los servicios de Cloudera y Hadoop.
- Generar los diferentes escalamientos a los proveedores de sistema operativo, virtualización y Cloudera para la atención de incidentes.

Formación profesional:

- Título Profesional o superior en disciplina académica: Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones y Afines o Ingeniería de Sistemas, Telemática y Afines
- Experiencia de por lo menos 2 años gestionando la infraestructura de la plataforma hadoop y/o Claudera.

Experiencia laboral:

- Experiencia mínima de 2 años en administración de servidores con Sistema Operativo Linux.
- Experiencia mínima de 1 año en administración de redes.

2 SEGURIDAD INFORMÁTICA

El objetivo es proteger la integridad, confidencialidad y disponibilidad de la información que se gestiona a través de la infraestructura informática de la Alcaldía de Medellín y todo lo relacionado con esta (incluyendo la información contenida), bajo la aplicación de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas, para minimizar los posibles riesgos a la infraestructura o a la información comprendiendo: bases de datos, metadatos, archivos y todo lo que la organización valore como información privilegiada o confidencial y la infraestructura informática discriminada en la línea base y su crecimiento.

El equipo debe propender por:

- Definir las acciones y procedimientos a emprender y elegir los servicios a contactar en caso de detectar una posible intrusión.
- Sensibilizar a los diferentes responsables de administrar las plataformas tecnológicas sobre los temas relacionados con la seguridad de los sistemas informáticos, políticas y sus repercusiones, mínimo cada 6 meses, y en un tiempo no superior a 1 mes para los servicios nuevos dentro de la prestación del servicio.
- Presentación de planes y proyectos, así como avances de estos, para reducir los riesgos de acuerdo con la infraestructura de seguridad con la que cuenta el Alcaldía de Medellín de manera trimestral.
- Identificar, e informar a los responsables de las plataformas, las vulnerabilidades existentes en la infraestructura tecnológica (Servidores, aplicaciones, bases de datos, sistemas de información, entre otras), de acuerdo con las políticas de periodicidad que establezca el Alcaldía de Medellín.
- Todas las demás que implique el cumplimiento de los controles del Anexo A del estándar ISO 27001 versión 2013 o su versión más reciente.
- Mantener informado al Alcaldía de Medellín, sobre los eventos e incidentes de seguridad informática que se presenten en la infraestructura tecnológica.

- Documentar todas las acciones realizadas sobre la plataforma tecnológica, relacionadas con cambios, implementaciones, incidentes y todas las actividades propias del desempeño del grupo de Seguridad Informática.
- Entregar informes mensuales, con un resumen de las acciones que fueron ejecutadas con la misma. El detalle de estas deberá reposar en una carpeta por su posterior consulta.
- Documentar y mantener actualizada en diagramas e informes la topología que involucre componentes de seguridad informática de la línea base
- Socializar informes de seguridad informática al Alcaldía de Medellín, máximo el día 15 de cada mes.
- Proponer políticas que contribuyan a la seguridad de la información que reside en los sistemas informáticos de la Alcaldía de Medellín y su Infraestructura Tecnológica, tales políticas deben estar alineadas con los objetivos de la organización y deberán de ser avaladas por quien delegue la Administración Distrital para tal fin.
- Proponer mejoras a la gestión de la seguridad informática de la Alcaldía de Medellín, lo que puede incluir arquitectura, plataformas, herramientas, procedimientos, métodos y técnicas
- Instalación y configuración de IDS, IPS entre otros appliance según se requiera
- Administrar, gestionar y soportar la plataforma tecnológica de la Alcaldía de Medellín; referenciada en el documento “línea base de seguridad” y crecimiento de esta durante la vigencia del contrato. Verificar, analizar y proponer de manera escrita, nuevos niveles de control de acceso a la red de la Alcaldía de Medellín, en pro de la seguridad informática, con una frecuencia semestral.
- Establecer medidas de seguridad de acceso lógico mediante consulta y niveles de utilización de la información.
- Proponer políticas de seguridad informática para minimizar el riesgo de ataques externos e internos de manera que el diseño sea funcional para el Alcaldía de Medellín.
- Implementar y verificar el cumplimiento de las políticas de seguridad informática, mediante informe escrito con una periodicidad mensual.
- Dar cumplimiento a todas las políticas de seguridad informática definidas por el Alcaldía de Medellín.
- Aplicar de manera permanente controles a los recursos y/o servicios tecnológicos mediante las herramientas de seguridad informática, previa autorización de la Alcaldía de Medellín.
- Coordinar de manera permanente con el Alcaldía de Medellín las acciones y políticas que se deben aplicar en caso de violaciones a la infraestructura tecnológica.

- Acompañar la instalación y configuración de manera permanente, de soluciones o componentes de seguridad informática de la Alcaldía de Medellín.
- Operar y gestionar los equipos de seguridad informática de la Alcaldía de Medellín.
- Planear, y ejecutar laboratorios e investigaciones de las soluciones de seguridad informática que están bajo la administración de la Mesa, que apoyen y mejoren el área de Seguridad Informática. Los recursos para tales laboratorios serán suministrados por el Alcaldía de Medellín.
- Analizar e informar el estado de la capacidad de los equipos de seguridad informática al Alcaldía de Medellín, con una periodicidad mensual, detallando (Uso de Memoria, Uso de disco, Uso de red, estadísticas de crecimiento, Uso de procesador y demás recursos que ayuden a determinar la capacidad del o los dispositivos).
- Reportar de manera inmediata las novedades que se presenten con la plataforma de seguridad informática al Alcaldía de Medellín y al tercero con el cual se tenga el contrato de soporte.
- Identificar y reportar vulnerabilidades de seguridad que ponen en riesgo la infraestructura informática de la Alcaldía de Medellín, y proponer mejoras que minimicen el mismo.
- Acompañar a los demás administradores de la plataforma de infraestructura de red, en la remediación de las vulnerabilidades identificadas.
- Llevar a cabo las implementaciones que sean necesarias con el propósito de establecer controles orientados a la seguridad de la infraestructura tecnológica de la Alcaldía de Medellín.
- Presentar ante el comité de cambios, las propuestas de cambios que ayuden a prevenir o solucionar riesgos asociados a la infraestructura de tecnológica de la Alcaldía de Medellín.
- Capacitarse y actualizarse en las herramientas de Seguridad informática del Municipio.
- Optimizar la infraestructura de seguridad informática, con el fin de aprovecharla de acuerdo con las necesidades de protección de la Alcaldía de Medellín.
- Detectar, informar y proponer oportunamente medidas de control ante eventos, en aras de evitar o prevenir un incidente de seguridad informática con implicaciones que generen una afectación en la autenticidad, integridad, disponibilidad y confidencialidad, de la Información soportada en la infraestructura tecnológica de la Alcaldía de Medellín.

2.1 Coordinador de seguridad informática

Las actividades por desarrollar por el coordinador de seguridad informática son la siguientes:

- Establecer e implementar políticas relacionadas con la seguridad.
- Dar respuestas y atención de consultas técnicas al equipo de TI de la Alcaldía de Medellín.
- Asegurar la confidencialidad, integridad y disponibilidad de la información en lo que a las tecnologías de la información y las comunicaciones con respecto a los servicios prestados.
- Apoyar a la coordinación del proyecto ante incidentes de seguridad aplicando el plan de respuestas definido, con el fin de atender rápidamente este tipo de eventualidades.
- Hacer seguimiento a la base documental sobre la resolución de incidentes acorde a los servicios prestados.
- Promover la creación y actualización de las políticas de seguridad informática, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.
- Supervisar el cumplimiento normativo, garantizar la privacidad de los datos.
- Apoyar el equipo ante Incidentes de seguridad informática relacionados con la prestación del servicio.
- Proponer procedimientos de seguridad que fortalezcan la política de seguridad informática del Distrito.
- Validar los análisis de vulnerabilidades que solicite el cliente y verificar los informes
- de gestión correspondientes.
- Proponer acciones correctivas para asegurar que se provea la seguridad adecuada en la prestación del servicio.
- Revisar y evaluar periódicamente la política de seguridad y sugerir a la gerencia de la mesa de servicio los cambios necesarios.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en:
- Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática e Informática.
- CISSP o Maestría en seguridad informática

- Acreditar mínimo certificación de “Auditor Interno” en ISO 27001 (Sistemas de Seguridad Informática).
- Experiencia en seguridad informática por un mínimo de 60 meses en empresas de más de 500 usuarios.
- Certificar experiencia con conocimientos de seguridad en entornos tecnológicos, Windows y UNIX, bases de datos Oracle o SQL, en redes WAN y LAN.
- Certificación en Hacking ético.

Experiencia laboral:

- Certificar experiencia en el área de seguridad informática mínimo 36 meses.

2.2 Gestión de seguridad informática en redes de datos y telecomunicaciones

Será responsable de la administración, configuración, disponibilidad y trazabilidad de los dispositivos de seguridad perimetral de la Alcaldía de Medellín asignados, incluyendo la atención de incidencias y su escalamiento al proveedor cuando sea requerido; también debe realizar la detección, reporte y corrección de eventos y alarmas de seguridad informática de las plataformas a su cargo; así como del mantenimiento operativo de las plataformas, según el licenciamiento adquirido y las recomendaciones del fabricante, incluyendo las actividades de actualización permanente de los productos; adicionalmente, debe identificar las vulnerabilidades relacionadas con la infraestructura de redes y telecomunicaciones, reportarlas y verificar de manera periódica el estado de las acciones de remediaciones que hayan sido solicitadas; Mantener actualizado los procedimientos e instructivos utilizados para la prestación de los servicios de operación de las plataformas a su cargo y remitirlos a la Unidad de Seguridad Informática para su aprobación; adicionalmente debe ejecutar todas las actividades que se requieran por la Unidad de Seguridad informática propias del desarrollo de sus actividades. Realizar las configuraciones requeridas para configurar y mantener el balanceo de carga en las peticiones realizadas desde el lado de NGINX y Wordpress.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática e Informática.

- Acreditar certificación en CCNA Security Vigente (Cisco Certified Network Associate Security) o Especialización profesional en Seguridad Informática, esta última si relacionó experiencia mínima de 12 meses en seguridad informática.
- Deseable: Acreditar certificación vigente CBROPS (Cisco Certified Cybersecurity Operations).

Experiencia laboral:

- Experiencia mínima de 12 meses en seguridad informática o Especialización profesional en Seguridad Informática. Acreditar conocimiento en ISO 27001 (Sistemas de Gestión de Seguridad de la información).

2.3 Gestión de seguridad informática en bases de datos

Será responsable de la administración, configuración, disponibilidad y trazabilidad de los dispositivos de seguridad de bases de datos de la Alcaldía de Medellín asignados, incluyendo la atención de incidencias y su escalamiento al proveedor cuando sea requerido; también debe realizar la detección, reporte y corrección de eventos y alarmas de seguridad informática de las plataformas a su cargo; así como del mantenimiento operativo de las plataformas, según el licenciamiento adquirido y las recomendaciones del fabricante, incluyendo las actividades de actualización permanente de los productos; adicionalmente, debe identificar las vulnerabilidades relacionadas con los motores de bases de datos existentes en la plataforma de la entidad, reportarlas y verificar de manera periódica el estado de las acciones de remediaciones que hayan sido solicitadas; Mantener actualizado los procedimientos e instructivos utilizados para la prestación de los servicios de operación de las plataformas a su cargo y remitirlos a la Unidad de Seguridad Informática para su aprobación; adicionalmente debe ejecutar todas las actividades que se requieran por la Unidad de Seguridad informática propias del desarrollo de sus actividades.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática e Informática.
- Acreditar conocimiento ISO 27001(Sistemas de Seguridad Informática),
- Certificar conocimientos en seguridad de aplicaciones Web.
- Certificar formación y/o conocimientos en Hacking ético.

Experiencia laboral:

- Experiencia mínima de 18 meses en seguridad informática.

