ANEXO No. 1
ESPECIFICACIONES TÉCNICAS

Objeto:
DISPONER EL OUTSOURCING DE UN SISTEMA DE MESA DE AYUDA Y SERVICIOS CONEXOS PARA ATENDER LAS SOLICITUDES COMO INCIDENCIAS O PROBLEMAS DE LOS SERVICIOS DE TI, DENTRO DE LA JEP.
Objetivos específicos:
1. Proveer a la JEP una solución de Mesa de ayuda.
a. Prestar el servicio centralizado de Mesa de Ayuda bajo procesos ITIL.
b. Realizar la gestión del servicio de mesa de ayuda con los procesos: Solicitudes, Incidentes, Problemas, Catálogo de Servicios, Reportes y Transferencia de conocimiento.
c. Realizar el mantenimiento correctivo a los recursos computacionales a que hubiera lugar y la gestión de una bolsa de repuestos.
2. Proveer a la JEP con una solución de Gestión del Servicio de TI (ITSM- IT Service Management).
a. Proveer una herramienta para realizar la Gestión de Servicios de TI.
b. Implementar la herramienta para la realización de Gestión de Servicios de TI.
c. Capacitar a la JEP para la administración de las herramientas de Gestión de Servicios de TI.
3. Proveer a la JEP con una solución de seguridad enfocada en el Gobierno y Administración de Identidades (IGA) y Accesos Unificados.
a. Proveer una herramienta para administrar y controlar las identidades y accesos a diferentes aplicaciones y plataformas de JEP de manera automatizada.
b. Implementar la solución de seguridad enfocada al Gobierno y Administración de Identidades (IGA) y Acceso Unificados.
c. Prestar el servicio de seguridad enfocado en la gestión de usuarios internos.
Alcance:
El alcance del objeto incluye, entre otros: 1. Contratar el servicio de Mesa de ayuda, soporte en sitio que garanticen la gestión, análisis, documentación y solución de todos los incidentes y

requerimientos tecnológicos para el soporte de primer nivel en: equipos de cómputo ofimáticos, redes LAN y WLAN (Wifi local), comunicaciones unificadas (incluye telefonía IP), aplicaciones misionales, estratégicas, de soporte a los procesos y otras que se adquieran durante la vigencia del contrato solicitados por los funcionarios de la entidad en relación con los servicios de TI, basándose en las buenas prácticas ITIL.

2. Prestar un servicio centralizado de mesa de ayuda, desde un punto único de contacto donde el usuario (Funcionario o Contratista) focalice las solicitudes de servicios que requieran los colaboradores de la (JEP), brindando atención sobre aquellos incidentes y requerimientos solucionables por el personal de soporte remoto, soporte en sitio y especialistas de nivel dos para la atención en gestión de identidades, gestión de seguridad y administración de seguridad perimetral, realizando seguimiento y monitoreo a la efectividad de las soluciones entregadas y a las escaladas a un nivel superior de conocimiento, enmarcados en los acuerdos de niveles de servicios (ANS) establecidos por la Entidad**.**

3. Adquirir una herramienta para la Gestión de Servicios de TI, en la cual se desplieguen los módulos para la prestación del servicio de Mesa de Ayuda y se implementen los procesos requeridos. La cantidad de procesos y módulos descritos en este anexo.

4. Adquirir una solución integral de seguridad enfocada en la gestión de usuarios internos para operar de manera más efectiva la gestión y gobierno de identidades, así como el "Inicio de Sesión Unificado". Dicha solución deberá ser operada por el contratista de manera óptima rigiéndose bajo los Acuerdos de Niveles de Servicio establecidos. Dada la importancia de la solución de Seguridad se requiere que todos los componentes, módulos, herramientas, productos, que hagan parte de la solución global se integren y sean de un mismo fabricante.

Tabla Ficha Descripción General.

REQUERIMIENTOS TÉCNICOS

1. SOLUCIÓN DE MESA DE AYUDA

Entre las funciones de la Mesa de Ayuda está la de atender TODOS los incidentes y requerimientos que ingresen desde los diferentes canales de comunicación: Línea Telefónica, Intranet de la Entidad, Correo Electrónico y/o chat, garantizando la atención y la solución de los requerimientos del servicio.

Para la prestación del servicio, el proveedor deberá incluir, pero no limitarse a lo siguiente:

- Disponer y mantener en sus oficinas el espacio físico adecuado para albergar a los funcionarios que realizarán la Gestión de Mesa de Ayuda.
- Dotar a sus funcionarios de las facilidades tecnológicas asociadas a la Gestión de Servicios a su cargo, compuestas entre otros por: acceso a Internet, herramienta de atención telefónica, distribución de llamadas, computadores, diademas, teléfonos móviles con plan de datos, herramientas y demás recursos idóneos, necesarios para realizar eficientemente su labor.
- La Mesa de Ayuda deberá confirmar con el usuario la solución efectiva de las solicitudes.
- La Mesa de Ayuda deberá garantizar el Soporte de Primer Nivel (modalidad Remota) para todos los casos reportados (Atención) y Solución cuando está a su alcance.
- Aceptar, cumplir y ajustar sus procedimientos operativos a las políticas de seguridad de la información que sean requeridas por la JEP.
- Garantizar que todas las solicitudes que se deban escalar a un Nivel de Soporte superior tengan la documentación mínima necesaria para poder atenderlos sin pérdida de tiempo. A continuación, se indica la documentación mínima necesaria:

  i. Descripción del soporte realizado por la Nivel 1 indicando las pruebas solicitadas y resultados obtenidos.

  ii. Imágenes de errores ocurridos en los aplicativos o en las computadoras.

  iii. Adjuntar el correo enviado por el usuario.

  iv. Para aplicativos describir el paso a paso donde se presenta el error.

  v. Otro que sea de utilidad para la solución oportuna.

- Realizar el seguimiento al ciclo de vida de todos los casos registrados en la herramienta de Gestión de Servicio, así como el cumplimiento de los ANS de dichos servicios establecidos con los grupos resolutores.
- Escalamiento y gestión con la JEP y proveedores de las solicitudes que requieren escalamiento, en base a la matriz de escalamiento definida.
- Garantizar que la atención de las solicitudes realizada por sus funcionarios se haga con base a las mejores prácticas recomendadas en ITIL.
- La mesa de ayuda debe garantizar que todas las solicitudes, atendidas por los Niveles 1, 2 y 3 sean documentadas, describiendo cómo se le dio solución.
- Los profesionales requeridos para prestar el Servicio en Mesa de Ayuda, deberán cumplir con los requisitos de la tabla equipo de trabajo de acuerdo con lo establecido en anexo 1 Especificaciones Técnicas.

1.1. CARACTERÍSTICAS TÉCNICAS DE LOS SERVICIOS

Las siguientes son las especificaciones técnicas mínimas requeridas que debe cumplir la propuesta:

1.1.1 SERVICIO DE MESA DE AYUDA

El Proveedor de Servicio deberá implementar un modelo de servicio garantizando la estructura para la gestión y atención a las solicitudes de los usuarios que consumen los servicios tecnológicos de la JEP, con sus correspondientes niveles de escalamiento a las líneas de servicio, para lo cual también deberá realizar gestión a las siguientes actividades señaladas:

- Seguimiento a las solicitudes de servicio, escaladas a otras líneas de servicio, nivel especializado de parte del cliente, fabricantes y proveedores de servicios tecnológicos.
- Soporte en Salas de Audiencia: Se establecerá la atención a los requerimientos que surjan para el acompañamiento del personal de soporte en sitio, en apoyo técnico y funcional en el manejo de los equipos audiovisuales y de computo, garantizando el buen desarrollo de las audiencias.
- Soporte en el manejo de la Pagina Web e Intranet de la Entidad.
- Soporte de Segundo Nivel a Especialistas: Atención y solución a los requerimientos de servicio escalados en las especialidades de:

- Gestión de Identidades: Para permisos, roles y accesos a los aplicativos de la Entidad.
- Gestión de protección perimetral e incidentes de seguridad: Resguardar mediante políticas de seguridad y componentes tecnológicos la información de la Entidad.

1.2 HORARIO DE PRESTACIÓN DEL SERVICIO

El servicio prestado por la Mesa de Ayuda atenderá en la siguiente franja de horario:

- Lunes a viernes de 7:30 a.m. a 8:00 p.m.
- Soportado mediante mallas de turnos para garantizar el cubrimiento del horario.

MALLAS DE TURNOS SOPORTE REMOTO	
Horario	Cantidad de Recurso Humanos
7:30 A.M. a 5:00 P.M.	1
8:00 A.M. a 5:30 P.M.	2
10:00 A.M a 8:00 P.M	1

MALLAS DE TURNOS SOPORTE EN SITIO	
Horario	Cantidad de Recurso Humanos
7:30 A.M. a 5:00 P.M.	2
8:00 A.M. a 5:30 P.M.	3
10:00 A.M a 8:00 P.M	1

Los anteriores recursos humanos estarán dedicados tiempo completo a la gestión del contrato. Las actividades que se desarrollarán estarán enmarcadas en las buenas prácticas de ITIL, a fin de facilitar la gobernabilidad de la gestión de los servicios tecnológicos para la JEP.

No obstante, esta disponibilidad debe contar con flexibilidad para atender eventos no programados o actividades extraordinarias en horarios diferentes a los estipulados anteriormente. Cuando se requiera realizar actividades con un horario diferente al mencionado se programarán con un día de anterioridad (en casos de urgencia con dos (2) horas de anticipación), para acordar con el coordinador de la Mesa la logística y demás actividades para su desarrollo.

1.3 ALCANCE DEL SOPORTE EN SITIO Y REMOTO

El soporte de primer nivel estará en contacto directo con el usuario y solucionará las incidencias triviales, basado en un protocolo, bases de datos de consulta y otras ayudas para el soporte.

Este es el nivel de asistencia inicial, responsable de las incidencias básicas del cliente. Su principal función, es reunir información de los usuarios y determinar la prioridad de la incidencia mediante el análisis de los síntomas y la determinación del problema. Debe contar con una base de conocimiento, un protocolo de atención y un procedimiento claramente definido, en el cual se puedan atender la mayor cantidad de incidentes, basados en los casos conocidos que son de mayor ocurrencia en las JEP.

Las siguientes son las actividades demarcadas para el soporte en sitio y soporte remoto en la prestación de los servicios técnico funcional del equipamiento Informáticos propiedad de la JEP, para lo cual se establece el siguiente alcance donde el Contratista debe garantizar:

1. Atender de manera remota y presencial el servicio de soporte técnico de primer nivel en la infraestructura de equipos ofimáticos basados en los lineamientos de buenas prácticas de ITIL.
2. Registrar TODAS las solicitudes de servicios llámense incidentes o requerimientos en la Herramienta de gestión de mesa de ayuda.
3. Dar soporte de primer nivel de servicio para:
   a. El servicio de la Telefonía IP.
   b. El servicio de Televisión de la JEP.
   c. Equipos de cómputo a nivel ofimático.
   d. Conectividad WLAN y LAN, configuración de entorno de red en los PC, pruebas de conectividad en los puestos de trabajo de los usuarios.

e. Aplicaciones que requiera la Entidad - Instalaciones y reinstalaciones de software.
f. Servicio de Impresión, fotocopiado y escaneado.
g. Atención a fallas originadas por mal funcionamiento del software y hardware.
h. Traslado de equipos entre las dependencias y registro de estos para actualizar permanentemente el inventario.
i. Atención al proceso de recuperación de información. Para ello se utilizará software entregado por la firma para tal fin.
j. Apertura de casos directamente con proveedores, con el fin de dar solución a inconvenientes presentados.
k. Formatear, Instalar y configurar las estaciones de trabajo en los equipos actuales o futuros que la entidad adquiera.
l. Soporte e instalación de otros equipos que se encuentren relacionados en el Anexo 2. Inventario de Equipos JEP.
m. Apoyar en otras actividades, en caso de ser requerido.