2.4 Gestión de seguridad informática en servidores

Será responsable de la administración, configuración, disponibilidad y trazabilidad de los dispositivos de seguridad destinados a la protección de los servidores de la Alcaldía de Medellín asignados, incluyendo la atención de incidencias y su escalamiento al proveedor cuando sea requerido; también debe realizar la detección, reporte y corrección de eventos y alarmas de seguridad informática de las plataformas a su cargo; así como del mantenimiento operativo de las plataformas, según el licenciamiento adquirido y las recomendaciones del fabricante, incluyendo las actividades de actualización permanente de los productos; adicionalmente, debe identificar las vulnerabilidades relacionadas con los servidores existentes en la plataforma de la entidad, reportarlas y verificar de manera periódica el estado de las acciones de remediaciones que hayan sido solicitadas; Mantener actualizado los procedimientos e instructivos utilizados para la prestación de los servicios de operación de las plataformas a su cargo y remitirlos a la Unidad de Seguridad Informática para su aprobación; adicionalmente debe ejecutar todas las actividades que se requieran por la Unidad de Seguridad informática propias del desarrollo de sus actividades.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática e Informática.
- Acreditar certificación en ISO 27001 (Sistemas de Gestión en Seguridad de la información).
- Acreditar certificación en CBROPS (Cisco Certified Cybersecurity Operations) o CISSP vigentes.
- Acreditar conocimientos de seguridad en entornos tecnológicos, Windows y UNIX.
- Acreditar conocimientos en Informática forense. Se puede acreditar mediante una constancia emitida por la empresa donde labora que desarrolla actividades orientadas al tema o mediante un curso del tema (no certificación).
- Acreditar conocimientos en criptografía.
- Acreditar conocimientos en IDS e IPS.

Experiencia laboral:

- Experiencia mínima de 18 meses en seguridad informática.

2.5 Gestión de seguridad informática en aplicaciones

Será responsable de la administración, configuración, disponibilidad y trazabilidad de los dispositivos de seguridad de aplicaciones de la Alcaldía de Medellín asignados, incluyendo la atención de incidencias y su escalamiento al proveedor cuando sea requerido; también debe realizar la detección, reporte y corrección de eventos y alarmas de seguridad informática de las plataformas a su cargo; así como del mantenimiento operativo de las plataformas, según el licenciamiento adquirido y las recomendaciones del fabricante, incluyendo las actividades de actualización permanente de los productos; Mantener actualizado los procedimientos e instructivos utilizados para la prestación de los servicios de operación de las plataformas a su cargo y remitirlos a la Unidad de Seguridad Informática para su aprobación; adicionalmente debe ejecutar todas las actividades que se requieran por la Unidad de Seguridad informática propias del desarrollo de sus actividades.

También será responsable de la identificación de vulnerabilidades en las aplicaciones que se pretendan integrar o se encuentren integradas a los servicios informáticos de la Alcaldía de Medellín sujeto a las herramientas que serán provistas por la entidad, y de acuerdo con las solicitudes emitidas desde la unidad de seguridad informática, elaborando el reporte de los resultados obtenidos y remitiéndolos a la misma, así como verificando posteriormente el proceso de remediación solicitado y emitiendo concepto al respecto; además del diseño y aplicación de pruebas de penetración para la identificación de vulnerabilidades y defectos de seguridad en las aplicaciones que sean puestos bajo se revisión. También deberá, a partir de las vulnerabilidades que sean identificadas, emitir recomendaciones orientadas a mejorar la configuración de los equipos existentes para mantener o aumentar la protección de las aplicaciones operadas por la Alcaldía de Medellín.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática e Informática.
- Acreditar certificación vigente de Seguridad en Aplicaciones Web CSWAE (Certified Secure Web Application Engineer).
- Experiencia mínima de 18 meses en seguridad informática en aplicaciones web, para la identificación o remediación de vulnerabilidades.

Experiencia laboral:

- Experiencia mínima de 24 meses en desarrollo de software en aplicaciones web.

2.6 Gestión de seguridad informática en protección de punto final

Será responsable de la administración, configuración, disponibilidad y trazabilidad de los dispositivos de seguridad destinados a la protección de los equipos de usuario final de la Alcaldía de Medellín (Herramientas de Protección de Punto Final Corporativa) asignados, incluyendo la atención de incidencias y su escalamiento al proveedor cuando sea requerido; también debe realizar la detección, reporte y corrección de eventos y alarmas de seguridad informática de las plataformas a su cargo; así como del mantenimiento operativo de las plataformas, según el licenciamiento adquirido y las recomendaciones del fabricante, incluyendo las actividades de actualización permanente de los productos; adicionalmente, debe identificar las vulnerabilidades relacionadas con los equipos. De igual manera, aplicar las configuraciones de políticas necesarias para la administración de la consola y los agentes de las herramientas de seguridad de punto final implementadas: instalación, actualización, configuración, usuario final existentes en la entidad, reportarlas y verificar de manera periódica el estado de las acciones de remediaciones que hayan sido solicitadas; Mantener actualizado los procedimientos e instructivos utilizados para la prestación de los servicios de operación de las plataformas a su cargo y remitirlos a la Unidad de Seguridad Informática para su aprobación; adicionalmente debe ejecutar todas las actividades que se requieran por la Unidad de Seguridad informática propias del desarrollo de sus actividades.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática e Informática.
- Certificación en protección antimalware de punto final, expedida por el fabricante.

Experiencia laboral:

- Experiencia mínima de 18 meses en administración de herramientas antimalware.

2.7 Gestión de seguridad informática en detección y respuesta

Será responsable de la visibilidad, detección, respuesta y contención de los incidentes de seguridad informática y la administración, configuración, disponibilidad y trazabilidad de los dispositivos de seguridad destinados a la gestión de alertas y visibilidad de eventos presentados (Herramientas de manejo y consolidación de logs y correlación de eventos) asignados, incluyendo la atención de incidencias y su escalamiento al proveedor cuando sea requerido; también debe realizar la detección, reporte y corrección de eventos y alarmas de seguridad informática de las herramientas a su cargo; así como del mantenimiento operativo de las plataformas, según el licenciamiento adquirido y las recomendaciones del fabricante, incluyendo las actividades de actualización permanente de los productos; adicionalmente, mantener actualizado los procedimientos e instructivos utilizados para la prestación de los servicios de operación de las plataformas a su cargo y remitirlos a la Unidad de Seguridad Informática para su aprobación; así como ejecutar todas las actividades que se requieran por la Unidad de Seguridad informática propias del desarrollo de sus actividades.
De igual manera, aplicar las configuraciones de políticas necesarias para la administración de las herramientas de seguridad a su cargo (instalación, actualización, configuración, desinstalación), así como brindar el soporte adecuado a los usuarios, según las incidencias reportadas o detectadas.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática e Informática.
- Acreditar conocimientos de seguridad en entornos tecnológicos, Windows y UNIX.
- Acreditar conocimiento en ISO 27001 (Sistemas de Gestión de Seguridad de la información).
- Certificación Analista de SOC – CSA o experiencia verificable que incluya temas asociados al análisis y procesamiento de logs.

Experiencia laboral:

- Experiencia mínima de 18 meses certificable en funciones propias de seguridad informática.

2.8 Gestión de seguridad informática en el control de acceso de usuarios con cuentas privilegiadas

Será responsable de la administración, configuración, disponibilidad y trazabilidad de los dispositivos de seguridad destinados al control de acceso de usuarios con cuentas privilegiadas a dispositivos de la plataforma informática de la Alcaldía de Medellín con cobertura disponible, incluyendo la atención de incidencias y su escalamiento al proveedor cuando sea requerido; también debe realizar la detección, reporte y corrección de eventos y alarmas de seguridad informática de las plataformas a su cargo; así como del mantenimiento operativo de las plataformas, según el licenciamiento adquirido y las recomendaciones del fabricante, incluyendo las actividades de actualización permanente de los productos; adicionalmente, debe identificar las vulnerabilidades relacionadas con los servidores existentes en la plataforma de la entidad, reportarlas y verificar de manera periódica el estado de las acciones de remediaciones que hayan sido solicitadas; Mantener actualizado los procedimientos e instructivos utilizados para la prestación de los servicios de operación de las plataformas a su cargo y remitirlos a la Unidad de Seguridad Informática para su aprobación; adicionalmente debe ejecutar todas las actividades que se requieran por la Unidad de Seguridad informática propias del desarrollo de sus actividades.

De igual manera, ejecutar las actividades que sean necesarias para la puesta en operación adecuada del control de acceso de usuarios con cuentas privilegiadas de acuerdo con las medidas de control adoptadas por la entidad, para facilitar la implementación de acciones que permitan controlar el acceso no autorizado a los dispositivos de tecnologías de información y de las comunicaciones cubiertos por la plataforma, así como la implementación de medidas de trazabilidad del acceso de usuarios con cuentas privilegiadas en las ventanas de tiempo autorizadas y para los servicios debidamente autorizados, así como la segregación de privilegios asociados a la ejecución de comandos desde las cuentas de usuario privilegiadas, la rotación de las contraseñas de cuentas de usuarios privilegiadas, entre otras que puedan aportar a mitigar los riesgos de afectación a la disponibilidad, confidencialidad o integridad sobre la plataforma informática.

Formación profesional:

- Título profesional en disciplina académica del Núcleo Básico del Conocimiento - NBC en: Ingeniería Electrónica, Telecomunicaciones o Ingeniería de Sistemas, Telemática e Informática.
- Acreditar conocimientos de seguridad en entornos tecnológicos, Windows y UNIX.
- Acreditar conocimiento en ISO 27001 (Sistemas de Gestión de Seguridad de la información).

Experiencia laboral:

- Experiencia mínima de 18 meses certificable en funciones propias de seguridad informática.

3. PERSONAL DIRECTIVO DE LA MESA DE SERVICIO

3.1 Gerente de proyecto

Deberá gestionar el desarrollo y la puesta en marcha de la operación de la Mesa de Servicios, asegurar el cumplimiento de los niveles de servicio definidos por el Alcaldía de Medellín, generar y presentar informes, coordinar y liderar el personal a su cargo, presentar y desarrollar planes de mejora para la operación, tener relacionamiento adecuado con el cliente, planificar y controla r los recursos asignados (económicos, técnicos, humanos, etc.), tener capacidad de organización y trabajo en equipo, liderazgo y fluidez comunicacional.

Actividades:

- Velar por el cumplimiento de los indicadores del contrato.
- Liderar los proyectos relacionados con el marco de referencia ITIL.
- Liderar lo procesos de documentación al interior de la mesa de servicio.
- Liderar todo el equipo humano a su cargo.
- Gestionar con el proveedor las necesidades que surjan en la ejecución del contrato.
- generar la facturación mensual e acuerdo a los recurso consumidos.
- Propender por la calidad en el servicio.
- Realizar esfuerzos para aumentar las medidas preventivas en cada una de las plataformas tecnológicas.
- Proponer mejoras en la prestación del servicio.
- Generar informes de riesgos sobre cada una de las plataformas tecnológicas.

Formación Profesional:

- Formación profesional en el área de tecnologías de la información y las comunicaciones.
- Academia PMP o preferiblemente certificación Project Management Institute (PMI).
- Acreditar certificación ITIL V3 Foundation.

Experiencia laboral:

- Experiencia profesional mínima 60 meses en labores de gerencia de mesas de servicio.
- Experiencia profesional mínima de 36 meses en Gerencia de Proyectos TI certificada.

3.2 Coordinador de mesa de servicio

Controlar aspectos técnicos durante la ejecución del proyecto, velar por la correcta interacción de los grupos de trabajo, garantizando el cumplimiento de los ANS pactados con el cliente. Planear, coordinar, controlar y evaluar actividades que buscan el cumplimiento de los objetivos del proyecto. Garantizar además el cumplimiento de las responsabilidades según el rol de los procesos que se le asigne.

Principales Responsabilidades:

- Revisión con el gerente de proyecto para presentar seguimiento a los incidentes que se presentan en cualquier momento y que afectan la operación para buscar alternativas inmediatas de solución.
- Realizar los llamados de atención respectivos al personal cuando sea necesario, en pro de cumplir lo solicitado por el Cliente.
- Asistir a reuniones de seguimiento periódico con el grupo de Mesa de ayuda del proyecto y el cliente para revisión de la operación.
- Asistir al comité de gestión de problemas con el cliente 1 vez al mes

- Informar al jefe inmediato y hacer seguimiento a los eventos masivos que puedan afectar la prestación del servicio.
- Informar al jefe inmediato eventos que puedan afectar la ejecución del proyecto.
- Presentar propuestas de mejora en conjunto con los líderes de grupo para ser presentadas al cliente en función de optimizar los servicios prestados en los distintos niveles de soporte que componen el proyecto.
- Coordinar en conjunto con los líderes a cargo, días de compensatorio a asignar teniendo presente no afectar la prestación del servicio.
- Revisar los patrones de compensatorios generados por el personal del proyecto con el fin de mitigar o evaluar cambios en funciones que diere lugar para evitar generar dichos tiempos.
- Revisar y programar las vacaciones de las personas para evitar afectaciones en la operación.
- Apoyar en la elaboración de informes de incidentes masivos donde se identifica la causa raíz, acciones correctivas y preventivas a corto y largo plazo para asegurar el cumplimiento contractual de la disponibilidad de todas las plataformas de tecnología.

- Gestionar ante los responsables de los diferentes equipos de trabajo de TGI las necesidades que tenga el personal del proyecto para la ejecución de sus labores tales como instalaciones de software no estándar, gestión de permisos, de acceso a recursos tecnológicos con las justificaciones correspondientes.
- Generar los informes de gestión, cumplimiento de ANS´s y disponibilidad para revisión con el gerente de Negocio.
- Atención de incidentes o requerimientos particulares con prioridad que el Cliente solicita.
- Generación de estadísticas y reportes del servicio de la mesa de soporte nivel 1 y nivel 2, realizar análisis con el gerente de negocio para tomar medidas que permitan el cumplimiento de compromisos pactados en el contrato.
- Crear, documentar, publicar y actualizar modelos de incidentes, instructivos, protocolos de atención, matrices de escalamiento y garantizar que estos se cumplan.
- Garantizar el cumplimiento con los estándares de operación definidos para la administración de los incidentes y requerimientos del soporte nivel 1 y nivel 2.
- Garantizar que la base de datos de conocimientos de propiedad del cliente sea constantemente actualizada por todos los integrantes de la mesa soporte nivel y nivel 2, donde se almacenará la información referente a los productos y servicios de tecnología con sus respectivos errores conocidos.
- Revisión de las PQRS que se generan en la prestación del servicio en la mesa.
- Coordinar y controlar los recorridos de la camioneta y la ejecución de las actividades que deben realizar soporte nivel 1 y soporte nivel 2.
- Ser el gestor de incidentes y requerimientos de la mesa de servicios, realizar una revisión constante de los incidentes y requerimientos que cumplan con las políticas indicadas por el cliente.
- Reunirse con el gestor de incidentes y requerimientos del cliente para revisar las políticas y el cumplimiento de los procesos.
- Generar informe de encuestas de satisfacción de toda la mesa, realizar análisis, retroalimentar a los analistas. Garantizar que se cumplan los indicadores de satisfacción del usuario pactados en el contrato.
- Generar semanalmente el reporte de los casos abiertos y realizar retroalimentación a los analistas, tomar medidas para garantizar el cumplimiento del cierre de los casos.
- Generar semanalmente el reporte del cumplimiento de ANS´s y realizar retroalimentación a los analistas, tomar medidas para garantizar el cumplimiento de los indicadores.

Formación Académica:

- Formación profesional en Ingeniería de sistemas.
- Acreditar certificación en ITIL V3 Foundation.
- Acreditar certificación OSA de ITIL.
- Experiencia Laboral:
- Experiencia de trabajo en el área de sistemas, mínima de 60 meses, certificada.

3.3 Coordinador de infraestructura de almacenamiento, servidores, bases de datos y backup

Dirigir y coordinar los procesos de atención a los usuarios y el soporte nivel 2 a la infraestructura, para garantizar el cumplimiento de los ANS pactados con el cliente; coordinar la correcta interacción entre los grupos de soporte (Centro de llamada, soporte remoto, soporte en sitio, INSTALAR, MOVER, ACTUALIZAR Y/O CAMBIAR (IMAC) y Laboratorio).

Principales responsabilidades:

- Garantizar que se cumplan las políticas y lineamientos definidos por el cliente para el grupo de soporte nivel 2 y que garanticen las condiciones del contrato.
- Garantizar que se registren y clasifiquen los incidentes, a través de una completa guía de categorización y de prioridades, a través de la herramienta de gestión de incidentes y requerimientos que se emplee.
- Proveer los recursos y el personal necesario a todos los niveles para restaurar el servicio según se define en el ANS correspondiente.
- Garantizar que los diagnósticos que se realicen desde segundo nivel de soporte escalado vía telefónico o en sitio, se pueda concluir que se trata de una solicitud de un cambio, modificación o instalación de uno o más elementos de la configuración sobre la infraestructura del cliente.
- Garantizar que se clasifiquen los incidentes y solicitudes de servicio de acuerdo con la categorización establecida por el cliente: Categoría, subcategoría, síntoma, causa, detalle, grupo y responsable.
- Garantizar Consultar las bases de datos de conocimiento, de Errores Conocidos y de la Gestión de la Configuración, con el fin de encontrar facilidades de análisis, diagnóstico y solución.
- Coordinación y enrutamiento a los diferentes grupos de soporte de los incidentes que no pueden ser solucionados en primer nivel: Si una vez realizado el diagnóstico del incidente

se determina que la solución de este no se puede implementar por la Mesa de Servicios, el incidente debe escalarse al nivel de soporte y analistas del cliente correspondiente, de conformidad con las matrices de escalamiento.

- Generación de estadísticas y reportes del servicio de la mesa de servicio soporte nivel 1.
- Generar y mantener actualizados los procedimientos del servicio, entrenamiento básico a los usuarios para la resolución de cada problema que se presente.
- Crear, documentar, publicar y actualizar modelos de incidentes, instructivos, protocolos de atención, matrices de escalamiento.
- Garantizar el cumplimiento con los estándares de operación definidos para la administración de los incidentes y requerimientos del soporte nivel 1.
- Proponer los procedimientos de cambio o movimiento de equipos, los cuales serán validados y aprobados por el cliente.
- Mantener actualizada la base de datos de conocimientos de propiedad del cliente, donde se almacenará la información referente a los productos y servicios de tecnología con sus respectivos errores conocidos.
- Gestión de PQRS asociadas a la operación del servicio.
- Ser el gestor de problemas de la mesa de servicios, realizar una revisión en tiempo real de cada petición de cambio y actualizar el registro con la decisión de CAB durante la reunión de éste. Garantizar que se cumplan los indicadores de Cambios pactados en el contrato.

- Ser el gestor de cambios de la mesa de servicios, realizar una revisión constantel de cada petición de cambio y actualizar el registro con la decisión de CAB durante la reunión de éste. Garantizar que se cumplan los indicadores de Cambios pactados en el contrato.
- Generar informe de encuestas de satisfacción, realizar análisis, retroalimentar a los analistas y llamar a los usuarios. Garantizar que se cumplan los indicadores de satisfacción del usuario pactados en el contrato.
- Generar diariamente el reporte de los casos abiertos y realizar retroalimentación a los analistas.
- Realizar gestión con las personas del equipo de trabajo de los casos que llevan más de 5 días abierto.
- Documentar todos los procedimientos realizados generando una base de datos de conocimiento.
- Cumplir con los SLA´s, OLA´s o UC´s que se tienen pactados con el cliente.

Formación profesional:

- Formación profesional en áreas relacionadas con ingeniería de sistemas.
- Deseable en ITIL V3 Foundation.

Experiencia laboral:

- Experiencia profesional mínima de 24 meses.
- Experiencia de trabajo certificada en el área, como mínimo de 24 meses.

3.4 Líder de telecomunicaciones

Responsable del monitoreo y supervisión de los equipos y enlaces de comunicaciones, garantizando la correcta operación y disponibilidad de los servicios.
Definir y mantener los criterios tecnológicos y procedimentales para todas las implementaciones de nuevos equipos y enlaces de comunicaciones, estructurando documentación de la infraestructura a cargo, basados en las mejores prácticas y lineamientos o requerimientos del cliente.
Soportar tecnológicamente la infraestructura, equipos y enlaces provistos para la operación, dando gestión y solución a incidentes y problemas de alta complejidad, dentro de los acuerdos de niveles de servicio pactados.

Establecer planes de trabajo, que garanticen el mejoramiento continuo de los servicios.

Principales responsabilidades:

- Disponibilidad de tiempo completo, cuya sede de trabajo será la del Cliente durante el tiempo la ejecución del contrato en sitio.
- Monitoreo y supervisión permanente de las condiciones de funcionamiento de los equipos y enlaces de comunicaciones.
- Medición de tendencias de tráfico y desempeño de la red para prever escalamiento de anchos de banda, optimización de tiempos de respuesta y demás aspectos técnicos relevantes propios del desempeño de la red WAN con el fin de garantizar los niveles de servicio solicitados.
- Atención, diagnóstico y gestión de la corrección de fallas de nivel 1 y 2 de la red WAN.
- Revisión, análisis y gestión sobre los reportes de alarmas y log de eventos generados por los sistemas de administración de los equipos de la red de datos.

- Generación de reportes y estadísticas del desempeño de los equipos de la red WAN a nivel de alarmas, fallas, niveles de utilización y disponibilidad de los enlaces de telecomunicaciones.
- Realizar gestión y definición de problemas con proveedores de servicio.
- Supervisar el tráfico sobre los enlaces y capacidad de reconocimiento de problemas.
- Generación de informes mensuales de gestión y operación del cliente, informes de disponibilidad de canales, servidores y de appliances incluidos en el contrato.
- Atender y dar respuestas a consultas técnicas del cliente.
- Acompañamiento y soporte a la implementación y operación de IPV6.
- Realizar el rol de interventor o acciones de interventoría cuando estos le sean asignados por el superior inmediato, soportando de manera eficiente y oportuna las administraciones de los acuerdos comerciales asociados.
- Participar en la implementación (cuando se requiera) y en el cumplimiento de las políticas y lineamientos establecidos por la Compañía para su normal funcionamiento y el logro de sus objetivos.
- Garantizar el cumplimiento de buenas prácticas y requisitos legales aplicables de los Sistema de Gestión Integral, orientadas a la mejora continua y la calidad de la operación

- Conocer y aplicar la normatividad asociada a los procesos y procedimientos en los cuales participa y se encuentran definidos por la organización.
- Desempeñar las demás funciones complementarias a su rol, asignadas por el superior inmediato.

Formación profesional:

- Título profesional en Ingeniería de Sistemas, o en Telemática, o en Informática, o en Electrónica, eléctrica o en Telecomunicaciones.
- Certificación CCNA.
- Deseable ITIL v3.

Experiencia laboral:

- Mínimo 2 años de experiencia certificada como Ingeniero de Red (Networking).

3.8 Servicio de gestión de seguridad de protección y filtrado en la Nube

- Apoyo en tareas operativas básicas de plataformas de seguridad. Gestión de incidentes de seguridad de bajo impacto. Recolección de evidencia, generación de reportes iniciales.
- Evaluar los posibles impactos a las aplicaciones ya desplegadas al actualizar la plataforma.
- Solucionar problemas operativos relacionados con la implementación publicación y despliegues.
- Gestionar casos de soporte.
- Asegurar los recursos tecnológicos adecuados para la sostenibilidad y el funcionamiento de las aplicaciones y plataformas.
- Realizar mediciones constantes sobre la gestión de los recursos de la plataformas y plantear estrategias de su optimización.
- Implementar las recomendaciones de seguridad, parchado de las plataformas.
- Realizar monitoreo del estado de las plataformas.
- Realizar las actualizaciones menores y mayores (update y upgrades) de las plataformas.
- Realizar mensualmente el análisis de la capacidad de recursos de la plataforma para la toma de decisiones y hacer recomendaciones.
- Generar y entregar al equipo de TI, un informe mensual con el estado de la plataforma de acuerdo con la ejecución de las actividades descritas en los puntos anteriores.
- Documentar todos los procedimientos realizados, generando una base de datos de conocimiento.

Formación profesional:

- Formación Técnica, Tecnológica o mínimo 6 semestres de formación profesional certificada en áreas relacionadas con la tecnología de información.
- Formación y/o conocimientos en ITIL V3 Foundation.
- Conocimientos en Office 2013 o superior.
- Formación en atención y/o servicio al cliente

Experiencia laboral:
Experiencia en soporte de tecnología mínima de 12 meses.

4. Upgrades Mayores y Migraciones

Para los diferentes ítems de servicios se tendrá en cuenta en este contrato 5 migraciones o upgrades mayores, siempre y cuando no requieran contratar servicios profesionales adicionales y se contemple un plan de trabajo / cronograma acordado entre las partes; los recursos requeridos (licencias/hardware) para estas actividades serán proporcionados por el Distrito de Medellín.

5. PLAN DE ESCALAMIENTO DEL SERVICIO

Confidencialidad

El contratista y el Contratante se obligan a mantener en reserva la información clasificada como confidencial a la que tenga acceso con ocasión de la ejecución del presente contrato, independientemente de que se relacione directa o indirectamente con su objeto, y por lo tanto se obliga a:

- No revelar, divulgar, exhibir, mostrar o comunicar dicha información en cualquier forma o por cualquier medio, a cualquier persona diferente de sus representantes o a aquellas personas que razonablemente deban tener acceso a la misma (Por ejemplo, el equipo de trabajo asignado a la ejecución del Contrato), sin el consentimiento previo y por escrito de la otra parte.
- No utilizar la información para fines distintos a los relacionados con el ejercicio y cumplimiento de sus obligaciones emanadas del presente Contrato, salvo los que la ley dispone.
- En consecuencia, el contratista ejercerá sobre la información confidencial de la Alcaldía de Medellín, el mismo grado de diligencia que utiliza para proteger sus propios bienes intangibles al tenor de lo señalado en los artículos 196 y 200 del Código de Comercio Colombiano.
- Nota 1: El contratista deberá informar de forma expresa qué información tiene el carácter de confidencial para que el Alcaldía de Medellín tenga especial consideración en su tratamiento.
- Nota 2: En todo caso el Alcaldía de Medellín no se encuentra en la obligación de dar tratamiento de información confidencial a aquella en la que la ley expresamente indica lo contrario.