4. Documentar los servicios soportados en el nivel 1 y alimentar la base de datos de errores conocidos (KEDB).
5. Establecer comunicación con el soporte de segundo nivel para la resolución de incidentes o requerimientos de servicio.
6. Mantener a los usuarios informados del progreso de la solicitud en caso de que la solución no sea inmediata (establecer protocolos de interacción con usuarios previa aprobación de la JEP).
7. Apoyar permanentemente el diagnóstico de las garantías de fabrica para los equipos de cómputo ofimáticos que se requieran dar escalamiento a un tercero o fabricante.
8. Analizar, investigar, interpretar y solucionar los problemas específicos que se detecten a nivel de plataforma tecnológica en equipos de cómputo ofimáticos, redes, comunicaciones y seguridad informática.
9. Dar cumplimiento a los estándares de gestión de calidad establecidos en la Entidad en la instalación de las herramientas ofimáticas en los equipos de cómputo.
10. Aplicar el conocimiento, mediante el uso y análisis de tendencias para identificar las condiciones y evitar su ocurrencia, alimentando una base del conocimiento.
11. Resolver los problemas en forma integral en la medida en que se ubican las causas raíz de estos.

12. Documentar los procedimientos básicos en la base de datos del conocimiento y realizar difusión de estos documentos. Dicha base de datos es de propiedad de la JEP.
13. Implementar un plan de reducción de incidentes basado en la herramienta de gestión de incidentes orientado a elevar la disponibilidad de los servicios y los usuarios y entregarlo mensualmente.
14. Realizar las pruebas necesarias que aseguren el correcto funcionamiento de los servicios informáticos a través de la lista de chequeo entregada por la Dirección de TI de la JEP, con el fin de asegurar una salida controlada de la prestación del servicio.

1.4 ALCANCE DEL SOPORTE DE ESPECIALISTAS

A continuación, se demarca el alcance en las actividades para el soporte a los servicios especializados en líneas de servicio.

1.4.1 Gobierno Y Administración De Identidades:

Mediante políticas establecidas por la Entidad, se realizará la administración de usuarios y sus derechos de acceso mínimo a 7 aplicaciones; de forma automatizada y estandarizando las credenciales de los 1300 usuarios de la JEP en dichas aplicaciones y debe estar disponible para nuevas aplicaciones.

Las solicitudes de nuevos usuarios y/o cambios serán tomadas desde el portal de la solución, la cual maneja todos los requerimientos, solicitudes, relacionados con los accesos de los usuarios en las aplicaciones mencionadas.

1.4.2 Otros Servicios:

a. Gestión de protección perimetral e Incidentes de seguridad:

Velar que la información sea correcta, completa y resguardada ante posibles pérdidas o vulnerabilidades, donde este siempre a disposición de la Entidad y que sea utilizada sólo por aquellos que tienen autorización para obsérvala, modificarla y cambiarla.

b. Gestión de Medios Audiovisuales:

Garantizar el apoyo técnico funcional de los equipos de medios audiovisuales que garantizarán el desarrollo de las audiencias en la JEP.

c. Gestión de Portal Web

Administrar y gestionar los contenidos de diferentes portales web e intranet de la JEP.

1.5 PROFESIONALES REQUERIDOS

La mesa de ayuda debe estar conformada por seis (6) agentes en sitio, responsables del seguimiento al incidente hasta su solución final, cuatro (4) agentes remotos, responsables de dar apoyo telefónico, gestión de incidentes reportados en la herramienta y escalamientos a soporte de segundo nivel, seis (6) Ingenieros de Sistemas o Electrónico o Telecomunicaciones, para realizar las siguientes labores y ubicados de la siguiente forma:

- Seis (6) agentes en Sitio ubicados en la Sede principal de la JEP -Justicia Especial para la Paz- en la carrera 7 No 63-44 Pisos 1 al 11, en la ciudad de Bogotá, para atender a los usuarios finales internos.
- Cuatro (4) agentes remotos, responsables de dar apoyo telefónico y gestión de incidentes reportados en la herramienta y escalamientos a soporte de segundo nivel, ubicados en las instalaciones que designe el CONTRATISTA, en la ciudad de Bogotá.
- Un (1) Ingeniero de Sistemas o Electrónico o Telecomunicaciones ubicado en la Sede principal de la JEP -Justicia Especial para la Paz- en la carrera 7 No 63-44 Pisos 1 al 11, en la ciudad de Bogotá, para la coordinación de la mesa de ayuda.

- Dos (2) Ingenieros de Sistemas o Electrónico o Telecomunicaciones ubicado en la Sede principal de la JEP -Justicia Especial para la Paz- en la carrera 7 No 63-44 Pisos 1 al 11, en la ciudad de Bogotá, para dar soporte de segundo nivel, en lo relacionado con la seguridad y Gestión de Identidades.
- Un (1) Ingeniero de Sistemas o Electrónico o Telecomunicaciones ubicado en la Sede principal de la JEP -Justicia Especial para la Paz- en la carrera 7 No 63-44 Pisos 1 al 11, en la ciudad de Bogotá, para ofrecer soporte de segundo nivel, en lo relacionado con Gestión de protección perimetral.
- Un (1) Ingeniero de Sistemas o Electrónico o Telecomunicaciones ubicado en la Sede principal de la JEP -Justicia Especial para la Paz- en la carrera 7 No 63-44 Pisos 1 al 11, en la ciudad de Bogotá, para ofrecer soporte de segundo nivel, en

lo relacionado con Gestión eventos de seguridad informática Gestión de protección perimetral e Incidentes de seguridad.

- Un (1) Ingeniero de Sistemas o Electrónico o Telecomunicaciones ubicado en la Sede principal de la JEP -Justicia Especial para la Paz- en la carrera 7 No 63-44 Pisos 1 al 11, en la ciudad de Bogotá, para ofrecer soporte de segundo nivel. En lo relacionado con Gestión de Medios Audiovisuales.
- Un (1) Ingeniero de Sistemas o Electrónico o Telecomunicaciones ubicado en la Sede principal de la JEP -Justicia Especial para la Paz- en la carrera 7 No 6-44 Pisos 1 al 11, en la ciudad de Bogotá, para ofrecer soporte de segundo nivel. En lo relacionado con las funciones de Webmaster.

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
1	Coordinador Mesa de Ayuda	Profesional en Ingeniería de Sistemas, Electrónica, telecomunicaciones, Ingeniería de Software o carreras afines. Certificaciones en ITIL Intermedio OSA y Foundation o superior. Tarjeta Profesional	Experiencia mínima de cuatro (4) años en cargos relacionados con la coordinación en mesas de ayuda, apoyo al soporte técnico y/o atención al usuario final. - Manejo de herramientas de mesa de ayuda y de Call Center reconocidas en el mercado para la generación de indicadores de	• Asegurar el cumplimiento de la JEP - Jurisdicción Especial para la Paz en la atención de los incidentes y requerimientos de servicio de TI reportados en la Mesa de Ayuda • Coordinar las tareas del grupo de agentes de la Mesa de Ayuda, para la solución de incidentes y requerimientos de servicio TI • Realizar seguimiento a los casos de

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
			gestión de la mesa de ayuda. - Generación de informes de gestión para el cumplimiento del contrato de mesa de ayuda. - Implementación de los procesos de ITIL en la operación en mesa de ayuda. Excelentes relaciones interpersonales y liderazgo en equipos de trabajo a su cargo, Interacción y manejo del Cliente	atención prioritaria • Realizar seguimiento diario a la gestión realizada por los agentes • Escalar al interior de la Dirección de Gestión de Información y Tecnología los incidentes y requerimientos de servicio de TI que requieran de atención prioritaria. Realizar análisis mensual del Informe de evaluación de gestión de incidentes y requerimientos de servicio de TI y proponer acciones de mejora • Dedicación 100% del tiempo de ejecución del servicio

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
4	Agentes de Soporte Remoto	Técnico, Tecnólogo o estudiante de (4) semestres en sistemas, electrónica, telecomunicaciones o carreras afines Tarjeta Profesional (si aplica)	Dos (2) años de experiencia mínima en funciones de: Soporte telefónico, soporte técnico en equipos de cómputo como son (Equipos de escritorio, portátiles, impresoras, video beam, escáneres). Manejo en herramientas de mesa de ayuda reconocidas en el mercado. Conocimientos básicos en el soporte de sistemas operativos como son Windows y sus últimas versiones. La última experiencia laboral en mesa de ayuda	• Recibir, registrar y gestionar todos los incidentes o requerimientos de servicio de TI que se generan en la Entidad. • Proveer la primera línea de atención, investigación, diagnóstico y escalamiento de los incidentes y requerimientos de servicio de TI reportados por los usuarios de la Entidad. • Emplear las herramientas remotas autorizadas para el diagnóstico y solución de los casos. • Mantener comunicación con los usuarios, informando los avances de los casos.

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
			tenga como mínimo una permanencia a nivel de contrato de seis (6) meses con funciones propias como agente de mesa de ayuda o de soporte en sitio	• Investigar, diagnosticar y escalar los incidentes o requerimientos de servicio de TI reportados por los usuarios de la Entidad. • Documentar en la herramienta de gestión de la mesa de ayuda todas las acciones realizadas para la atención de los incidentes o requerimientos de servicio de TI. • Informar al coordinador oportunamente de los casos que requieren atención especial y que no han sido solucionados. • Cumplir con los protocolos de atención establecidos por

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
				la Entidad, • Cumplir con las definiciones establecidas en el Procedimiento de Gestión de incidentes y requerimientos de servicio de TI. • Cumplir con los protocolos de atención establecidos por la Entidad • Dedicación 100% del tiempo de ejecución del servicio
6	Agentes en Sitio	Técnico, Tecnólogo o estudiante de (4) semestres en sistemas, electrónica, telecomunicaciones o carreras afines Tarjeta Profesional (si aplica)	Dos (2) años de experiencia mínima en funciones de: Soporte técnico en equipos de cómputo como son (Equipos de escritorio, portátiles, impresoras o video beam, escáneres).	• Recibir, registrar y gestionar todos los incidentes o requerimientos de servicio de TI que se generan en la Entidad. • Proveer la primera línea de atención, investigación, diagnóstico y escalamiento de los incidentes y

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
			Dentro de las funciones de soporte en sitio estén identificadas: Mantenimientos correctivos del parque computacional como son (Equipos de escritorio, portátiles, impresoras, video beam, escáneres). Conocimientos básicos en el soporte de sistemas operativos como son Windows y sus últimas versiones.	requerimientos de servicio de TI reportados por los usuarios de la Entidad. • Mantener comunicación con los usuarios, informando los avances de los casos. • Investigar, diagnosticar y escalar los incidentes o requerimientos de servicio de TI reportados por los usuarios de la Entidad. • Documentar en la herramienta de gestión de la mesa de ayuda todas las acciones realizadas para la atención de los incidentes o requerimientos de servicio de TI.

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
				• Informar al coordinador oportunamente de los casos que requieren atención especial y que no han sido solucionados. • Cumplir con los protocolos de atención establecidos por la Entidad, • Cumplir con las definiciones establecidas en el Procedimiento de Gestión de incidentes y requerimientos de servicio de TI. • Cumplir con los protocolos de atención establecidos por la Entidad • Dedicación 100% del tiempo de ejecución del servicio

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
1	Ingeniero de Gestión de Identidades	Ingeniero de sistemas, electrónica o telecomunicaciones. Tarjeta Profesional	Dos (2) años de experiencia mínima en: 1- En funciones de gestión de accesos o de identidades, en la herramienta ofrecida. 2- En la Creación y gestión de perfiles en aplicaciones misionales, estratégicas, de soporte a los procesos y otras que se adquieran durante la vigencia del contrato.	• Operar la Gestión de Identidades para brindar los permisos necesarios a los colaboradores de la JEP en los recursos tecnológicos de la Entidad, con el objetivo de administrar de manera controlada los permisos y accesos a los usuarios. • Dedicación 100% del tiempo de ejecución del servicio
1	Ingeniero de Protección perimetral	Ingeniero de sistemas, electrónica o telecomunicaciones. Con especialización en	Dos (2) años de experiencia mínima en funciones de administración en equipos de seguridad perimetral. También en la	• Apoyar de manera conjunta con el equipo de infraestructura el monitoreo de los equipos de protección perimetral e

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
		seguridad informática. Tarjeta Profesional	gestión de eventos e incidentes de seguridad.	incidentes de seguridad, identificando alertas de seguridad y reportarlas • Las actividades que se desarrollarán estarán enmarcadas en las buenas prácticas de seguridad en ISO 270001. • Dedicación 100% del tiempo de ejecución del servicio .
1	Ingeniero de Gestión eventos de seguridad informática	Ingeniero de sistemas, electrónica o telecomunicaciones. Tarjeta Profesional	Dos (2) años de experiencia mínima en funciones de administración en equipos de seguridad perimetral. También en la gestión de eventos e incidentes de seguridad.	• Apoyar de manera conjunta con el equipo de infraestructura el monitoreo de los equipos de protección perimetral e incidentes de seguridad, identificando alertas de seguridad y reportarlas

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
				• Las actividades que se desarrollarán estarán enmarcadas en las buenas prácticas de seguridad en ISO 270001. • Dedicación 100% del tiempo de ejecución del servicio .
1	Profesional en Medios Audiovisuales	Profesional en medios audiovisuales y/o Ingeniería de sistemas, electrónica, telecomunicaciones o carreras afines. Tarjeta Profesional (si aplica)	Dos (2) años de experiencia mínima en funciones de administración y funcionalidad de equipos audiovisuales. Dentro de las funciones realizadas del cargo este:	Responsable del soporte en medios audiovisuales de los equipos de video conferencias en apoyo técnico funcional, conociendo la importancia de mantener funcional y operativos los equipos audiovisuales dispuestos en cada una de las salas de audiencias. Velar por la funcionalidad y

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
				soporte de los equipos de las salas multimedia los fallos que se presenten
1	Ingeniero Web Master	Ingeniero de sistemas, electrónica o telecomunicaciones. Tarjeta Profesional	Profesional en Ingeniería de sistemas o carreras afines, con 2 años de experiencia como web master de sitios sobre Sharepoint. Conocimientos en SEO, patrones de diseño, Sharepoint	Administrar y gestionar los contenidos de diferentes portales web e intranet de la JEP. Estructura e implementación de Navegación para portales web Realización de Backups de los sitios, mantenimiento y actualización de Backups Desarrollo, análisis, optimización y seguimiento de estrategia SEO para portales web desarrollados sobre SharePoint para los clientes y

Cantidad	Perfil	Formación	Experiencia Específica	Responsabilidad y Dedicación
				para la compañía. Apoyo en los procesos de migración Mantenimiento de la seguridad de los sitios

1.6 ALCANCE DEL COORDINADOR MESA DE AYUDA

Las siguientes son las actividades que demarcan la gestión del Coordinador de la mesa de ayuda en la prestación de los servicios en el soporte técnico funcional del equipamiento Informático, propiedad de la JEP, para lo cual se establece el siguiente alcance donde el Contratista debe garantizar:

- Supervisar la operación de la mesa de ayuda durante la ejecución del contrato.
- Velar y ejecutar los compromisos contractuales dando el cumplimiento a los acuerdos de nivel de servicio (ANS).
- Realizar encuestas e informes de satisfacción del servicio mediante muestreo de llamadas de los usuarios de la entidad a la mesa de ayuda, para conocer la percepción del servicio en cuanto a la atención y solución de los tickets gestionados.
- Presentar los informes de gestión que el supervisor de contrato considere entregar para la gestión del contrato de la mesa de ayuda incluyendo el soporte de los especialistas de segundo nivel de servicio.
- Asistir a las reuniones de seguimiento que se coordinen con la supervisión del contrato.
- Apoyar activamente a los recursos de soporte en sitio y agentes remotos en la operación de la mesa de ayuda.
- Velar por el cumplimiento de los acuerdos contractuales, soportados mediante entregables.
- Tramitar todo movimiento de activos tecnológicos de la JEP en apoyo de la Dirección de TI.

- Deberá presentar como mínimo los siguientes informes:

DESCRIPCIÓN	FRECUENCIA	PROPUESTA
Histórico de casos registrados por mes (3 meses)	Mensual	Top 10 de Incidentes y Requerimientos
Trazabilidad de los casos abiertos en meses anteriores por grupo solucionador (Backlog)	Semanal y Mensual	Backlog
Top 10 Incidentes y Requerimientos.	Mensual	Top 10 de Incidentes Top 10 de Requerimientos
Informe de incidentes y solicitudes por prioridad y tiempo promedio de solución	Mensual	Prioridad de incidentes y solicitudes
Análisis de los indicadores con los datos y gráficas que permitan visualizar comparativos acumulados histórico y mensual por grupo solucionador (Se definirá junto con la Entidad dentro del informe mensual cuales indicadores necesitan tener comparativo acumulado histórico o mensual y tiempo que se mostrará en el histórico).	Mensual	Tendencia mensual incidentes (gráfico) Tendencia mensual requerimientos (Gráfico)
Porcentaje de solución de casos solucionados en primer nivel.	Mensual	Cumplimiento ANS-B - % solución primer nivel

DESCRIPCIÓN	FRECUENCIA	PROPUESTA
Reporte cumplimiento ANS	Mensual	Reporte cumplimiento ANS mensual
Informe por tipo de categoría y por tipo de ingreso	Semanal y Mensual	Top 10 de Incidentes Top 10 de Requerimientos
Reporte de presupuesto de la Bolsa de Repuestos Cantidad de casos sin aprobar	Mensual	Reporte de consumo de la bolsa de repuestos Indicador de ejecución presupuestal mensual Cantidad de casos sin aprobar
Otro que complemente la información necesaria para tomar decisiones sobre el servicio	Mensual	

1.7 ALCANCE DEL SOPORTE MESA DE AYUDA Y EN SITIO

Las actividades mínimas que debe ejecutar el personal de soporte remoto y en sitio de parte de El CONTRATISTA son:

- Gestionar y solucionar los tickets que le son asignados de acuerdo con los ANS establecidos, de acuerdo a mejores prácticas de ITIL.
- Realizar desplazamiento al sitio, documentando la información en el ticket, dando soluciones oportunas de acuerdo con los niveles de servicio establecidos. Para tal fin cada soporte en sitio deberá contar con las herramientas necesarias para la operación normal entre ellas: teléfono móvil, kit de herramientas la cual debe contener los elementos necesarios para operar en cumplimiento a las labores del servicio.
- Dar soporte de primer nivel de LAN referente a los centros de cableado. El personal de soporte en sitio deberá tener conocimientos básicos en red LAN y aprovisionar herramientas de trabajo (pinzas de compresión, generador de tonos, etc.).
- Dar soporte de primer nivel en aplicaciones de la Entidad (Todos los Sistemas de información implementados y en producción). para lo cual se brindará la

respectiva capacitación para la atención de los requerimientos de primer nivel en cuanto a aplicaciones y sistemas de información se refiere.

- El soporte en sitio y soporte remoto debe realizar los cierres de tickets y las demás actividades requeridas por la Entidad.
- El personal de soporte deberá participar activamente en tareas masivas y en aquellas que se derivan por la gestión de cambios en la Entidad.
- Los requerimientos tipo IMAC (Instalaciones, Movimientos, Adiciones y Cambios) están catalogados como cambios estándar dentro de las mejores prácticas de ITIL en la Dirección de Tecnologías de la Información, involucran, como su nombre lo indica, nuevas instalaciones, movimientos, adiciones, cambios y remociones, realizados en sitio como parte de un soporte. Estos soportes se realizan de manera programada y el plan de trabajo es definido en conjunto con la Entidad, siempre y cuando sean superiores a diez (10) en un día. Las Instalaciones y Movimientos tendrán un trato especial y se realizará programación para su ejecución previa aprobación de la JEP.
- Garantizar que el personal asignado a la mesa de Ayuda brindará solución remota a los casos reportados por los usuarios si es posible la solución remota de estos, de lo contrario se desplazará personal técnico a los puestos de trabajo.
- TODAS las solicitudes de servicio deben ser registradas en la herramienta de gestión de la mesa de ayuda.
- Realizar escalamiento a las diferentes líneas de servicio.
- Seguimiento a los casos escalados en el primer nivel, segundo nivel de soporte y casos escalados a fabricantes o terceros.
- Mantener la confidencialidad de la información propiedad de la JEP-. Jurisdicción Especial para la Paz. a que tenga acceso en el marco de ejecución del contrato, así mismo cuando termine el contrato deberá entregar al JEP-. Jurisdicción Especial para la Paz. toda la información que este solicite garantizando que la misma es propiedad de la JEP-. Jurisdicción Especial para la Paz. EL PROPONENTE se compromete a no divulgar la información obtenida de la JEP - Jurisdicción Especial para la Paz, durante la ejecución del contrato a terceras personas.
- Identificación del Personal del Contratista: TODO el personal del CONTRATISTA deberá portar el carné con foto en un lugar visible que lo identifique como empleado de EL CONTRATISTA y para el personal de soporte remoto y en sitio como mínimo una prenda de identificación puede ser (Chaleco o camisa definido por la Entidad) que contenga el logo o marquilla con el nombre Institucional de la Entidad, en aprobación a la supervisión del contrato, para facilitar la adaptación y

reconocimiento por parte de los Colaboradores (funcionarios y contratistas); estas prendas deben estar siempre en buen estado.