- Las partes manifiestan y aceptan que se entiende y clasifica como "Información Confidencial":

- Toda la información relativa a las actividades, asuntos o propiedades de la Alcaldía de Medellín o de cualquiera de las dependencias que hagan parte de sus entes descentralizados, de la que se hubiere conocido con ocasión de la celebración y ejecución del Contrato y/o dentro de las fases de negociación y/o de ejecución de cualquier proyecto relacionado con el mismo, en forma escrita y/o verbal y/o visual y/o cualquier otro medio conocido o por conocer, es decir, independientemente de la forma en que haya sido recibida.
- Toda la información técnica, financiera, legal, comercial, administrativa o estratégica de la Alcaldía de Medellín que se constituya como reservada al tenor de lo señalado en las normas sobre propiedad intelectual que resulten aplicables, incluyendo pero sin limitarse a los planes de proyectos, inversión y desarrollo, proyecciones financieras, planes de negocio y planes de productos y servicios, relacionada con las operaciones o negocios presentes y futuros de la Alcaldía de Medellín y sus entidades descentralizadas.
- Análisis, compilaciones, estudios u otros documentos o archivos de propiedad de la Alcaldía de Medellín, que se hubieren generado a partir de la información anteriormente mencionada o que la refleje.
- Toda la información sobre la cual previamente el Alcaldía de Medellín hubiere advertido su carácter de confidencial y que se hubiere comunicado a la otra parte durante la fase de ejecución del Contrato.
- El contratista se obliga a mantener en reserva la información relativa a los datos personales de empleados de la Alcaldía de Medellín o de terceros que trabajen para él, listados de direcciones electrónicas de empleados de la Alcaldía de Medellín o de terceros con quienes el Alcaldía de Medellín tenga relaciones comerciales.
- La obligación de confidencialidad que adquiere el contratista aplicará también con respecto de los formatos, direccionamiento, configuraciones, diseños, modelos, esquemas, procedimientos y especificaciones sobre programas de software, modelos de operación, planes de calidad y procesos de negocio de la Alcaldía de Medellín, a los cuales tuviere acceso el contratista.
- La obligación de confidencialidad no otorga al contratista ningún tipo de derecho o autorización en relación con la Información de la Alcaldía de Medellín.

- La información y/o documentos, análisis, diseños y productos de software que se produzcan como resultado de la ejecución del presente Contrato, es de propiedad de la Alcaldía de Medellín, por lo cual su divulgación a terceros o incluso al personal del contratista no vinculado directamente con la ejecución del Contrato, deberá contar con la previa autorización de la Alcaldía de Medellín.

- La obligación de confidencialidad no se aplicará a aquella información que:
- Es de dominio público o está clasificada como pública.
- Fue recibida, después de su elaboración, de una tercera parte que tenía el derecho legítimo a divulgar tal información.
- Ha sido legalmente divulgada por una tercera persona que no tenía obligación de mantener la confidencialidad, o:
- Fue independientemente desarrollada por una tercera persona sin referencia a información confidencial de cualquiera de las Partes.
- Cuando el Alcaldía de Medellín o el Contratista deban hacer entrega de la información clasificada como confidencial, por orden de autoridad administrativa y/o judicial.

- El contratista se obliga a divulgar entre su personal y subcontratistas vinculados para la ejecución del Contrato, la presente Cláusula de Confidencialidad. Sin perjuicio de todo lo indicado en esta Cláusula, el Alcaldía de Medellín, podrá exigir la firma de un Acuerdo de Confidencialidad.
- El contratista se obliga a generar espacios de prevención contra ataques de ingeniería social y cualquier otra técnica que permita a un tercero tener acceso a información de la Alcaldía de Medellín.
- Las obligaciones de confidencialidad aquí señaladas deberán ser cumplidas indefinidamente en el tiempo, independientemente de la vigencia del contrato, de esto se dará fe mediante la firma de un acta de confidencialidad.

6. DERECHOS DE AUTOR Y PROPIEDAD INTELECTUAL

Todos los derechos de autor, propiedad intelectual de desarrollos de software, cambios, renovaciones, actualizaciones, migraciones, documentos y demás aspectos producto de los

servicios prestados por el contratista relacionados con la ejecución y cumplimiento de los servicios especificados para los diferentes grupos, serán propiedad exclusiva y titularidad de los derechos patrimoniales de la Alcaldía de Medellín, y no podrán ser utilizados por el contratista para sus propios fines. La ocurrencia de esta situación dará pie a la cancelación unilateral del contrato, decisión que, de ser tomada, será informada al contratista con tiempo por parte de la Alcaldía de Medellín.
Por lo anterior la empresa contratista deberá transferir o ceder todos los derechos patrimoniales al Alcaldía de Medellín quien será su único propietario.

7. ADMINISTRACIÓN DE GARANTÍAS

Administración de Garantías de acuerdo con los contratos establecidos entre el Alcaldía de Medellín y sus proveedores de hardware y software:
Se debe disponer del recurso humano, físico y procedimental para el trámite de las garantías de acuerdo con los contratos establecidos entre el Alcaldía de Medellín y sus proveedores, cubrimiento y tiempos de garantía y solo se atenderán garantías de activos objeto de este contrato.
Se debe registrar el requerimiento en la herramienta de gestión de incidentes y colocarlo en estado de garantía.
Se debe mantener un registro de los incidentes de garantías y reportarlo en los informes mensuales.
Realizar el seguimiento a los trámites de garantías y a su estricto cumplimiento.

8 ACUERDOS DE NIVELES DE SERVICIO SOPORTE A LA INFRAESTRUCTURA TECNOLÓGICA

La definición de los Acuerdos de Niveles de Servicio o ANS para el soporte a la infraestructura tecnológica se apoya en la criticidad definida para los diferentes servicios y el impacto negativo que su afectación genere sobre la operación normal de la plataforma tecnológica. Adicionalmente se tienen en cuenta los indicadores obtenidos durante el último año por el equipo responsable de la prestación del servicio.

La Administración de la mesa de servicio se realizará por seguimiento al cumplimiento de Acuerdos de Niveles de Servicio (ANS) definidos por el Alcaldía de Medellín para cada uno de los servicios soportados.

En los casos que el Alcaldía de Medellín tenga actualizados sus contratos de soporte y mantenimiento del hardware y software que conforma su plataforma tecnológica, el contratista podrá disponer de las mesas de servicio del fabricante cuando sea necesario.
Para el manejo y administración del servicio, el Alcaldía de Medellín cuenta con una herramienta de gestión de incidentes, la cual a su vez contiene diferentes módulos para la gestión de la Mesa de Servicios, inventarios, indicadores, informes, envío de software, monitores de dispositivos de red. Estas herramientas pueden variar, pero esencialmente son el apoyo a la Mesa de Servicios.

El impacto de los servicios está definido según el siguiente cuadro:

Servicio TI	Descripción Servicio	Impacto del servicio
Herramienta de ServiceDesk	Herramienta de gestión de incidentes, requerimientos, cambios y problemas	Critico
Correo Electrónico Cliente	Permitir el uso del correo electrónico por parte de todos los funcionarios	Critico
Soporte Dispositivos Móviles Corporativos	Permite la conexión de dispositivos móviles a la red de datos corporativa con las medidas de seguridad requeridas que garanticen la integridad de la información	Bajo
Gestión de Garantías	Tramitar las garantías antes los diferentes proveedores velando por el cumplimiento de los ANS definidos por el Alcaldía de Medellín en los procesos contractuales	Alto
Gestión de Software Estándar	Velar porque el software que contienen los equipos de cómputo institucionales cumpla con línea base de seguridad informática de la Alcaldía de Medellín.	Alto
Gestión de Software Específico	Velar porque las instalaciones de software específico correspondan al licenciamiento adquirido o contratado por las diferentes secretarias	Alto
Soporte en Equipos de Usuario Final	Garantiza la óptima operatividad del hardware y software de los equipos de cómputo de usuario final	Alto

Servicio de acceso a Internet	Permite el intercambio de servicios e información digital que son de carácter público. En este orden de ideas permite a los servidores públicos beneficiarse de múltiples servicios y productos que brinda la red pública (Internet). Por otro lado, permite a la Administración Distrital informar a la comunidad el desarrollo del programa de gobierno, beneficios y pagos tributarios.	Critico

Servicio TI	Descripción Servicio	Impacto del servicio
Servicio de Almacenamiento	Proveer los recursos de almacenamiento para alojar la información de la entidad.	Critico
Servicio de Base de Datos	Gestionar bases de datos para mantener la correcta operación de las aplicaciones que apoyan la gestión de los usuarios.	Critico
Servicio de disponibilidad de las plataformas	Permitir el acceso controlado a las herramientas para la gestión de la información de la entidad.	Critico
Servicio de Telefonía IP	Proporcionar la comunicación entre las diferentes sedes de la Alcaldía de Medellín (sede administrativa CAD y dependencias externas), mediante la integración e intercambio de voz, datos y video. Algunas de los servicios específicos proporcionados son: Telefonía Ip, buzón de voz. Sistema de Mensajería. Tarificación de llamadas. Programación y Envío de campañas masivas de correo y mensajes de voz Call Center. Conferencia.	Critico

Servicio de conectividad	Proporcionar la interconexión de las sedes externas de la Alcaldía de Medellín con el CAM, permitiendo que las diferentes sedes accedan a la red de datos con todos sus servicios.	Critico
Servicio de Red de Datos	Proporcionar la comunicación entre los usuarios mediante la red de datos corporativa, permitiendo el acceso a las diferentes aplicaciones de la entidad como: correo, impresión, Internet, sistemas de información, intranet.	Critico
Servicio de Backup	Respaldo y restauración de la información corporativa.	Critico
Servicio de aplicaciones	Cualquier aplicación de la Alcaldía de Medellín que genera una indisponibilidad o inconsistencias y requiera del apoyo del área de infraestructura y seguridad deberá tener un tratamiento crítico.	Crítico
Servicio de Gestión de Incidentes de Seguridad Informática	Servicio dirigido a la atención de los eventos de seguridad, que atenten contra la imagen corporativa o la seguridad de la información institucional.	Critico
Servicio de Servidores	Proporcionar los servidores para alojar aplicaciones, bases de datos e información corporativa que demandan los diferentes proyectos de la entidad.	Crítico

Así mismo la urgencia que la afectación de los servicios genere sobre la plataforma tecnología se define como:

Urgencia	Descripción

Critico	Eventos que afecten la prestación de servicios a la ciudadanía. Afectación del canal de Internet por eventos en dispositivos de la línea base administrada. Eventos que genere falla en la prestación de un servicio de TI crítico, definiendo estos como: SAP, correo, Internet, seguridad de la información, Website y telefonía, servicios y aplicaciones. Evento que afecte la prestación de algún servicio TI a usuarios del despacho del Alcalde. Eventos o incidentes que pongan en riesgo la plataforma tecnológica de la Alcaldía de Medellín y la información de esta.
Critico	Evento que afecte la prestación de servicio TI a Puntos de atención a los usuarios internos (empleados de la Alcaldía de Medellín) Evento que afecte la prestación de algún servicio TI a usuarios VIP. Falla que afecte el servicio TI en aulas de capacitación, cuando se dicta una capacitación que afecte el tiempo comprometido por los usuarios Evento TI que impida el desarrollo total de las labores de un funcionario de la Alcaldía de Medellín.
Alto	Instalación o Reparación de Software no crítico que soporte las labores del funcionario Instalación de Hardware suministrado por usuario y que soporte las labores del funcionario. Evento TI que impida el desarrollo parcial de las labores de un funcionario de la Alcaldía de Medellín.
Medio	Instalación o reparación de software no crítico que no soporte las labores del usuario Instalación o reparación de hardware siempre y cuando se cuente con la parte a instalar. Solicitud de traslado de equipos, siempre y cuando el número de equipos sea inferior a 15.
Actividades Negociadas	Actividades especiales Actividades que por su complejidad superen los tiempos de solución anteriormente establecidos.