1.8. LINEA BASE DE RECURSOS TECNOLOGICOS

Los equipos objeto del servicio que se describen en el Anexo 2. Inventario de Equipos JEP, adicionalmente se debe tener en cuenta futuras adquisiciones de bienes tecnológicos por parte de la entidad. El CONTRATISTA deberá brindar el soporte remoto o en sitio de acuerdo con los niveles de servicio establecidos

1.9 MANTENIMIENTO CORRECTIVO A LOS RECURSOS tecnologicos CON SUMINISTRO DE REPUESTOS

Realizar mantenimientos correctivos los cuales consisten en atender en sitio los incidentes y/o problemas, realizar un diagnóstico de la causa de la falla e implementar una solución que puede requerir reinstalación de software o reparación o reemplazo parcial o total de alguno de los equipos o periféricos de la plataforma tecnológica, realizar las pruebas que garanticen la continuidad de la operación, documentar el caso y gestionar la suscripción del recibido a satisfacción por parte del usuario.

En los casos que las partes de los equipos puedan ser reparadas mediante el cambio de elementos electrónicos, eléctricos, mecánicos o electromecánicos entre otros, se deberá evaluar, definir y aplicar la mejor alternativa a fin de brindar los mejores tiempos de respuesta al usuario, bien sea reparando en sitio o solicitando el traslado a un laboratorio para su reparación en un tiempo no superior a quince (15) días calendario para retiro, reparación y devolución, con previa autorización del funcionario responsable del inventario y de la supervisión del contrato.

Procedimiento:

1. Realizar la sustitución del elemento averiado o defectuoso, por otro de idénticas o superiores características cuando el servicio de mantenimiento correctivo así lo requiera. Esta sustitución se realizará solamente después de ejecutar todas las pruebas necesarias y tener la seguridad de que la elemento no se puede reparar. En caso de que sea posible repararlo, EL CONTRATISTA procederá a efectuar dicha reparación.

2. Reemplazar la parte afectada en un máximo cuatro 4 días hábiles siguientes a la aprobación del repuesto. Adicionalmente, se deberá instalar una máquina de forma temporal para que el funcionario pueda seguir trabajando sin interrupción.
3. El daño de un elemento y su imposibilidad de reparación deberá ser aprobado por el supervisor del contrato, previa solicitud del repuesto en el software de administración de los servicios de atención y soporte a los usuarios finales a cargo del técnico nivel 2. Se deben enviar 3 cotizaciones para su respectiva autorización de compra por parte de la entidad. El tiempo máximo definido para realizar la solicitud de cotización (cambio de estado de "SOLICITUD DE REPUESTO" a "SOLICITUD DE COTIZACIÓN") después de la atención del servicio no debe exceder las dos (2) horas, y la entidad dispone de cuatro (4) días hábiles después de haber recibido las cotizaciones para aprobarlas o rechazarlas; este tiempo no se contabilizará.
4. Realizar la toma del Backup de datos de los archivos, cuando se trate de equipos de cómputo y el diagnóstico realizado por el técnico, así lo determine. Una vez realizada la reparación a la que haya lugar y la reinstalación del software (Sistema Operativo, herramientas de Office o el software de uso de la entidad) que resulte afectado, se debe proceder con la restauración del backup previamente tomado.
5. Formatear el disco duro del equipo reportado con inconvenientes, para los equipos de cómputo, según las necesidades y cuando así se requiera, previa autorización escrita del usuario. No obstante, lo anterior, ésta debe ser una alternativa final y se debe proponer su utilización sólo en casos excepcionales. Controlar y entregar al supervisor del contrato las partes dañadas y reemplazadas.
6. Los repuestos serán instalados sobre la base de canje (se retira el elemento dañado y se reemplaza por uno bueno). Por ningún motivo puede retirarse un equipo o parte de él sin que se deje su respectivo reemplazo.
7. Garantizar el correcto funcionamiento de las partes suministradas, reemplazadas o reparadas durante la ejecución del contrato. EI correcto funcionamiento significa entregar al usuario el bien en las mismas condiciones previas al daño que origino el servicio; es decir tiempos de respuesta, niveles de ruido, consumo de energía, compatibilidad con los suministros, etc.
8. Tiempo de reparación del bien: Solucionar la falla reportada dentro de las cuatro (4) días hábiles siguientes a la respuesta de la llamada.

9. Proveer un equipo del inventario de la JEP, mientras se resuelve el daño en equipo del funcionario.
10. Si dentro de treinta (30) días calendario siguientes a la atención de la llamada el bien no ha sido reparado, el contratista deberá reemplazarlo definitivamente por otro de iguales o superiores características, sin costo adicional para la JEP.
11. Cuando por razones de fuerza mayor se deba reemplazar por un equipo de una marca diferente, la JEP se reserva el derecho de aprobar o no el cambio.
12. Los criterios a tener en cuenta para determinar que el bien es de "iguales o superiores características" serán:
    a. Para microcomputadores
    b. Capacidad de memoria
    c. Tecnología y velocidad del procesador
    d. Capacidad de almacenamiento en disco
    e. Compatibilidad
    f. Apariencia física
    g. Características del monitor, teclado y mouse.
    h. Para impresoras
    i. Velocidad de impresión
    j. Compatibilidad de suministros
13. A la finalización del contrato no deberá quedar ningún servicio sin atender, equipo alguno sin reparar o sustituir. Las partes reemplazadas que tengan identificación (número de serie) deberán quedar debidamente legalizadas.
14. Responder por los vicios ocultos de los bienes que instale en desarrollo del mantenimiento correctivo con repuestos.
15. En la herramienta de atención de incidentes, que provee LA JEP se debe diligenciar como mínimo la siguiente información cuando se solicita el servicio:
    a. Número del servicio asignado automático por el sistema
    b. Fecha y hora del servicio asignado automático por el sistema
    c. Dependencia asignada por el sistema de acuerdo con los usuarios cargados
    d. Nombre del usuario
    e. Fecha y hora de la llamada asignada automáticamente por el sistema
    f. Tipo de falla: Hardware, Software, Aplicaciones, debe ser registrada por el técnico que atienda el requerimiento
    g. Nombre del Técnico asignado que atiende el incidente
    h. Dependencia y funcionario especialista de LA JEP, al que se escaló la llamada indicando la fecha y la hora en que se escaló y la solución dada

i. Tiempo (horas) empleado en la solución, lo calcula automáticamente el sistema.
j. Nombre del usuario que recibió a satisfacción

16. Criticidad de la falla:

a. Normal: el problema no afecta a más de un usuario y no genera mayor impacto en el desarrollo de sus labores.
b. Urgente: el problema afecta a un grupo de personas e impacta altamente los procesos.
c. Critica: el problema ocasiona la suspensión accidental de las operaciones del negocio o tiene un impacto significativo para LA JEP

Se debe presentar semanalmente a la supervisión del contrato, el informe del servicio correctivo detallado por equipo, modelo, ubicación, serial, descripción de la falla y fecha. Adicionalmente se deberá consolidar por tipos de fallas, ubicación, tipo de equipos, entre otros

Se excluyen únicamente: La provisión de insumos, entendidos estos como los bienes que tienen el carácter de suministro periódico y que se consumen con su uso, tales como tóner y cartuchos.

1.10 BOLSA DE REPUESTOS:

El Contratista deberá hacer un buen manejo adecuado de la bolsa de repuestos, procurando no sobrepasar los de **CIENTO OCHO MILLONES CIENTO SESENTA Y OCHO MIL QUINIENTOS OCHENTA PESOS ($108.168.580) M/CTE incluido IVA,** durante la ejecución del contrato garantizando la operación en mesa de ayuda. El uso de la bolsa de repuestos estará a cargo de la coordinación de la mesa de ayuda con la autorización por parte de la supervisión del contrato o su delegado.
La distribución del presupuesto para la bolsa de repuestos estará dada por vigencia de la siguiente manera.

VIGENCIA	VALOR CON IVA
2019	$ 1.971.588
2020	$ 7.886.352
2021	$ 7.886.352
2022	$ 90.424.288

Para adquirir las partes o repuestos que se requieran el proveedor deberá presentar tres (3) cotizaciones y los valores deberán obedecer al promedio del mercado. La JEP se reserva el derecho a verificar las cotizaciones con los precios del mercado o a obtener unas nuevas que se ajusten al precio del mercado.
Teniendo en cuenta la operación y el desempeño de este ítem, el porcentaje podrá ser revisado y ajustado de acuerdo con las necesidades de la Entidad, en caso de acumularse la bolsa de repuestos finalizando el contrato, se realizará una reunión para definir la inversión a realizar en equipos o elementos del servicio que se requieran.

Es importante que el Contratista entregue un informe mensual del consumo de la bolsa de repuestos para conocer su estado.

El tiempo máximo para la entrega, instalación y configuración del repuesto será al segundo día hábil siguiente de lo reportado.

En el caso de que el repuesto o parte sea muy costosos o de difícil consecución, El Contratista deberá presentar propuesta o alternativa que permitan tomar la decisión de actuar frente a la reposición o proceso de baja del activo de cómputo.

No se requiere contar con estos artículos en las instalaciones de la entidad, pero se debe tener la disponibilidad de suministrarlos al momento que lo requiera la operación de acuerdo con los ANS establecidos.

1.11 ACUERDOS DE NIVEL DE SERVICIOS (ANS):

Se establecen los siguientes Acuerdos de Nivel de servicio según la siguiente tabla resumen para el servicio en mesa de ayuda:

SERVICIOS	UNIDAD DE MEDIDA	META DEL INDICADOR	PERIODICIDAD DE ENTREGA INFORME
Atención de llamadas en un tiempo menor a 20 segundos	Porcentaje	>=95% en un tiempo menor a 20 segundos	Mensual

SERVICIOS	UNIDAD DE MEDIDA	META DEL INDICADOR	PERIODICIDAD DE ENTREGA INFORME
Abandono de llamadas en un tiempo mayor a 20 segundos	Porcentaje	<=2% en un tiempo mayor a 20 segundos	Mensual
Mesa de Ayuda – Tiempo máximo para la Asignación de Categoría y escalamiento de ticket o solución en primer nivel	Porcentaje	>=95% en un tiempo máximo de atención de 20 Minutos.	Mensual
Mesa de Ayuda - Tiempo de Solución	Porcentaje	>=95% y en un tiempo máximo de solución de acuerdo al tipo de solicitud y la prioridad asignada	Mensual
Soporte en Sitio - Tiempo de Solución	Porcentaje	>=95% y en un tiempo máximo de solución de acuerdo al tipo de solicitud y la prioridad asignada	Mensual
Gestión de Identidades – Tiempo de Solución	Porcentaje	>=95% y en un tiempo máximo de solución de acuerdo con el tipo de solicitud y la prioridad asignada	Mensual
Gestión de protección perimetral e incidentes de seguridad – Tiempo de Solución	Porcentaje	>=95% y en un tiempo máximo de solución de acuerdo con el tipo de solicitud y la prioridad asignada	Mensual

SERVICIOS	UNIDAD DE MEDIDA	META DEL INDICADOR	PERIODICIDAD DE ENTREGA INFORME
Soporte en medios audiovisuales – Tiempo de Solución	Porcentaje	>=95% y en un tiempo máximo de solución de acuerdo con el tipo de solicitud y la prioridad asignada	Mensual
Informes de Operación y Gestión	Porcentaje	>=98% Cumplimiento de los entregables de Informes	Mensual

El Proponente, teniendo como base los indicadores de servicio descritos, reportará la gestión del factor de calidad y cumplimiento de la operación de la Mesa de Ayuda. La JEP validará el resultado y aplicará la penalización al pago mensual del rubro de mesa de ayuda acorde con la siguiente tabla de resarcimientos si no se soporta y justifica a satisfacción las causales de incumplimiento:

		Descuentos	
Indicador	**Meta**	**Rango**	**Valor**
Atención de llamadas	≥95%	90%-94,99%	2%
		85%-89,99%	3%
		<85%	5%
Abandono de llamadas	<=2%	2%-2,99%	2%
		3%-3,99%	3%
		>4%	5%
Mesa de Ayuda – Tiempo máximo para la Asignación de Categoría y escalamiento de ticket o solución en primer nivel	≥95%	90%-94,99%	2%
		85%-89,99%	3%
		<85%	5%
Mesa de Ayuda - Tiempo de Solución	≥95%	90%-94,99%	2%
		85%-89,99%	3%
		<85%	5%
	≥95%	90%-94,99%	2%

Soporte en Sitio - Tiempo de Solución		85%-89,99%	3%
		<85%	5%
Gestión de Identidades - Tiempo de Solución	≥95%	90%-94,99%	2%
		85%-89,99%	3%
		<85%	5%
Gestión de protección perimetral e incidentes de seguridad - Tiempo de Solución	≥95%	90%-94,99%	2%
		85%-89,99%	3%
		<85%	5%
Soporte en medios audiovisuales - Tiempo de Solución	≥95%	90%-94,99%	2%
		85%-89,99%	3%
		<85%	5%
Informes de Operación y Gestión	≥98%	93%-97,99%	2%
		88%-92,99%	3%
		<88%	5%

El valor máximo penalizado por incumplimiento de ANS no excederá del 9% del valor total mensual del servicio facturado en caso de pérdida de tres o más indicadores en el mes, se iniciará proceso de incumplimiento de acuerdo con lo señalado en el Manual de Contratación.

NOTA 1: Los ANS serán ajustados a solicitud del supervisor de acuerdo como se establezcan los tiempos de solución configurados en las herramientas.

NOTA 2: Los ANS se verificarán a partir del inicio del contrato, pero durante el periodo de estabilización (2 meses) no serán sujetos de penalización.

2. SOLUCIÓN DE GESTIÓN DE SERVICIOS DE TI

REQUISITOS TÉCNICOS HABILITANTES HERRAMIENTA ITSM

La herramienta deberá estar certificado en los procesos ITIL 2011 versión 3, como mínimo debe contar con los siguientes ocho (8) procesos, con certificación Pink Verify 2011.

- Gestión de Activos de Servicio y Gestión de la Configuración o SACM (Service Asset & Configuration Management)

- Gestión del Catálogo de Servicios o SCM (Service Catalog Management)
- Cumplimiento de la Solicitud o RF (Request Fulfillment)
- Gestión de Incidentes o IM (Incident Management)
- Gestión de Problemas o PM (Problem Management)
- Gestión del Nivel de Servicio (SLM) o SLM (Service Level Management)
- Gestión de Cambios o CHG (Change Management)
- Gestión del Conocimiento o KM (Knowledge Management)

La solución debe estar dentro del cuadrante mágico de Gartner para herramientas ITCM de Julio de 2019, en la ubicación de líderes.

2.1 REQUISITOS GENERALES QUE DEBEN SER SOPORTADOS POR LA HERRAMIENTA

- La herramienta ofertada deberá integrarse con la solución propuesta para realizar el Gobierno y Administración de Identidades y Acceso Unificado (IDM-SSO).
- La herramienta ofertada debe poder configurarse mediante protocolo IPv6 o IPv4 con futura migración a IPv6 y así mismo soportar la comunicación con otros componentes de la arquitectura empresarial basados en estos 2 esquemas de direccionamiento.
- La herramienta y todos sus módulos deberán ser instalados localmente ("on premise") en los servidores que para tal fin asigne el contratante. No se aceptarán soluciones de "Software como Servicio" o SaaS.
- Todo el licenciamiento suministrado para habilitar cada uno de los componentes ofertados en la herramienta deberá quedar a nombre de la entidad contratante y su vigencia deberá ser a perpetuidad.
- El licenciamiento suministrado para la herramienta ofertada y todos sus módulos debe permitir el uso para 20 usuarios administradores y/o operadores, la atención de un mínimo 1.300 usuarios finales que puedan solicitar servicios de mesa de ayuda y el manejo sin restricciones de las bases de datos asociadas a los demás componentes.
- Todos los módulos que compongan la herramienta ofertada deberán utilizar la misma plataforma, ser parte de la misma suite y ser integradas nativamente.
- La herramienta ofertada deberá manejar un esquema de alta disponibilidad con tolerancia a fallas. Como el manejo del concepto de granja de servidores. La solución soportada deberá soportar bases de datos "Unicode".

- La herramienta ofertada deberá accederse a través del Web a través de interfaces como Java o HTML5.
- La herramienta ofertada deberá contar con interfaz en español con posibilidades de manejo de inglés de manera adicional.

- La herramienta ofertada deberá tener la capacidad arquitectónica de separar las capas Web, Aplicación y Datos en diferentes instancias de Hardware para contar con un mejor rendimiento.
- La herramienta ofertada deberá contar con la capacidad de ser monitoreada a través de traps de SNMP para que los eventos generados por la herramienta sean enviados a consolas de monitoreo para monitorear su disponibilidad y salud.
- La herramienta ofertada deberá contar con funcionalidad que permita acelerar las auditorías de cumplimiento.
- La herramienta ofertada deberá contar con la posibilidad de realizar mantenimiento de la base de datos sin afectar la data y la configuración de esta con el fin de garantizar un óptimo funcionamiento y rendimiento de la aplicación.
- La herramienta ofertada deberá permitir la Integración directa con otras herramientas complementarias de los procesos de las mejores prácticas de ITIL.
- La herramienta ofertada deberá enviar notificaciones de forma grupal o individual.
- La herramienta ofertada deberá permitir la generación personalizada de identificadores y grupos de identificadores para cada uno de los elementos de información claves que hacen parte de los módulos de la herramienta, como ID de incidentes, ID problemas, ID de acuerdos, ID de peticiones de cambio, ID de solicitudes de servicio, etc.
- La herramienta ofertada debe permitir la generación de informes bajo formatos predefinidos, así como su distribución automatizada y distribuirlos automáticamente. Los reportes deben poder ser exportados a formatos tales como Excel, HTML, PDF, DOC, XML y generar gráficos configurables por el usuario exportables a cualquier plataforma.
- Los informes deben entre otros poder ser configurados para que permitan la identificación de áreas en que no se cumplen los niveles de servicio propuestos y las gestiones realizadas.
- La herramienta ofertada debe ser compatible con servidores, estaciones de trabajo, computadoras portátiles, tabletas y dispositivos móviles que se basa en

HTML 5, que permite que cualquier dispositivo con un navegador utilice la herramienta.

- La herramienta ofertada debe ser una solución de acceso a través de dispositivos móviles basa en HTML 5, que permita que cualquier dispositivo con un navegador utilice la herramienta o aplicación nativa.
- La herramienta ofertada debe permitir gestionar, definir, mejorar y automatizar procesos. La automatización puede lograrse mediante flujos de trabajo o algún método similar.
- La herramienta ofertada debe disponer de un calendario de soluciones disponible para la fecha de vencimiento de la solución del caso por medición del SLA para el personal técnico.
- La herramienta ofertada debe el tipo de incidente o solicitud, debe permitir crear campos adicionales para obtener información adicional basada en un criterio, tema, área de solicitud, etc.
- La herramienta ofertada debe permitir crear formularios para capturar los datos requeridos (para incidentes o solicitudes).

2.2 PROCESOS ITIL QUE DEBEN SER SOPORTADOS POR LA HERRAMIENTA

2.2.1 Gestión de Activos de Servicio y Gestión de la Configuración o SACM (Service Asset & Configuration Management)

El objetivo principal del Proceso de Gestión de Activos y Configuración de Servicios ITIL (ITIL SACM) es identificar, documentar y administrar todos los Elementos de Configuración (CI) necesarios para la entrega de servicios de TI, incluidas sus relaciones y dependencias.

Requisitos:

- La herramienta ofertada debe permitir la identificación, control, registro reporte, auditoria, y verificación de cada atributo de los servicios de TI y otros elementos de configuración (CI), como versiones, líneas base, componentes constitutivos y relaciones.
- La herramienta ofertada debe permitir administrar y proteger la integridad de los CI a través del ciclo de vida del servicio trabajando en estrecha colaboración

con los módulos de gestión de cambios y asegurando que solo se usen los componentes autorizados y solo se implementen los cambios autorizados.

- La herramienta ofertada debe permitir mantener la integridad de los activos de servicio y los elementos de configuración estableciendo y manteniendo una base de datos de administración de configuración (CMDB) precisa y completa y un sistema de administración de configuración (CMS).

- La herramienta ofertada debe permitir mantener actualizada la información de configuración, el historial, estado actual y estados planeados de los servicios de ti y otros CI.
- Todos los módulos o aplicaciones de la herramienta deberán de integrarse de manera nativa a la base de datos de gestión de configuraciones (CMDB), siendo este un módulo independiente del resto y dedicado a las funciones propias de una CMDB.
- La herramienta ofertada debe permitir conocer y descubrir de forma automática, por integración con otras herramientas, desde el Active Directory/LDAP y por carga de archivos la información completa y actualizada de los recursos de hardware, software y dispositivos instalados o asociados por cada estación de trabajo y servido con el fin de configurar las bases de datos de activos y gestión de configuraciones (CMDB).
- Debe permitir rastrear el inventario automático basado en WMI (cualquier computadora con Windows) para mostrar la instalación de hardware en la computadora.
- La herramienta ofertada debe permitir conocer las actividades realizadas y el registro de esta en cada uno de los dispositivos, informando registrando el personal que las realizó

2.2.2 Gestión del Catálogo de Servicios o SCM (Service Catalog Management)

El objetivo principal del proceso de administración del catálogo de servicios de ITIL es garantizar que se produzca, mantenga y contenga información precisa sobre todos los servicios operativos y aquellos que están preparados para ejecutarse operacionalmente.

Este proceso también es responsable de proporcionar información vital, como los detalles del Servicio, el estado actual y las interdependencias del servicio, para todos los demás procesos de Gestión del Servicio.

Requisitos:

- La herramienta deberá soportar la creación, documentación, mantenimiento y publicación de un catálogo de servicios de servicio actuales y futuros con:
    - La descripción de las características de la oferta de cada servicio, sus funciones y beneficios en términos de los procesos de la entidad.
    - Soportar opciones de niveles de servicio y niveles de disponibilidad comprometidos.
    - Niveles de precio y costeo asociados a los niveles de servicio seleccionados.
    - Incluir componentes de servicio y sus atributos.
- La herramienta deberá organizar los servicios en grupos lógicos o estructuras jerárquicas las cuales puedan ser empleadas para reunir los servicios a los clientes en paquetes/ofertas relevantes al negocio.
- La herramienta ofertada debe permitir contar con una interfaz con el proceso de gestión del portafolio de servicios para sincronizar los contenidos de portafolio de servicios y catálogo de servicios.
- La herramienta ofertada debe sincronizarse con las demás herramientas de la solución, tales como la base de datos de gestión de configuraciones y gestión de niveles de servicio (Service Level Management – SLM) para garantizar que la información en el catálogo de servicios esté alineada con los objetivos de la entidad.
- La herramienta deberá facilitar la capacidad de publicar diferentes niveles del mismo servicio.
- La herramienta deberá facilitar vistas basadas en roles del catálogo de servicios tomando en cuenta las siguientes consideraciones:
    - Contar con una vista de TI para el diseño de servicios, gestión de niveles de servicio y abastecimiento de solicitudes de servicio.
    - Contar con una vista de usuario que incluya los servicios que un usuario en específico tiene acceso.