La clasificación de ANS se determina según el impacto del servicio y urgencia que dicha afectación genere sobre la operatividad de la plataforma tecnológica al interior de la entidad, plasmada en la siguiente matriz:

Los tiempos de respuesta y solución máximos para los diferentes servicios están consignados para cada ANS en los siguientes cuadros, tanto para incidentes como requerimientos:

ANS exigidos para la Gestión Incidentes por Servicio

	Baja		Medio		Alto		Máximo	
Servicio TI	Atención (minutos)	Solución (minutos)	Atención (minutos)	Solución (minutos)	Atención (minutos)	Solución (minutos)	Atención (minutos)	Solución (minutos)
Herramienta de ServiceDesk	20	520	20	160	5	120	5	70
Correo Electrónico Cliente	20	520	20	160	5	120	5	40
Soporte Dispositivos Móviles Corporativos	20	280	20	160	5	120	5	40
Gestión de Garantías	20	160	20	100	5	80	5	40
Gestión de Software Estándar	20	160	20	100	5	80	5	40
Gestión de Software Específico	20	340	20	160	5	100	5	70
Soporte en Equipos de Usuario Final	20	520	20	160	5	100	5	40
Servicio de acceso a Internet	20	520	20	160	5	100	5	40
Servicio de Almacenamiento *	20	160	20	100	5	80	5	40
Servicio de Base de Datos	20	160	20	100	5	80	5	40

Servicio de Transferencia segura de archivos	20	160	20	100	5	80	5	40
Servicio de Telefonía IP	20	160	20	100	5	80	5	40
Servicio de conectividad	20	160	20	100	5	80	5	40
Servicio de Red de Datos	20	160	20	100	5	80	5	40
Servicio de Backup	20	160	20	100	5	80	5	40
Servicio de aplicaciones **	20	160	20	100	5	80	5	40
Servicio de Gestión de Incidentes de Seguridad Informática	20	160	20	100	5	80	5	40
Servicio de Servidores ***	20	160	20	100	5	80	5	40

ANS Exigidos para la atención de Requerimientos por Servicio:

	Baja		Medio		Alto		Critico	
Servicio TI	Atención (minutos)	Solución (minutos)	Atención (minutos)	Solución (minutos)	Atención (minutos)	Solución (minutos)	Atención (minutos)	Solución (minutos)
Herramienta de ServiceDesk	30	1590	30	1050	20	780	20	510
Correo Electrónico Cliente	30	1590	30	1050	20	780	20	510
Soporte Dispositivos	30	1050	30	780	20	510	20	240
Gestión de	30	1050	30	780	30	510	30	240

Garantías								
Gestión de Software Estándar	30	1590	30	1050	30	780	30	510
Gestión de Software Específico	30	1590	30	1050	30	780	30	510
Soporte en Equipos de Usuario Final	30	1590	30	1050	30	780	30	510
Servicio de acceso a Internet	30	1590	30	1050	30	780	30	510
Servicio de Almacenamiento *	30	1590	30	1050	30	780	30	510
Servicio de Base de Datos	30	1590	30	1050	30	780	30	510
Servicio de Transferencia Segura de Archivos	30	1590	30	1050	30	780	30	510
Servicio de Telefonía IP	30	1590	30	1050	30	780	30	510
Servicio de conectividad	30	1590	30	1050	30	780	30	510
Servicio de Red de Datos	30	1590	30	1050	30	780	30	510
Servicio de	30	1590	30	1050	30	780	30	510

Backup								
Servicio de aplicaciones **	30	1590	30	1050	30	780	30	510
Servicio de Gestión de Incidentes de Seguridad Informática	30	1590	30	1050	30	780	30	510
Servicio de Servidores ***	30	1590	30	1050	30	780	30	510

Niveles de Soporte:

Nivel	Descripción
Primer nivel	Soporte brindado por el personal de la Mesa de Servicios de manera remota o en sitio en las diferentes instalaciones de la Alcaldía de Medellín. Si este nivel de la organización de servicio no puede resolver el incidente se debe escalar a los especialistas de soporte de Segundo Nivel.
Segundo nivel	Soporte brindado por el personal especialista de Outsourcing Tecnológico. Se debe observar con especial cuidado el cumplimiento de las políticas de TI de la Alcaldía.
Tercer nivel	Soporte solicitado a personal especializado en áreas específicas atendiendo solicitudes en virtud de los contratos de soporte y actualización previamente existentes.

Prioridades de los incidentes o requerimientos de servicio:

La identificación de los puntos de atención al ciudadano se hará mediante la información suministrada por el usuario que está reportando el evento.

La atención con prioridad Alta para usuarios VIP se realizará una vez se elabore un acta inicial que contenga la lista de los usuarios seleccionados por el Alcaldía de Medellín (Alcalde, primera dama, Secretarios, Subsecretarios, Directores, Subdirectores de despacho y asesores del despacho del alcalde.

De igual manera, para la atención de requerimientos e incidentes en las sedes externas, los tiempos de atención para el soporte, cuentan con una hora adicional de transporte, a partir del momento del registro en la herramienta de gestión.

Para los temas de Seguridad Informática, aplican los Acuerdos de Niveles de Servicio clasificados en prioridad máxima, según el Cuadro Prioridades de los incidentes.

Atención de la Mesa de Servicio:

La atención de la Mesa de Servicio en lo referente a las llamadas será evaluada de acuerdo con la siguiente tabla ANS.

Variable Evaluada	Criterio De Aceptación	Medición Del Criterio
Llamadas abandonadas	Porcentaje mensual de llamadas abandonadas inferior al 10%.	Reporte de ACD
Llamadas contestadas	El 90% de las llamadas deben ser contestadas antes de 20 segundos.	Reporte de ACD

Llamadas abandonadas:
Mide el porcentaje de llamadas a la Mesa de Servicios que son abandonadas luego de una espera mayor o igual a 10 segundos. Indicador que será válido a partir del momento en que el Distrito cuente con las herramientas de medida.

Fuente y medición
T: Número total de llamadas telefónicas realizadas a la Mesa de Servicios.
R: Número total de llamadas cuya espera fue mayor a 10 segundos y que fueron abandonadas.
X: Porcentaje mensual de llamadas abandonadas.

Criterio de aceptación
Porcentaje mensual de llamadas abandonadas inferior al 10%
X = R/T expresado en porcentaje

Tiempo de respuesta de llamadas:
Mide el porcentaje de llamadas a la Mesa de Servicios que son respondidas en un tiempo menor o igual a 20 segundos.

Criterio de aceptación:
Porcentaje mensual de llamadas respondidas en el tiempo especificado del 90%.

Fuente y medición
Reporte de ACD

T: Número total de llamadas telefónicas realizadas a la Mesa de Servicios.
R: Número total de llamadas respondidas en el tiempo definido.
TR: Tasa de respuesta

TR = (R/T) * 100

$$TR = (R/T) * 100 TR = (R/T) * 100$$

Otros Niveles de Servicio:

El presente Acuerdo de Niveles de Servicio no se cumplirá:

- *Ante eventos críticos por parte del cliente, donde se note un crecimiento inesperado de incidentes generados en la Mesa de Servicios, tales como: desastre natural, motín o guerra, o ante problemas causados por accidentes, causas de fuerza mayor y catástrofes naturales.*

- *En el momento en que el Alcaldía de Medellín no suministre información necesaria que llevan al no cumplimiento de los ANS.*

- *El contratista no se hará responsable por errores en el escalamiento, cuando el Alcaldía de Medellín realice cambios a la matriz y éstos no sean informados oportunamente. El contratista deberá informar oportunamente al Alcaldía de Medellín de algún impedimento que impida el cumplimiento de los ANS.*

9 INFORMES E INDICADORES

9.1 Informes

Los cinco (5) primeros días hábiles de cada mes, el contratista presentará al supervisor del contrato y a la supervisión designada por el Alcaldía de Medellín y/o al Alcaldía de Medellín, un reporte de operación de la Mesa de Servicios. Tal informe debe reflejar el comportamiento de la operación durante el mes anterior.

La estructura de los informes será pactada durante el primer mes, entre el gerente de proyecto, el interventor del contrato y la supervisión del contrato designada por el Alcaldía de Medellín.

Mensualmente el contratista deberá presentar, además, los siguientes informes:

- Indicadores de gestión de los niveles de servicio. El contratista debe asegurar que existan archivos confiables en caso de requerirse una consulta al detalle de un servicio en particular.

- Registro de consulta detallado de las estadísticas, que incluya servicios solicitados, servicios atendidos, servicios pendientes, tiempo promedio de atención y aquellos que sean requeridos por el Alcaldía de Medellín, de tal manera que permitan una consulta inmediata y real de cualquiera de los servicios.

- Análisis de datos de la encuesta para medir el grado de satisfacción de los usuarios. Cuáles son los puntos críticos del servicio y cuáles son los puntos a destacar.

- Informe detallado de los incidentes, requerimientos y problemas recurrentes, las acciones correctivas tomadas y la evolución de las mismas.

- Informe de las estadísticas generadas por los servidores y demás dispositivos, para los eventos no programados que afecten el servicio y presentar acciones tendientes a la mejora del servicio.

- Informe de consumo de hardware (cpu, memoria, etc), para proyectar la expansión del hardware.

- Informe sobre inventarios de software y hardware actualizado.

- Los demás que sean definidos por el Alcaldía de Medellín, acorde con las necesidades y las herramientas que se empleen para la ejecución de este servicio.

Los reportes entregados estarán determinados por los indicadores establecidos.

9.2 Indicadores

Indicadores definidos a nivel del contrato para el grupo de Mesa de Servicio:

Nombre	Descripción	Medición esperada (Mensual)	Observación

% Casos sin resolver	Seguimiento periódico al porcentaje calculado como: casos que se encuentran en estado abierto en el mes dividido por el número de casos creados en el mes *100	Máximo el 3% calculado .	Para el cálculo del indicador se tendrán en cuenta los casos no cerrados y con las siguientes exclusiones: ● Se excluirá los casos registrados en los últimos tres días hábiles del mes evaluado ● Se excluirá los casos cuyo estado "Suspendido" con las razones: "Espera por Usuario", "Asignado a proveedor", "Asignado a TI Municipio" o "Actualizar Inventario". Se utilizará la siguiente formula: ((Casos abiertos/Casos registrados)

Nombre	Descripción	Medición esperada (Mensual)	Observación
Porcentaje de casos atendidos en sitio	Seguimiento de casos atendidos en sitio, calculado como (el total de casos atendidos en sitio / el total de casos registrados) *100	Máximo el 30%	Para el cálculo del indicador se tendrán en cuenta los siguientes criterios: ●Incluir todos los grupos del proyecto GESTIÓN TECNOLOGICA. Se excluirá los casos de actividades especiales que no estén dentro del desarrollo normal de la operación. (instalaciones o traslados masivos de equipos.) Se tendrán en cuenta solo los casos gestionados y cerrados cuya razón de cambio sea "Solucionado en sitio". Se utilizará la siguiente formula: (Casos atendidos en sitio / casos registrados) *100

Cumplimiento ANS	Seguimiento de los casos que cumplen el ANS en la mesa de Servicios (este indicador será utilizado para la aplicación de penalizaciones) calculado como Total de casos que cumplen ANS/total de casos solucionados	Mayor al 98%	Para el cálculo del indicador se tendrán en cuenta los siguientes criterios: ● Se tendrá en cuenta los casos gestionados y cerrados durante el mes evaluado Se utilizará la siguiente formula: ((Casos gestionados + cerrados en el mes que cumplen ANS) / (total de casos gestionados + cerrados en el mes))*100
Efectividad en la solución de incidentes	Seguimiento de la efectividad del cierre de los incidentes de la mesa de servicios, calculado como: total de incidentes solucionados / total de incidentes registrados	Mayor al 95%	Para encontrar el valor de dicho indicador se tendrá en cuenta los siguientes criterios: ● Los incidentes gestionados cerrados por todos los grupos del proyecto Se utilizará la siguiente formula: (Total de incidentes gestionados o cerrados /Total de incidentes registrados)

Nombre	Descripción	Medición esperada (Mensual)	Observación

Efectividad en la solución de requerimientos	Seguimiento de la efectividad del cierre de los requerimientos de la mesa de servicios, calculado como: Total de requerimientos solucionados / total de requerimientos registrados	Mayor al 80%	Para encontrar el valor de dicho indicador se tendrá en cuenta los siguientes criterios: ● Los requerimientos gestionados y cerrados por todos los grupos del proyecto. Se utilizará la siguiente formula: Total de requerimientos gestionados o cerrados / (total de requerimientos registrados) *100
Efectividad en la Gestión de cambios	Seguimiento a la efectividad en la gestión de cambios propuestos por la mesa de servicios, calculado como: total de cambios exitosos / total de cambios aprobados *100 durante el periodo	Mayor al 90%	Todos los casos gestionados deben ser documentados en un plazo máximo de 5 días hábiles después de la ejecución del cambio. Los casos no documentados se tomarán como no exitosos.