- La herramienta ofertada debe proveer la capacidad de desplegar el catálogo de servicio vía una interfaz Web que permita a los usuarios el uso del catálogo de servicio localizar de una manera sencilla las ofertas de servicio y/o sus componentes.
- La herramienta deberá permitir la gestión del estado del ciclo de vida de los servicios. Por ejemplo, diferencia Diseño, Transición, Producción, etc.
- La herramienta deberá facilitar una gestión de Catálogo de Servicios distribuida basada en roles. Esto deberá incluir diferentes aspectos de configuración y mantenimiento del catálogo por diferentes roles, ejemplo: Rol de Administrador de Correo, etc.
- De igual manera los elementos de configuración podrán ser asociados o referenciados a los servicios contenidos en el catálogo de servicios. De esta manera un incidente registra el servicio afectado y también desde un servicio pueden verse los incidentes que tuvo

2.2.3 Cumplimiento de la Solicitud o RF (Request Fulfillment)

El proceso de cumplimiento de solicitud de ITIL es responsable de administrar el ciclo de vida de todas las solicitudes de servicio recibidas de los usuarios. Este proceso también es responsable de cumplir con varios tipos de solicitudes planteadas a la mesa de servicio y de cumplir exactamente lo que se solicita.

Según ITIL v3, una solicitud de servicio (o solicitud de servicio) es "una solicitud de un usuario para obtener información, asesoramiento, un cambio estándar o acceso a un servicio".

El objetivo principal del proceso de cumplimiento de solicitudes de ITIL es cumplir con las solicitudes de servicio planteadas por los usuarios para tomar varios servicios de apoyo, que en la mayoría de los casos son cambios menores (estándar).
Requisitos:

- La herramienta deberá integrarse con el módulo propuesto de gestión de solicitudes de servicio de forma bidireccional. Las solicitudes de servicio podrán asociarse a los servicios contenidos en el catálogo de servicios.
- La herramienta deberá facilitar la creación de reglas de negocio definidas por los usuarios y la automatización del flujo de trabajo para revisión, aprobación y asignación de solicitudes contra los servicios publicados, en la que se pueda indicar como mínimo:

- El responsable de la solicitud, quien podrá ser una persona o un grupo.
- Los pasos y aprobaciones que se deben seguir para entregar el servicio requerido.
- Los acuerdos de nivel de servicios aplicables para el tipo de solicitud.
- El escalamiento que se debe realizar cuando el servicio no se puede cumplir por su alcance o por el tiempo transcurrido.

- La herramienta ofertada debe permitir al usuario final ingresar una solicitud por varios medios, como vía acceso web o enviar un correo electrónico al sistema para que sus solicitudes se gestionen por los administradores y contar con la capacidad para crear automáticamente casos y aplicar reglas de negocios, reglas de TI, así como políticas y acuerdos de nivel de servicio (SLA).
- La herramienta ofertada debe integrarse con los demás módulos de la solución, gestión de catálogo de servicios y gestión de nivel de servicio con el fin de poder ofrecer a los usuarios solicitantes la información sobre los servicios disponibles y tiempos de entrega.
- La herramienta ofertada debe integrarse con el módulo de gestión del conocimiento con el fin de que las reglas, flujos y procedimientos programados cuenten con mecanismos para detallar el alcance de estos y documentar las mejoras que puedan surgir en su realización.
- La herramienta ofertada debe generar mediciones personalizadas sobre los tiempos de entrega de los servicios, ofrecer encuestas y la capacidad de que los usuarios califiquen si nivel de satisfacción frente a los servicios prestados y que puedan hacer peticiones, quejas o reclamos sobre los mismos.

2.2.4 Gestión de Incidentes o IM (Incident Management)

El objetivo principal del proceso de gestión de incidentes de ITIL es restaurar el servicio de TI a su estado normal lo más rápido posible. Se utiliza para administrar el ciclo de vida de todos los incidentes (interrupciones no planificadas o reducciones en la calidad de los servicios de TI o fallas de los componentes).

Requisitos:

- La herramienta ofertada debe contar con un módulo de gestión de incidentes y la programación de reglas de negocio que permitan:

    - El registro y categorización de incidentes.
    - El reporte proactivo a partes y usuarios afectados.
    - Aplicar medidas correctivas de primer nivel de soporte.
    - Realizar el escalamiento a los niveles de soporte superiores.
    - Permitir el manejo de incidentes mayores y gestiones alternativas.
    - Monitorear el estado de cada incidente y alertar sobre su evolución y escalamiento realizado a otros usuarios.
    - Hacer el cierre del incidente y permitir el registro de todo el ciclo de vida del incidente.
    - Generar reportes automáticos personalizados sobre la gestión de incidentes.

- La herramienta ofertada debe permitir la programación de procedimientos de solución automáticos o semiautomáticos de problemas y fallas de disponibilidad; se deben mostrar tableros de control por tipos de eventos y tendencias, así como el cálculo de indicadores de disponibilidad y verificar el cumplimiento de los SLA asociados.
- La herramienta ofertada debe contar con plantillas para la creación de incidentes definidos, que permiten resolver incidentes de manera eficiente y ofrecer criterios para la categorización de los tipos de incidentes para una mejor recopilación de datos y gestión de problemas.
- La herramienta ofertada debe gestionar de manera automática o semiautomática todo el ciclo de vida de los incidentes y su estado (Nuevo, asignado, en progreso, en espera, resuelto, en observación, cerrado).

- La herramienta ofertada debe permitir hacer priorización a los incidentes:

    - Incidente de alta prioridad: afecta a un gran número de usuarios o clientes, interrumpe o afecta la prestación de servicios y generalmente tiene un impacto financiero.
    - Incidente de prioridad media: afecta a algunos miembros del personal (o grupo) e interrumpe el trabajo hasta cierto punto. Los usuarios pueden verse ligeramente afectados o incomodados.

- Incidente de baja prioridad: incidentes menores que no tienen impacto o tienen poco impacto en el usuario único y tienen soluciones instantáneas.

- El componente de gestión de incidente deberá estar integrado a los demás componentes de la herramienta ofertada, en especial con:
  - El componente de gestión de cambios, para aquellos incidentes que requieran un cambio para su solución o que sean causados por la realización de cambios.
  - El componente de gestión de problemas para hacer uso y alimentar la base de datos de errores conocidos (Known Error Database - KEDB).
  - Bases de datos de infraestructura, aplicaciones y/o base de datos de gestión de configuraciones (CMDB) con el fin de identificar las relaciones entre los componentes del servicio y detectar cualquier evento de manera que estos puedan ser categorizados y se permita la creación automática de incidentes.
  - El componente de gestión de nivel de servicio para su invocación y tomar información de este.

2.2.5 Gestión de Problemas o PM (Problem Management)

El objetivo principal del proceso de gestión de problemas de ITIL es evitar que ocurran incidentes y minimizar el impacto de incidentes que no se pueden evitar.

Requisitos:

- La herramienta ofertada debe permitir identificar problemas ya sea a partir de incidentes recurrentes o incidentes puntuales que puedan desencadenar problemas conociendo su causa raíz y estableciendo el ciclo de vida del problema logrando gestionar cada caso de manera eficiente desde la definición de su origen, clasificación, enrutamiento, investigación y resolución permanente del problema aplicando tales soluciones a incidentes similares.

- La herramienta ofertada debe contar con una base de datos de errores conocidos (Known Error Database - KEDB) para ser mantenida con las soluciones previamente identificadas, considerando las cosas que se hicieron correctamente, que se hicieron mal, mejoras a futuro, evitar nuevos problemas similares y documentar las lecciones aprendidas.

- La herramienta ofertada debe estar integrada a los demás componentes de la solución, pero en especial debe integrarse con:
    - El componente de gestión de cambios, para aquellos problemas que requieran o que sean causados por la realización de cambios.
    - Los componentes de gestión de incidentes y eventos para poder relacionar los problemas detectados con categorías de estos.
    - Las bases de datos de infraestructura, aplicaciones y/o base de datos de gestión de configuraciones (CMDB) con el fin de identificar las relaciones entre los componentes implicados en los problemas analizados y sus soluciones.
    - El componente de gestión del conocimiento.

2.2.6 Gestión del Nivel de Servicio (SLM) o SLM (Service Level Management)

El objetivo principal del proceso de Gestión del nivel de servicio de ITIL es negociar acuerdos de nivel de servicio (SLA) con los clientes y diseñar servicios de acuerdo con los objetivos de nivel de servicio acordados.

Este proceso de ITIL SLM también es responsable de monitorear e informar los niveles de servicio actuales y también asegura que todos los Acuerdos de Nivel Operativo y los Contratos de Apoyo sean apropiados para lograr los objetivos de SLA.

Requisitos:

- La herramienta ofertada debe permitir registrar el registro de todos los Acuerdos de Nivel de Servicio (SLA), Acuerdos de Nivel Operacional (OLA) y Contratos de Apoyo (UC) relacionados con todos los componentes de servicio y los proveedores asociados.
- La herramienta deberá facilitar la automatización y el control de contratos de proveedores y acuerdos con proveedores terceros.
- La herramienta deberá permitir la gestión de la programación del ciclo de revisión y renovación de SLA's, OLA's y contratos de proveedores.
- La herramienta ofertada debe considerar horarios de oficina, días festivos y 'times-out' del personal dentro de la definición de los acuerdos.

- La herramienta deberá soportar el monitoreo y gestión de las métricas de acuerdos de nivel operacional y con proveedores.
- La herramienta deberá permitir la gestión y automatización de metas de nivel de servicio en términos de reglas de negocio automatizadas, alertas, escalamiento y notificaciones.
- La herramienta deberá facilitar la presentación de informes contra los requerimientos de SLA. Por ejemplo, los informes de logros de servicios contra SLA´s, informes de las razones infracciones de los Acuerdos de Nivel de Servicio e informar de excepciones contra los SLA's.
- La herramienta deberá integrarse con los demás componentes de la solución, en especial con los componentes de Gestión de incidentes, gestión de Requerimientos, gestión de Cambios y gestión de problemas para garantizar que se logren la calidad y los niveles de servicio requeridos utilizando los recursos acordados para una adecuada gestión financiera.

2.2.7 Gestión de Cambios o CHG (Change Management)

El objetivo principal del proceso de gestión de cambios de ITIL es controlar cada cambio a lo largo del ciclo de vida de gestión de cambios. El objetivo es facilitar que se incorporen cambios beneficiosos, con una interrupción mínima de los servicios de TI.

Otros objetivos son aportar claridad sobre el resultado del cambio antes de que se implemente y permitir el uso económico de los recursos involucrados en un proceso de cambio.

Requisitos:

- En la herramienta se deberá visualizar de una forma sencilla y grafica las fases por las que pasa un cambio durante su ciclo de vida.

- La herramienta deberá tener una sección para el registro de los detalles de la petición de cambio, tales como
- En la herramienta se deberá tener una sección donde se pueda registrar los datos del usuario que registra la petición del cambio, así como la información del lugar donde se efectuará el cambio y la persona quien solicita el cambio.

- La herramienta deberá permitir de realizar una clasificación de la solicitud de cambio, como el tipo, razón del cambio, justificación de negocio, ambiente del cambio.
- La herramienta deberá contar con la posibilidad de agregar información necesaria para cada petición de cambio.
- La herramienta ofertada debe guardar automáticamente el tiempo y hora de registro del cambio.
- La herramienta deberá solicitar las fechas de petición para el cambio y deberán de ser obligatorias para el registro del cambio.
- La herramienta deberá permitir crear relaciones de manera rápida y concisa entre el cambio y otros módulos o las áreas impactadas o los elementos de configuración impactados por el cambio.

- La herramienta deberá estar basada en las mejores prácticas de ITIL para el cambio de los estados de las peticiones de cambio, solicitando en algunos de ellos una razón de estado.
- La herramienta deberá proporcionar la opción de asignar a un administrador del cambio, un asignado al cambio y un implementador del cambio.
- La herramienta ofertada debe proporcionar la capacidad de configurar autorizadores durante las distintas fases de aprobación por las que pase un cambio.
- La herramienta deberá proporcionar la facilidad de configurar autorizaciones del comité de cambios, tal y como lo señala ITIL.
- La herramienta deberá proporcionar la facilidad para configurar diversos esquemas de aprobación, como definir si va a ser un aprobador en específico o si puede ser variante.
- La herramienta deberá permitir configurar aprobaciones para determinados tipos de cambios en los cuales se requiera una aprobación más.
- Durante la fase de alguna aprobación necesaria la herramienta deberá permitir rechazar la petición de cambio y en esté deberá verse reflejado con un estatus de Rechazado.
- La herramienta también deberá dar la oportunidad de agregar aprobadores alternos de forma manual durante la fase que se esté aprobando.
- En la herramienta deberá existir una forma de identificar los usuarios que han aprobado o rechazado el cambio.

- La herramienta deberá facilitar la acción de aprobar o rechazar un cambio, ya sea utilizando una interfaz gráfica adicional o contando con una sección dedicada únicamente a las aprobaciones de cambios.
- La herramienta deberá permitirle al aprobador la posibilidad de agregar comentarios al cambio que se desea aprobar.
- En la herramienta deberá permitir registrar las fechas programadas para la implementación del cambio.
- La herramienta deberá contar con un candelario de cambios en el cual se pueda observar los cambios programados.
- La herramienta deberá validar las fechas de solicitud del cambio con las fechas de programación del cambio.
- La herramienta deberá brindar la posibilidad de asignar una tarea específica relacionada con el cambio ya sea hacia una persona o un grupo en específico.

- La herramienta deberá llevar el registro del tiempo que se ha invertido en un cambio.
- La herramienta deberá permitir agregar información adicional durante la implementación del cambio.
- La herramienta deberá brindar opciones de Asignación Automática de cambios a los grupos administradores e implementadores.
- La herramienta deberá notificar automáticamente a los usuarios implicados cuando se registre una nueva petición de cambio.
- La herramienta deberá permitir realizar notificaciones de forma manual con los detalles del cambio.
- La herramienta deberá enviarle una notificación al usuario responsable para la aprobación del cambio.
- La herramienta ofertada debe considerar horarios de oficia, días festivos y 'times-out' del personal de soporte durante la asignación de cambios.
- La herramienta deberá permitir el uso de indicadores de Impacto, Urgencia y el nivel de riesgo para la clasificación de los cambios y estos deben estar relacionados con los objetivos de servicios en los SLA´s y OLA´s establecidos dentro de las áreas operativas y usuarios finales respectivamente.
- La herramienta deberá integrarse con los demás componentes de la solución, en especial con los componentes de:
  - Gestión de activos y configuración de servicios, en especial base de datos de administración de configuración (CMDB)

- Gestión de incidentes y la gestión de problemas en caso de que necesiten implementar cambios para resolver cualquier problema crítico.
- Gestión de Ediciones e Implementación para realizar un seguimiento de los cambios realizados entre dos cambios de lanzamiento consecuentes.
- Gestión de niveles de servicio para asegurar el cumplimiento de SLA durante el proceso.

2.2.8 Gestión del Conocimiento o KM (Knowledge Management)

El objetivo principal del proceso de gestión del conocimiento de ITIL es recopilar, analizar, almacenar y compartir conocimientos e información dentro de una organización. También reduce la necesidad de redescubrir el conocimiento, por lo tanto, mejora la eficiencia del servicio.

Este proceso también es responsable de mantener el sistema de gestión del conocimiento del servicio (SKMS), que simboliza el cuerpo total de conocimiento dentro de la organización. Aquí el objetivo es capturar, organizar, clasificar y almacenar cada bit de conocimiento organizacional y ponerlos a disposición donde sea necesario.

Requisitos:

- La herramienta ofertada debe contar con facilidades que le permitan construir y mantener un sistema de gestión del conocimiento del servicio (SKMS) a nivel especializado para soportar el trabajo de especialistas de la dirección de tecnología como para los usuarios de los servicios de TI.

- El SKMS debe integrarse con otras bases de datos críticas de la herramienta ofertada como:

    - Configuration Management Database (CMDB)
    - Known Error Database (KEDB)
    - Configuration Management System (CMS)

- La herramienta ofertada debe tener la capacidad de mantener procedimientos de solución de problemas, guías de capacitación, preguntas frecuentes y vincularlas a tickets o ponerlas a disposición de los usuarios finales para ayudar a resolver

problemas por medio de FAQs sin acudir a la mesa de servicio. Estos artículos deberán ser aprobados, clasificados y publicados, dependiendo del tipo de información que contengan. Estos artículos pueden ser de consulta pública o privada, con la opción de calificación por parte del usuario.

- La herramienta ofertada debe integrarse con los demás componentes de la solución para proporcionar conocimiento de soporte a todos los procesos.

2.3 SERVICIOS ASOCIADOS A LA IMPLEMENTACIÓN DE LA HERRAMIENTA

2.3.1 IMPLEMENTACIÓN

El oferente deberá realizar la implementación de la herramienta en las siguientes fases:

Fase 1 - Procesos ITIL:

- Gestion de Solicitudes o RF (Request Fulfillment)
- Gestión de Incidentes o IM (Incident Management)
- Gestión del Nivel de Servicio (SLM) o SLM (Service Level Management)
- Gestión de Cambios o CHG (Change Management)
- Gestión del Conocimiento o KM (Knowledge Management)

2.3.2 PERFIL DEL IMPLEMENTADOR

- El implementador debe ser ingeniero de sistemas o electrónico con mínimo tres (3) años de experiencia profesional.

El implementador deberá haber participado como mínimo en 2 proyectos de implementación de la herramienta ofertada y preferiblemente contar con certificación en ITIL Practitioner o superior.

2.3.3 SOPORTE Y ACTUALIZACIONES

- La herramienta ofrecida deberá contar con un esquema de soporte remoto a nivel telefónico, por chat y por correo electrónico en español para tratar con cualquier

duda que surja en relación con la instalación y operación de la herramienta con disponibilidad 7 x 24.

- Todas las actualizaciones liberadas por el proponente durante la vigencia del contrato para cada uno de los componentes de la herramienta ofertada deberán ser suministrados e instalados sin costo adicional para el contratante.

3 SOLUCIÓN DE SEGURIDAD ENFOCADO A LA ADMINISTRACION Y GOBIERNO DE USUARIOS Y SESION UNIFICADA (IGA)

3.1 ESPECIFICACIONES TÉCNICAS IGA, GOBIERNO Y ADMINISTRACION DE IDENTIDADES

La solución requerida debe cumplir con los siguientes requisitos:

1. La herramienta y/o software para administrar y gobernar las identidades y accesos para 7 diferentes aplicaciones de la JEP. Las características técnicas que deberá cumplir se encuentran detalladas en la Matriz de Especificaciones Técnicas.
2. Aconsejar, sugerir, recomendar y proponer acerca de cómo estructurar la Gestión de Identidad y Acceso en la JEP para las aplicaciones que se integrarian en el presente proceso.
3. El servicio de implementación y puesta en funcionamiento de la herramienta y/o software ofrecido con todas las funciones requeridas.
4. Servicio de transferencia de conocimiento al personal de JEP.
5. La solución debe estar dentro del cuadrante mágico de Gartner para Identity governance and Administration (IGA) de febrero 2018, en la ubicación de líderes.
6. La herramienta debe ser IPV6 o IPV4 con futura migración a IPV6. Se debe entregar el cronograma con la posible fecha de migración no mayor al 31 de diciembre del 2020.
7. Licenciamiento mínimo para 1300 usuarios de la JEP.

3.1.1 Análisis a realizar

Previamente al proceso de implantación del sistema es necesario realizar el levantamiento de información respecto a las necesidades de accesos según las

funciones de cada área de la organización, lo anterior con el fin de aconsejar, sugerir, recomendar, así como de proponer a la JEP mediante documento escrito la estructuración de la Gestión de Identidad y Acceso en la entidad.

Las características de la propuesta de solución son:

- La administración de accesos basada en Roles y Perfiles para el otorgamiento de accesos a todas las plataformas tecnológicas.

- Contar con los controles necesarios para lograr una eficiente administración de las identidades, aprovisionamiento de usuarios y el acceso: auditoría, monitoreo y seguimiento de la seguridad.

- Los componentes de la solución estarán integrados en forma nativa tanto para la solución de IGA y Sesión Unificada, con la finalidad de prevenir sobre costos en la administración de la seguridad, además de prevenir brechas de seguridad provenientes de la implantación de soluciones de seguridad aisladas.

- La solución deberá apalancar la certificación de la JEP en la norma ISO 27001 en el dominio de Control de Accesos.

3.2 MATRIZ ESPECIFICACIONES TÉCNICAS IGA

CONSIDERACIONES	El oferente deberá informar el hardware requerido con el software de base requerido (sistema operativo, web server, web application server, bases de datos, etc.) para que la solución a implementar pueda dar respuesta a todos los requerimientos, ya sea en Producción como en ambientes de Testing y Desarrollo (Especificar).
	La solución debe estar desarrollada y ser propiedad de un mismo fabricante.
	La solución debe tener más de 5 años en el mercado.
	Integrarse con siete (7) aplicaciones de la entidad al término del contrato.