Calidad de la Mesa de Servicios	Seguimiento periódico para conocer la gestión de casos con inconformidad por parte del usuario. Calculados como: (# casos calificados como Regular o Malo) / (# de casos evaluados	Menor al 5%	Para encontrar el valor de dicho indicador se tendrá en cuenta los siguientes criterios: Para el total de casos cerrados, se deberán tener en cuenta los cerrados del mes evaluado, más los casos cerrados de meses anteriores; dado que la encuesta se activa al cerrar el caso. Se tomará el número de casos calificados como regular o malo en la pregunta 3 "Evalúe su nivel de satisfacción a la atención de su caso." Se utilizará la siguiente formula: (Total de casos calificados como regular o malo / (total de casos evaluados durante el mes)
Nombre	Descripción	Medición esperada (Mensual)	Observación
	durante el periodo) *100		

Mensualmente se genera el reporte de casos que utilizan el estado suspendido o cancelado y las razones de cambio asociados; para todos ellos se realiza una revisión detallada y aquellos casos en los cuales se determine mal manejo del estado o mala documentación se tendrán en cuenta para la afectación de los diferentes indicadores del periodo (casos sin resolver, incumplimiento de ANS, Efectividad en la solución de Incidentes y Efectividad en la solución de Requerimientos).

NOTA: Estos indicadores serán exigidos en condiciones normales de operación, en casos excepcionales se negociará con el proveedor.

10 CLAUSULAS DE INCUMPLIMIENTO

Las cláusulas de incumplimiento están fundamentadas en los indicadores. En el siguiente cuadro se detalla cada uno de los indicadores con su respectivo descuento a la factura mensual. El descuento se calcula con relación al valor mensual de la factura.

Ítem	Nombre	Métrica	Medición esperada (Mensual)	Penalización		
				<=	>	Descuento
1	Elementos de telecomunicaciones	Está descrita en el ítem DISPONIBILIDAD DE LAS PLATAFORMAS	99,8	100,0%	99,8%	0
				99,7%	99,4%	2%
				99,3%	99,1%	5%
				99,0%	98,0%	10%
				97,0%	0,0%	100%
2	Telefonía IP	Está descrita en el ítem DISPONIBILIDAD DE LAS PLATAFORMAS	99,8	100,0%	99,8%	0
				99,7%	99,4%	2%
				99,3%	99,1%	5%
				99,0%	98,0%	10%

Ítem	Nombre	Métrica	Medición esperada (Mensual)	Penalización		
				<=	>	Descuento
				97,0%	0,0%	100%
3	Elementos de seguridad	Está descrita en el ítem	99,6	100,0%	99,6%	0
				99,5%	99,4%	2%

		DISPONIBILIDAD DE LAS PLATAFORMAS		99,3%	99,1%	5%
				99,0%	98,0%	10%
				97,0%	0,0%	100%
4	Plataforma de servidores	Está descrita en el ítem DISPONIBILIDAD DE LAS PLATAFORMAS	99,6	100,0%	99,6%	0
				99,5%	99,4%	2%
				99,3%	99,1%	5%
				99,0%	98,0%	10%
				97,0%	0,0%	100%
5	Servicio de correo	Está descrita en el ítem DISPONIBILIDAD DE LAS PLATAFORMAS	99,8	100,0%	99,8%	0
				99,7%	99,4%	2%
				99,3%	99,1%	5%
				99,0%	98,0%	10%
				97,0%	0,0%	100%
6	Servicio de internet	Está descrita en el ítem DISPONIBILIDAD DE LAS PLATAFORMAS	99.8	100,0%	99,8%	0
				99,7%	99,4%	2%
				99,3%	99,1%	5%
				99,0%	98,0%	10%
				97,0%	0,0%	100%
7	Servicio de portales	Está descrita en el ítem DISPONIBILIDAD	99.8	100,0%	99,8%	0
				99,7%	99,4%	2%
				99,3%	99,1%	5%

Ítem	Nombre	Métrica	Medición esperada (Mensual)	Penalización		
				<=	>	Descuento
		DE LAS PLATAFORMAS		99,0%	98,0%	10%
				97,0%	0,0%	100%
8	Servicio de intranet		99.8	100,0%	99,8%	0
				99,7%	99,4%	2%
				99,3%	99,1%	5%
				99,0%	98,0%	10%
				97,0%	0,0%	100%
9	% Casos sin resolver	Seguimiento periódico al porcentaje calculado como: casos que se encuentran en estado abierto en el mes dividido por el número de casos creados en el mes *100	Máximo el 3% calculado	3%	0%	0
				5%	3.1%	2%
				10%	5.1%	5%
				20%	10.1%	10%
				100%	20.1%	100%
10	Porcentaje de casos atendidos en sitio	Seguimiento de casos atendidos en sitio, calculado como (el total de casos atendidos	Máximo el 30%	30%	0%	0
				50%	30.1%	2%
				60%	50.1%	5%

		en sitio / el total de casos registrados)*100		70%	60.1%	10%
				100%	70.1%	100%
11	Cumplimiento ANS	Seguimiento de los casos que cumplen el ANS en la mesa de Servicios (este indicador será utilizado para la	Mayor al 98%	100%	98%	0%
				97%	95%	2%
				94%	90%	5%
				89%	85%	10%

Ítem	Nombre	Métrica	Medición esperada (Mensual)	Penalización		
				<=	>	Descuento
		aplicación de penalizaciones) calculado como Total de casos que cumplen ANS/total de casos solucionados		84%	0%	100%
12	Efectividad en la solución de incidentes	Seguimiento de la efectividad del cierre de los incidentes de la mesa de servicios, calculado como:	Mayor al 95%	100%	95%	0%
				94%	91%	2%
				90%	89%	5%
				88%	80%	10%

		total de incidentes solucionados / total de incidentes registrados		79%	0%	100%
13	Efectividad en la solución de requerimientos	Seguimiento de la efectividad del cierre de los requerimientos de la mesa de servicios, calculado como: Total de requerimientos solucionados / total de requerimientos registrados	Mayor al 80%	100%	80%	0%
				79%	75%	2%
				74%	69%	5%
				68%	63%	10%
				62%	0%	100%
14	Efectividad en la Gestión de cambios	Seguimiento a la efectividad en la gestión de cambios propuestos por la mesa de servicios, calculado como: total de cambios exitosos / total de	Mayor al 90%	100%	90%	0%
				89%	85%	2%
				84%	80%	5%
				79%	73%	10%
				72%	0%	100%
Ítem	Nombre	Métrica	Medición esperada (Mensual)	Penalización		
				<=	>	Descuento
		cambios aprobados *100 durante el periodo				
15				5%	0%	0%

	Calidad de la Mesa de Servicios	Seguimiento periódico para conocer la gestión de casos con inconformidad por parte del usuario. Calculados como: (# casos calificados como Regular o Malo) / (# de casos evaluados durante el periodo) *100	Menor al 5%	9%	6%	2%
				12%	10%	5%
				16%	13%	10%
				100%	17%	100%

11 CORRESPONSABILIDAD DEL CONTRATISTA EN EL MARCO DEL CONTRATO DE PRESTACIÓN DEL SERVICIO CON LA SEGUIRIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ENTIDAD

Coherente con las necesidades institucionales relacionadas con la prestación de servicios de administración, gestión, soporte, mantenimiento y operación de servicios y soluciones de tecnologías de información y de las comunicaciones de la Alcaldía de Medellín y en atención a lo dispuesto en el artículo 3 de la Ley 80 de 1993 que precisa: “Los servidores públicos tendrán en consideración que al celebrar contratos y con la ejecución de los mismos, las entidades buscan el cumplimiento de los fines estatales, la continua y eficiente prestación de los servicios públicos y la efectividad de los derechos e intereses de los administrados que colaboran con ellas en la consecución de dichos fines.

Los particulares, por su parte, tendrán en cuenta al celebrar y ejecutar contratos con las entidades estatales que, colaboran con ellas en el logro de sus fines y cumplen una función social que, como tal, implica obligaciones.” Y coherente con los principios de la Contratación Pública, en particular lo dispuesto en el numeral 1 del artículo 26 de la Ley 80 de 1993 relacionado con el principio de Responsabilidad que precisa “Los servidores públicos están obligados a buscar el cumplimiento de los fines de la contratación, a vigilar la correcta ejecución del objeto contratado y a proteger los derechos de la entidad, del contratista y de los terceros que puedan verse afectados por la

ejecución del contrato.", y en atención a los dispuesto por el Ministerio de Tecnologías de Información y Comunicaciones en materia normativa:
A través de la Resolución 0500 de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" y en particular lo precisado en:
Artículo 3. Lineamientos Generales. Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución.
Para todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura critica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital.

Así mismo, lo dispuesto en el numeral 2 del artículo 5, referido a "Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.", así como lo precisado en el numeral 5 del mismo artículo concerniente a: "La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.".
De igual manera, lo dispuesto en el numeral 1 del artículo 6 referido a: "Definir controles considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de usuarios, evaluación del riesgo y servicios prestados por la entidad.".
Así mismo, lo dispuesto en el artículo 7 referente a las operaciones seguras, "Los sujetos obligados deben implementar mecanismos de gestión y monitoreo que protejan la infraestructura de TI de amenazas físicas y digitales.".
También lo precisado en el numeral 1 del artículo 9 referido a: "Gestionar los incidentes de seguridad digital, según el procedimiento establecido por MinTIC, para lo cual deben crear una bitácora que contenga la descripción de cada una de las actividades desarrolladas en la gestión de estos".
Así mismo lo previsto en el artículo 11 referido a: Los sujetos obligados deben emplear mecanismos para la autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información. Para ello, deben seguir el modelo de servicios ciudadanos digitales en particular el modelo de autenticación digital.
Principalmente lo previsto en el artículo 14 relacionado con Terceros, Colaboradores y Seguridad Digital referido a: "Los sujetos obligados deben incluir en su estrategia de seguridad digital y su plan de Seguridad y privacidad de la información las medidas y obligaciones pertinentes para la

adopción y el cumplimiento de políticas y controles para la gestión de los riesgos de seguridad y privacidad de la información por parte de terceros y colaboradores."
De igual manera, lo dispuesto en el artículo 15, referido a: "Los sujetos obligados deben establecer los mecanismos de control al interior de la entidad que permitan verificar el cumplimiento de las disposiciones establecidas en la política de seguridad de la información que hayan aprobado internamente, realizando auditorias de seguridad de la información al menos una vez al año, que contemplen aspectos técnicos de la seguridad digital como análisis de vulnerabilidades a sistemas de información críticos, entre otros.
Así mismo lo dispuesto en los numerales 1.1. y 1.2. del numeral 1. Del articulo 17 referido a: "Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales), protección de infraestructura y gestión de identidades, privacidad y protección de la información."
Y "Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información" respectivamente.

De igual manera, lo dispuesto en la resolución 0746 de 2022 que en su artículo 3 adiciona el numeral 6.1 a la resolución 0500 de 2021, que precisa:
Los sujetos obligados deben determinar e implementar los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital señalados en el Anexo número 2 de la presente resolución, así como cumplir con los siguientes requerimientos y características.

1. Definir claramente los roles y responsabilidades de seguridad de la información con respecto a la relación con el proveedor.
2. Propender por mantener una arquitectura de seguridad al adquirir productos o servicios de Seguridad Digital
3. Analizar los riesgos de Seguridad Digital propios de la integración de soluciones e implementar controles para su mitigación.
4. Implementar controles que permitan minimizar los riesgos asociados a la transferencia de datos generada por cambios de fabricante o proveedor.
5. Identificar la vida útil de los productos y servicios adquiridos con el fin de planificar cualquier migración o transferencia y respaldar los datos para garantizar la continuidad de la operación.
6. Optimizar la gestión de los riesgos de Seguridad Digital estableciendo estrategias soportadas en servicios de nube.

Finalmente, partiendo de que la relación entre la Entidad y el Contratista en relación con los servicios incluidos en el contrato de mesa de servicio se basa en la prestación de unos servicios de administración, gestión, soporte, mantenimiento y operación de servicios y soluciones de tecnologías de información y de las comunicaciones de la Alcaldía de Medellín, que representan activos de información clasificados según la norma ISO 27005 como de Soporte y clasificados como tipos de información por el artículo 2.8.2.5.2 del Decreto 1080 de 2015, así como el personal que realizará las acciones sobre estos activos, se requiere que el contratista pueda adoptar desde su

corresponsabilidad en la prestación de servicios de tecnologías de información y de las comunicaciones, las orientaciones que se suministren para la gestión de los activos de información a su cargo y la gestión de los riesgos de seguridad y privacidad de la información que sean de su responsabilidad sobre dichos activos de información, así como la gestión de los controles identificados e implementados de acuerdo con su corresponsabilidad en la prestación de los servicios de tecnologías de información y de las comunicaciones. De igual manera, las responsabilidades asociadas al tratamiento de incidentes de seguridad y privacidad de la información que puedan ser de su alcance, así como contribuyendo al fortalecimiento de la apropiación de la seguridad y privacidad de la información del personal involucrado en la prestación de servicios, en la gestión de vulnerabilidades técnicas y en la efectividad de los controles de su responsabilidad.

Es importante destacar, que las medidas de corresponsabilidad recaen sobre todo el personal que participe en la prestación de los servicios ofertados y aplica sobre las responsabilidades asociadas a cada uno de los servicios, plataformas, aplicaciones o infraestructura tecnológica a su cargo y que no tienen que ver de manera explícita con las responsabilidades que desempeña el grupo de seguridad informática que apoya las actividades de operación de la unidad de seguridad informática frente a ciberamenazas, por lo cual es importante que se incluya como parte integral del contrato las siguientes obligaciones:

1. Acatar e implementar en sus procesos, con la orientación de la Entidad, la ejecución de acciones orientadas a aportar a la identificación, clasificación y valoración de activos de información, sobre los cuales ustedes desempeñan labores de administración, gestión, soporte, mantenimiento y operación.
2. Acatar e implementar con la orientación de la Entidad, la ejecución de acciones orientadas a aportar a la identificación, análisis y valoración de riesgos de seguridad y privacidad de la información sobre los activos de información, sobre los cuales ustedes desempeñan labores de administración, gestión, soporte, mantenimiento y operación.
3. Acatar e implementar con la orientación de la Entidad, la ejecución de acciones orientadas a aportar a la identificación, implementación, seguimiento y evaluación de acciones de tratamiento, que puedan aportar a mitigar los riesgos de seguridad y privacidad de la información implementados, sobre los activos de información de los cuales ustedes desempeñan labores de administración, gestión, soporte, mantenimiento y operación.
4. Acatar e implementar con la orientación de la Entidad, la ejecución de acciones orientadas a aportar a la notificación y tratamiento de incidentes de seguridad y privacidad de la información, que puedan ser identificados sobre los activos de información de los cuales ustedes desempeñan labores de administración, gestión, soporte, mantenimiento y operación.
5. Acatar e implementar con la orientación de la Entidad, la ejecución de acciones orientadas a aportar a la apropiación de la seguridad y privacidad de la información por parte de todo el personal involucrado en la prestación de los servicios a su cargo.
6. Acatar e implementar con la orientación de la Entidad, la ejecución de acciones orientadas a aportar a la identificación y remediación de vulnerabilidades técnicas sobre los activos de

información, sobre los cuales ustedes desempeñan labores de administración, gestión, soporte, mantenimiento y operación.
7. Acatar e implementar con la orientación de la Entidad, la ejecución de acciones orientadas a aportar a la efectividad de los controles implementados, para mitigar riesgos de seguridad y privacidad de la información sobre los activos de información, sobre los cuales ustedes desempeñan labores de administración, gestión, soporte, mantenimiento y operación.
8. Elaborar y presentar durante los primeros 15 días posteriores al acta de inicio los planes de seguridad y privacidad de la información y de tratamiento de riesgos de seguridad y privacidad de la información sobre los activos de información (personas, servicios o tecnologías de información) bajo su responsabilidad en atención a las actividades de administración, gestión, soporte, mantenimiento y operación contratadas.
9. El plan de seguridad y privacidad de la información debe incluir:
las actividades relacionadas con la identificación, clasificación y valoración de activos de información (personas, servicios o tecnologías de información) bajo su responsabilidad en atención a las actividades de administración, gestión, soporte, mantenimiento y operación contratadas.
Los riesgos de seguridad y privacidades de la información identificadas, analizadas y valores al alcance de su responsabilidad y sobre los activos de información (personas, servicios o tecnologías de información) bajo su responsabilidad.
Las acciones de tratamiento que se derivan del análisis y valoración de riesgos.
Las acciones para articular la atención de eventos e incidentes de seguridad de la información sobre los activos de información (personas, servicios o tecnologías de información) bajo su responsabilidad en atención a las actividades de administración, gestión, soporte, mantenimiento y operación contratadas, en estricta coherencia con los riesgos de su responsabilidad identificados.
Las acciones para fortalecer la cultura de seguridad y privacidad de la información de todo el personal involucrado en la prestación de servicios, así como el fortalecimiento de las acciones legales relacionadas con el control en la contratación y retiro del personal vinculado al proyecto y la aplicación de cláusulas de confidencialidad de acuerdo con el rol asignado en la operación; así como la inclusión de actividades orientadas a dar cumplimiento a prácticas de seguridad establecidas para los diferentes roles, que incluyan la seguridad y privacidad de la información en relación con el quehacer de los diferentes roles vinculados (administración, gestión, soporte, mantenimiento y operación) que aporten a que la prestación de servicios incluya la seguridad y privacidad en todos las fases que hacen parte de la responsabilidad contractual.
Las acciones para verificar la efectividad de los controles dispuestos en atención a los riesgos identificados y establecer las acciones de mejora que sean requeridas para fortalecer las prácticas de seguridad y privacidad de la información en la prestación del servicio contratado.

9. Elaborar y presentar informes mensuales de avance y seguimiento en la ejecución de actividades relacionadas con el cumplimiento de los planes presentados.

Para lo cual es importante que se pueda tener como entregable durante los primeros 15 días del inicio del contrato los planes de:

Plan de Seguridad y privacidad del Contratista sobre los activos de información (personas, servicios o tecnologías de información) bajo su responsabilidad en atención a las actividades de administración, gestión, soporte, mantenimiento y operación contratadas.
Plan de Tratamiento de Riesgos de Seguridad y privacidad sobre los activos de información (personas, servicios o tecnologías de información) bajo su responsabilidad en atención a las actividades de administración, gestión, soporte, mantenimiento y operación contratadas.

Y durante la ejecución del contrato:
Informes mensuales de seguimiento y avance en el cumplimiento de los planes de seguridad y privacidad de la información y de los planes de tratamiento de riesgos de seguridad y privacidad de la información.

Además, es importante precisar que el alcance más relevante en primera medida sobre la identificación de riesgos tiene que ver con:

Acciones Intencionadas ejecutadas por personal involucrado como parte del equipo de administración, gestión, soporte, mantenimiento y operación de los servicios y tecnologías de información que puedan afectar la disponibilidad, confidencialidad e integridad de los activos de información (personas, servicios o tecnologías de información) bajo la responsabilidad del contratista.

Errores no intencionados que se derivan de la ejecución de actividades del personal involucrado como parte del equipo de administración, gestión, soporte, mantenimiento y operación de los servicios y tecnologías de información que puedan afectar la disponibilidad, confidencialidad e integridad de los activos de información (personas, servicios o tecnologías de información) bajo la responsabilidad del contratista.

Debilidades administrativas que ocasiones que personal de la organización, un hacker o personal del equipo contratista o por una falla generalizada no atendida de manera oportuna que pueda afectar disponibilidad, confidencialidad e integridad de los activos de información (personas, servicios o tecnologías de información) bajo la responsabilidad del contratista en atención a sus actividades de administración, gestión, soporte, mantenimiento y operación, debido a una inadecuada gestión de los usuarios, gestión de los accesos, gestión de los eventos, gestión de los cambios, gestión de los incidentes, gestión de las configuraciones, gestión de los logs, gestión de la capacidad, entre otros, por una inadecuada aplicación de los controles propuesto en el Anexo A de la NTC ISO 27001.

12 TRANSICIÓN

Se deben contemplar una transición, la cual tiene como objetivo el empalme entre el contratista que se encuentra actualmente prestando el servicio y el proveedor ganador que resulte dentro de algún proceso de selección, y cuyo objetivo será el empalme entre el contratista que en ese momento estuviere prestando el servicio y aquél que vaya a asumir la prestación del servicio con posterioridad, sin exceder 17 días calendario.

12.1 Transición del contrato

a) Durante la transición el proveedor al que se adjudique el presente proceso deberá garantizar la continuidad de la operación.

b) La duración de la transición no podrá ser superior a 17 días Calendario.

c) Durante la transición se realizará la prestación del servicio a manera de "Operación controlada" buscando ajustar (si es necesario) el diseño de los procesos, el personal asignado y los demás elementos para que se puedan garantizar los ANS e indicadores comprometidos. En esta fase no se realizará penalización por incumplimiento de ANS por considerarse en transición, siempre y cuando cada uno de los ANS pactados esté por encima del 80%.

d) Los indicadores deberán medirse a partir del primer mes de la operación y presentarse los informes respectivos.

e) Finalizada la transición se procederá a la entrada en operación total donde aplicarán todas las características de servicio contratadas.

f) Durante la transición, el contratista saliente debe garantizar los siguientes servicios:

Mesa de servicio
Servicio de administración y soporte de la plataforma de almacenamiento del Datacenter principal y del alterno.
Servicio de administración y soporte servidores.
Servicio de administración de aplicaciones.
Servicio de administración de la plataforma AIX
Servicio de administración de bases de datos SQL server
Servicio de administración de bases de datos Oracle y postgresql
Servicio de administración de la plataforma de backup

Servicio de Gestión y administración de la red de datos
Servicio de gestión de Enlaces de datos
Servicio de administración de la plataforma de telefonía IP
Servicio de seguridad informática
Servicio de la plataforma de datos abiertos (Hadoop)

c) Los costos de la transición deben ser asumidos por el contratista saliente.

d) El contratista (proveedor al que se adjudique el nuevo contrato) deberá entregar a la Alcaldía de Medellín las actas de entrega y toda la documentación requerida en el marco de las actividades y obligaciones especificadas en el presente documento.

NOTA 1: la transición aplica únicamente cuando se presente cambio de proveedor.

13 OBLIGACIONES DE LAS PARTES

La gestión de la infraestructura Tecnológica se refiere a aquellos servicios orientados a la gestión sobre la Infraestructura Tecnológica del Municipio, con el fin de garantizar la continuidad de las operaciones diarias y la permanente prestación de los servicios a los ciudadanos de la Alcaldía de Medellín y a los servidores públicos.

La realización de actividades especiales por parte del grupo de Soporte a la Infraestructura Tecnológica debe ser pactada con previa anticipación entre la supervisión del contrato asignado por el Alcaldía de Medellín y el Gerente de Negocio para el proyecto asignado por el contratista. Estas actividades especiales comprenden instalaciones masivas de hardware e instalaciones de equipos que no estén dentro del inventario de esta propuesta (ver documento “Línea Base”). Si la ejecución de dichas actividades genera gastos adicionales, como el pago de horas extras o la contratación de recursos adicionales, estos gastos serán asumidos por el Alcaldía de Medellín.

Las siguientes son las responsabilidades de la Alcaldía de Medellín con el cumplimiento de la Mesa de Servicio:

14 Obligaciones de la Alcaldía de Medellín para la mesa de servicio

- Realizar la administración y manejo de licencias. Si el proveedor de servicios instala una licencia sin autorización del Distrito de Medellín, el proveedor de servicios asumirá los costos que se generen y responderá ante los entes de control por dicha instalación.
- Informar oportunamente al proveedor de servicios, los cambios a realizar en la plataforma de tecnología y las soluciones para los efectos que dichas actividades puedan generar.
- Proveer la infraestructura necesaria para el envío de las notificaciones a analistas y usuarios del servicio.
- Mantener actualizada la Mesa de Servicios acerca de cambios en la matriz de escalamiento de analistas y proveedores.
- Dar a conocer los acuerdos de niveles de servicio suscritos con terceros.
- Difundir los servicios a la comunidad de usuarios
- Entregar al proveedor de servicios de forma oportuna procesos, procedimientos, formatos, y los instructivos necesarios para dar soporte a las aplicaciones propias del negocio.
- Hacer uso de la herramienta de gestión para documentar y gestionar los casos asignados.
- Informar al proveedor de servicios, periódicamente los nombres de los usuarios o procesos VIP.
- Entregar la infraestructura relacionada con: lugar físico, telefonía, equipos de cómputo, escritorio y silla en las instalaciones del Distrito de Medellín para cada una de las personas requeridas en sitio (sedes de la administración).
- Tener disponible el stock necesario de cintas y sistemas de almacenaje para las tareas de backup.
- Proveer al proveedor de servicios toda la información de los usuarios nuevos (Identificación, Nombre, Teléfono, Cargo, Secretaría, etc.).
- Operar y gestionar el software de monitoreo existente al interior de la entidad.
- Verificar el cumplimiento del pago de salarios / honorarios y demás obligaciones laborales, así como los aportes al Sistema de Seguridad Social Integral, conforme a lo señalado en el Artículo 50 de la Ley 789 de 2002 y normas reglamentarias.
- Cuando se realice ingreso de un nuevo elemento a la infraestructura tecnológica a soportar por el proveedor de servicios, el Distrito de Medellín hará entrega formal del elemento; realizando la transferencia de conocimiento, entrega de arquitectura de la solución, documentación, diseño, plan de escalamiento siempre y cuando se requiera.
- Verificar el cumplimiento del protocolo de bioseguridad registrado y aprobado por la ARL del proveedor de servicios. Así mismo, vigilar que, durante toda la ejecución del contrato, el proveedor de servicios aplique las medidas necesarias de protección y bioseguridad de todos los trabajadores y de toda la cadena de producción, transporte y distribución.
- Informar al proveedor de servicios con anticipación la solicitud de extensión del horario de la Mesa de Servicios para fechas especiales.

15 Obligaciones del contratista

El CONTRATISTA se obliga para con EL DISTRITO DE MEDELLÍN a cumplir con todas las especificaciones técnicas que se relaciona en el estudio previo y en la propuesta presentada por EL CONTRATISTA y aceptada por EL DISTRITO DE MEDELLÍN, las cuales hacen parte integrante del contrato.

A continuación, se detalla las actividades que debe cumplir el contratista:

- Cumplir completamente el objeto del Contrato.
- Implementar y mantener un esquema de gobierno, atribuciones, políticas y procedimientos específicos para identificar, valorar, controlar y monitorear los diferentes tipos de riesgos operativos inherentes a la prestación de servicios contratados.
- Implementar y mantener los procedimientos o protocolos para identificar, reportar, analizar, valorar y gestionar la materialización de eventos de riesgo inherentes a la prestación de los servicios contratados.
- Cumplir con políticas de seguridad establecidas por el Gobierno TI del cliente asociadas a la protección de todos aquellos activos de información (físicos y electrónicos) que se gestionarían durante la prestación del servicio contratado
- Presentar por escrito de forma mensual al Distrito de Medellín, los informes de gestión a través de los cuales se pueda evidenciar el resultado y cumplimiento de los indicadores, los tiempos de atención y respuesta, los avances, los hallazgos y los inconvenientes presentados en el desarrollo del servicio contratado
- Gestionar que durante la ejecución del Contrato se cumplan y garanticen los procedimientos necesarios para asegurar la calidad del servicio.
- Informar de manera inmediata al Distrito de Medellín aquellos casos en que se evidencien cambios, alteraciones, manipulación o modificaciones en los equipos e infraestructura utilizada para la prestación del servicio.
- Gestionar los Canales de Internet.
- Cumplir con las políticas de seguridad de información del Distrito de Medellín.
- Registrar en la herramienta de gestión todos los casos que llegan a la Mesa de Servicios a través de los diferentes medios ofrecidos.
- Realizar las pruebas que aseguren el correcto funcionamiento de los servicios informáticos.
- Documentar en la herramienta de gestión todas las actividades de acuerdo con las plantillas definidas por Distrito de Medellín.

- Compartir y socializar los OLA y ANS que han sido definidos para el proyecto.
- Informar oportunamente los eventos que afectan el cumplimiento de los ANS definidos por el Distrito de Medellín.
- Mantener la continuidad y disponibilidad de la plataforma tecnológica en los niveles acordados.
- Proveer un ambiente seguro y de confidencialidad para el Distrito.
- Brindar un trato amable y respetuoso a los usuarios de los servicios.
- Solicitar autorización para ejecutar procedimientos que modifiquen los estándares de hardware o software tales como: actualización de BIOS, drivers, fixes, service packs, actualizaciones de versión etc. (Gestión de Cambios).
- Realizar las actualizaciones de las diferentes aplicaciones de usuario final y migraciones de plataformas.
- Realizar los upgrades, updates, cambios de versión e instalaciones de hardware y software que requiera el Distrito de Medellín, en sus diferentes plataformas tecnológicas, tales como: servidores, motores de bases de datos, almacenamiento, correo, directorio activo, etc. El distrito Medellín asume los costos de licenciamiento que se requiera. Para las actualizaciones mayores, migraciones, upgrades o proyectos nuevos se debe realizar factibilidad técnica y económica
- Permanecer en las instalaciones del Distrito siempre con el carné visible que lo identifica como Tigo.
- Cuando se preste el servicio en sitio, dejar el puesto de trabajo del usuario tal cual lo encuentra.
- Capacitar y actualizar al servicio en las diferentes plataformas tecnológicas del Distrito de Medellín para la prestación de un servicio eficiente.
- Mantener a su servicio actualizado en el software de usuario final utilizado por los funcionarios de la entidad.
- Operar la herramienta de gestión de incidentes conforme a las instrucciones y configuraciones dadas por Distrito de Medellín.
- Generar y documentar todos los procesos y procedimientos necesarios para garantizar la estandarización de la operación en el Distrito de Medellín.
- Disponer de los medios y herramientas requeridos para la realización de mantenimientos correctivos y preventivos, esto es, desplazamientos, transporte de equipos y partes de contingencia, entre otros.

- Facilitar el desplazamiento de sus empleados a las diferentes sedes externas, o disponer de un sistema alterno para atención a sedes externas, que le permitan cumplir lo definido en este documento.
- Facilitar al Distrito de Medellín software open source que permita un mejor desempeño y visibilidad de las plataformas tecnológicas.
- Mantener el servicio necesario para la prestación de los servicios solicitados de manera que permita el cumplimiento de ANS e indicadores definidos.
- Registrar solicitudes de servicio: Recibir la solicitud por cualquiera de los medios habilitados para la recepción de estos.
- Reportar cada inconveniente técnico que se presente en cada una de las plataformas
- Entrega de un único número de identificación para el caso (Ticket) que facilite su búsqueda, actualización y seguimiento.
- En todos los casos proporcionar un informe detallado de cada evento con un impacto masivo como máximo 24 horas después de ocurrido el evento. Se consideran para esta actividad los casos de máxima y alta.
- Detalles del caso en el cual se especifique claramente los componentes de la infraestructura (hardware, software, dispositivos de comunicaciones y otros elementos) involucrados en el incidente, así mismo como la descripción de los síntomas o errores que se presentan cuando el usuario intenta ejecutar funciones en particular en cualquiera de los sistemas de información. La documentación de los casos se hará de acuerdo con las plantillas y procedimientos definidos por el Distrito de Medellín.
- Cumplir con el protocolo de bioseguridad registrado y aprobado por la ARL del proveedor de servicios. Así mismo, el proveedor de servicios deberá garantizar durante toda la ejecución del contrato la aplicación de las medidas necesarias de protección y bioseguridad de todos los trabajadores y de toda la cadena de producción, transporte y distribución.
- Clasificar incidentes y solicitudes de servicio de acuerdo con la categorización establecida entre las partes: Categoría, subcategoría, síntoma, causa, detalle, grupo y responsable.
- Generar una encuesta de servicio relacionada con la calidad del servicio de manera aleatoria a los usuarios que hicieron uso del servicio en el mes. Esta actividad será realizada por el área interna de Calidad.
- Diagnosticar y Solucionar incidentes: determinar cuáles son las causas básicas que están impidiendo que el usuario ejecute las funcionalidades de las tecnologías de información que tiene a disposición y sobre las cuales se ha reportado el incidente. Si al momento de realizar el diagnóstico se encuentra que el registro y la clasificación inicial del mismo no son los correctos, este debe reclasificarse en los términos reales del incidente.

- Consultar las bases de datos de Conocimiento, de Errores Conocidos y de la Gestión de la
- Configuración, con el fin de encontrar facilidades de análisis, diagnóstico y solución.
- Alineación con los planes de continuidad de negocio definidos por el Municipio, esto es, acatar los protocolos de respuesta ante incidentes mayores y/o desastres naturales. Aplicar los protocolos de contingencia y recuperación.
- Coordinación y enrutamiento a los diferentes grupos de soporte de los incidentes que no pueden ser solucionados en primer nivel: Si una vez realizado el diagnóstico del incidente se determina que la solución de este no se puede implementar por la Mesa de Servicios, el incidente debe escalarse al nivel de soporte y analistas del cliente correspondiente, de conformidad con las matrices de escalamiento. Este escalamiento está complementado con un seguimiento y control por parte del Gestor de Incidentes apoyándose en las alertas de la herramienta de gestión. Los grupos de soporte del Distrito de Medellín son: Aplicaciones, Hardware y Seguridad.
- Generación de estadísticas y reportes del servicio.
- Explicar al usuario los procedimientos realizados durante la prestación del servicio, así como la operación cuando se trata de instalaciones, actualizaciones, configuraciones y similares; de esta manera se disminuye el riesgo que el servicio afecte los procesos del usuario.
- Generar y mantener actualizados los procedimientos del servicio, entrenamiento básico a los usuarios para la resolución de cada problema que se presente.
- Documentar en el registro del incidente o requerimiento, las configuraciones o modificaciones realizadas en la infraestructura a nivel físico y/o lógico. Ej. Activación de casillas de verificación, configuración de puertos, adición de módulos de memoria, ejecución de utilidades, eliminación de archivos, etc. Activación de casillas de verificación, configuración de puertos, adición de módulos de memoria, ejecución de utilidades, eliminación de archivos, etc.
- Documentar las pruebas realizadas para verificar la eficacia de la solución planteada y los resultados obtenidos, soluciones fallidas, solución final y causas.
- Mantener actualizada la base de datos de Conocimiento.
- Apoyar al servicio del Distrito de Medellín en la solución de Incidentes y requerimientos.
- A disposición de los usuarios de Distrito de Medellín, se dispondrá de un mecanismo de atención de sugerencias y reclamos.
- Recibir, analizar, atender y resolver los requerimientos de mantenimiento correctivo hechos por los usuarios del Distrito de Medellín a través de la Herramienta de gestión con el propósito de restablecer la normal operación del servicio.

- Cumplir con los estándares de operación definidos para la administración de incidentes y requerimientos.
- Proponer los procedimientos de cambio o movimiento de equipos, los cuales serán validados y aprobados por el Distrito de Medellín.
- Escalar los incidentes que después de un adecuado análisis y/o tiempo definido no pueda resolver.
- Mantener actualizada la base de datos de conocimientos de propiedad del Distrito de Medellín, donde se almacenará la información referente a los productos y servicios de tecnología con sus respectivos errores conocidos.
- Garantizar que la información, matrices de escalamiento, instaladores y los procedimientos relacionados con su actividad se encuentren disponibles en un sitio seguro en internet, de forma que los soportes tengan acceso.
- Entrega de documentación, errores conocidos, instructivos de instalación entre otros.
- Entrega de medios de instalación, drivers, Service Pack, entre otros, por parte del Distrito de Medellín.
- Las demás actividades inherentes a la atención de la Mesa de Servicios. realizar reuniones previas, posteriores y durante los cambios.
- Notificación del cambio desde su concepción por parte de las instancias administrativas, el área de TI o donde se origine.
- Capacitación al servicio de soporte en sitio y mesa.

16 Obligaciones del contratista referente al cumplimiento del sistema de gestión de la seguridad y salud en el trabajo (SGSST)

- El Contratista debe cumplir las disposiciones contempladas en el Decreto 1072 de 2015, Capítulo 6 y la Resolución 0312 de 2019 y las demás disposiciones vigentes en materia de Seguridad Social y Seguridad y Salud en el Trabajo.
- Obligación que será verificada por los supervisores con los siguientes documentos:
- La autoevaluación del SGSST o autoevaluaciones del año en curso. Conforme al resultado de la autoevaluación que aporte el contratista, este asume unas obligaciones que están

expresas en el artículo 28 Resolución 0312 de 2019, las cuales serán verificadas por el supervisor según sea el caso.

- Plan de Trabajo del SG-SST acorde a la autoevaluación o autoevaluaciones del año en curso.
- En los contratos donde el contratista deba dotar de Elementos de Protección Personal, el supervisor debe constatar en campo dicha obligación, y solicitar al contratista formato de entrega de los Elementos de Protección Personal que lleve la firma de los trabajadores que están prestando sus servicios en el Alcaldía de Medellín, dejando todas las evidencias en el informe parcial de supervisión, y debe ser revisada en cada pago.