	El oferente y los miembros del equipo asignado al proyecto deben tener como mínimo dos (2) años de experiencia en proyectos similares en Colombia. La herramienta debe ser capaz de crear, modificar, eliminar usuarios en las aplicaciones mencionadas.
	La herramienta debe proveer un portal de autoservicio para los usuarios en donde se realizarán las solicitudes de accesos a las aplicaciones integradas, así como la recuperación de la contraseña de los usuarios.
	La solución debe poder ser instalada y configurada en Appliance Virtual con el fin de ahorrar costos de sistemas operativos.
	La herramienta debe ser capaz de crear, modificar, eliminar usuarios en las aplicaciones mencionadas. Acceso completo a todas las funcionalidades requeridas para usuarios finales en el presente pliego relacionadas a autogestión.
	El cliente para el usuario final debe contar con las siguientes funcionalidades: • Acceso completo a todas las funcionalidades requeridas para usuarios finales en el presente documento relacionadas a Password self service. • Acceso completo a todas las funcionalidades requeridas para usuarios finales en el presente documento relacionadas a Solicitud de accesos y recursos por workflows. • Acceso completo a todas las funcionalidades requeridas para usuarios finales en el presente documento relacionadas a autogestión.
CONTROL DE CALIDAD Y LIMPIEZA DE PRIVILEGIOS	• La solución debe soportar un repositorio de identidades de todas las aplicaciones de TI.
SOFTWARE DE BASE	• La herramienta de administración debe ser Web, deberá ser multiplataforma, soportando como mínimo alguna las siguientes plataformas:

	- Linux Server - Windows Server • En el caso de que la arquitectura técnica ofertada incluya funcionalidades de base de datos (para workflows o auditoría), las mismas deben ser del tipo relacional. La solución debe ser compatible con al menos alguna de las siguientes bases de datos: - MS SQL SERVER - Oracle, etc • La herramienta de administración debe ser Web, adaptable de manera automática a los diversos dispositivos (tipo responsive) y soportar los siguientes navegadores (especificar versiones soportadas en cada caso): - Internet Explorer - Safari - Firefox - Chrome

FUNCIONALIDADES DE APROVISIONAMIENTO	La solución debe permitir sincronización de contraseñas en plataformas tales como Windows, Linux, etc. • La solución debe poder administrar no solo el provisioning de cuentas o accesos a sistemas, de manera sincronizadas con el componente. • La sincronización de contraseñas debe ser en tiempo real, es decir en el momento que el usuario cambio su contraseña (Por ejemplo, en AD) y no mediante un proceso de reconciliación programado. • La solución debe soportar la sincronización de usuarios, grupos y cualquier otro tipo de objetos (ej: dispositivos, cuentas, organizaciones, áreas, etc.) • Debe permitir la asociación de cuentas con nombre diferente en los sistemas conectados • Debe permitir la detección de cuentas para asociar por medio de otros atributos que no sean el nombre de la cuenta • Las gestiones realizadas en los sistemas integrados deben sincronizarse en tiempo real, y debe soportar también procesos de reconciliación y/o verificación programados. • El motor de provisioning debe permitir definir "equipos de trabajo" (más allá de las relaciones jerárquicas). • El motor de provisioning debe soportar el concepto de "Jobs". Por ejemplo, la ejecución de tareas programadas de provisioning, cambio de contraseñas • La solución debe detectar de manera automática los esquemas de objetos existentes en las plataformas / aplicaciones a integrar.
INTERFAZ	• La solución debe tener una administración web online de las aplicaciones integradas que permita:

	• Administrar/Integrar múltiples aplicaciones desde un único lugar (tanto predefinidos como dinámicos) • Manejar múltiples cuentas, grupos y atributos de conectores dinámicos definidos 'adhoc' por el usuario • Tener un control granular de relaciones entre cuentas y grupos • Explorar los contenidos de un endpoint, correlacionar las cuentas • Definir tipos de aplicaciones • La interfaz del usuario debe poder ser customizada en forma simple y fácil, permitiendo a la organización cambiar la estructura de las páginas (encabezamiento, pie de página). También utilizar los logos institucionales. • La solución debe permitir que los usuarios autogestionen sus contraseñas a través de la consola WEB de la solución.
AUTOSERVICIO DE CONTRASEÑAS	• Los usuarios deben acceder por medio de una interfaz web a las funcionalidades de password self service INTERFAZ • La solución debe permitir tener múltiples políticas de Password activas • Cada política de Password self Service debe permitir configurar: ✓ Listado de preguntas random a utilizar para la autenticación (definidas por el administrador) ✓ Listado de preguntas a utilizar para la autenticación (definidas por el usuario) ✓ Posibilidad de mostrar por pantalla al usuario la política de contraseña cuando quiera cambiar su Password ✓ Campos del usuario que la contraseña no puede contener en su valor.

	✓ Longitud de la contraseña ✓ Cantidad de caracteres alfabéticos ✓ Cantidad de caracteres numéricos ✓ Cantidad de símbolos especiales ✓ Cantidad de caracteres únicos ✓ Palabras contenidas en un diccionario de palabras ✓ Password Case-Sensitive ✓ Cantidad de caracteres en mayúscula ✓ Cantidad de caracteres en minúscula • La solución debe tener la posibilidad de cambiar su contraseña ya sea porque expiró o por un cambio voluntario. • La solución debe permitir el auto desbloqueo de usuario (NO deshabilitación) tras confirmación de identidad (ej.: Preguntas/Respuestas). • La solución debe contar con la posibilidad de sincronizar la contraseña nueva ingresada en el módulo de Password Self Service, con los sistemas integrados en la solución de provisioning. • La solución debe incluir un generador de contraseñas random para que los administradores puedan periódicamente cambiar contraseñas de ciertas cuentas de manera automática. • Los conjuntos de preguntas para recuperar contraseñas deben poder ser definidos por el administrador. • Las funcionalidades de recupero de contraseña deben incluir la capacidad de enviar un enlace de recuperación por correo. • La solución debe proveer un servicio de Identificación de Usuario Olvidado, que permite mediante un desafío de preguntas/respuestas recuperar la información de usuario.

AUTOSERVICIO DE USUARIOS	• La solución debe proveer un portal de auto servicio y auto gestión para los usuarios, desde donde se pueda tener el seguimiento de las solicitudes de acceso, así como desde éste el ingreso directo a las aplicaciones integradas. • La solución de Self Service debe estar integrada a la aplicación de workflows y password self service. • La información existente en el directorio debe ser alimentada por medio de los colectores que toman información / integran cada solución en la arquitectura de provisioning. • La solución debe permitir a los usuarios realizar búsquedas por diversos atributos como nombre, apellido, legajo, área, etc. • La solución debe permitir que el usuario final pueda visualizar y hacer un seguimiento activo del proceso de solicitud de acceso siguiendo una línea de tiempo (cuando fue pedido, cuando fue aprobado, que queda pendiente). • El usuario tiene que tener la capacidad de modificar sus datos de acuerdo los permisos que se le otorgan. • Permitir Actualizar Elementos de su Perfil de Usuario. • Permitir que un usuario final pueda ver los roles asignados así mismo, y dependiendo de cómo este configurado ver roles que pueden delegar a otras personas. • Las modificaciones realizadas por el usuario deben poder propagarse a los sistemas conectados en la arquitectura de Provisioning. • La solución debe permitir a los usuarios realizar búsquedas por diversos atributos como nombre, apellido, legajo, área, etc.

	• El usuario tiene que tener la capacidad de modificar la importación/exportación de datos vía archivos CSV y LDIF • Requerir el acceso a: ✓ A un rol o permiso ✓ A un servicio de negocio o aplicación ✓ A la creación de un nuevo rol • La solución debe permitir a un usuario visualizar los ítems siguientes cuando realiza un requerimiento de acceso: ✓ Los permisos que el usuario tiene actualmente ✓ Las aplicaciones que el usuario tiene permiso actualmente junto con las aplicaciones para las cuales puede pedir permiso ✓ Las cuentas que el usuario tiene actualmente y permitirle requerir acceso a permisos de cuenta en forma directa (por ej: grupos de AD) ✓ Roles que los administradores puede sugerir de acuerdo al perfil de trabajo del usuario ✓ Usuarios similares de manera que puedan visualizar los permisos de otros usuarios y solicitarlos • La solución debe permitir que el usuario pueda cancelar una solicitud en progreso
INTEGRACIÓN	• El sistema de Identity Management debe estar integrado de manera nativa al sistema de Control de accesos y Web Single Sign on, utilizando el mismo repositorio de identidades. • El sistema de Identity Management debe poder aprovisionar de manera automática las credenciales en el sistema deSesion unificada, al momento de la creación de las diversas cuentas en los sistemas integrados.

	• El sistema de Identity Management debe poder aprovisionar de manera automática las credenciales en el sistema de Control de accesos y Web Single SIgn On, generadas de manera random. • Permitir la construcción de servicios que interactúen con servidores lDAP, PKI y entidades certificadoras.
CONTROL DE CALIDAD Y LIMPIEZA DE PRIVILEGIOS	• La solución debe soportar un repositorio de identidades de todas las aplicaciones de TI.
	• La solución debe proveer una visión consolidada de los usuarios, roles y privilegios asociados junto con las uniones entre cada uno de ellos.
	• La solución debe soportar la sincronización de datos de: ✓ SAP ✓ Directorio Activo ✓ Motores de bases de datos (Oracle, MS SQL, MySQL) ✓ Servicios SCIM ✓ Office 365 ✓ Otros tipos de aplicaciones (ej. Oracle EBS)
	• La solución debe permitir la importación y administración de datos que sea ejecutada en forma inmediata o planificada a intervalos regulares en forma batch.
	• La solución debe permitir la importación/exportación de datos vía archivos CSV y LDIF.
	• La solución debe poder identificar automáticamente y remediar las siguientes excepciones a privilegios tales como: ✓ Cuentas, roles y recursos huérfanos ✓ Colectores de privilegios excesivos ✓ Privilegios fuera de patrón

	• La solución debe permitir automatizar los procesos de consulta a los propietarios de roles/recursos que validen las excepciones necesarias.
	• La solución debe permitir la generación de reportes en forma simplificada para identificar las excepciones de privilegios.
	• La solución debe proveer un Catálogo de Permisos de manera de poder simplificar el Requerimiento de Accesos a los usuarios de la JEP sin la necesidad de conocer el nombre técnico del permiso dentro de la aplicación.
	• La solución debe permitir la reconciliación de cuentas entre el sistema IGA y las aplicaciones integradas.
	• La solución debe ser simple de instalar, configurar y mantener con un minimo costo de TCO, es decir, evitar costos ocultos de balanceadores, elementos para él HA.
FLUJOS DE TRABAJO	• Los workflows deben permitir manejar flujos de aprovisionamiento no solo de identidades, sino también de membresía a grupos, asignación de recursos, modificación de atributos, etc. • Los workflows deben soportar asignar una tarea a un grupo de usuarios y un miembro de este grupo debe poder realizar un "reservar" de las mismas para que no pueda ser tomada por otra persona. • La solución debe permitir enviar una alerta al usuario por email cuando tiene una tarea pendiente. • La solución debe permitir delegar una tarea a un colaborador en tiempo real para su ejecución. • La delegación de workflows debe poder definirse por tiempos determinados. Por ejemplo, si una persona sale de vacaciones debe

	poder delegar las tareas de aprobación de accesos por una semana a una persona. • La solución debe permitir la asignación de grupos de trabajo y en base a esos grupos debe permitir solicitar recursos para miembros del grupo. • La solución debe permitir la creación automática de procesos de aprobación basándose en eventos de los usuarios y cambios de sus atributos. • La solución debe permitir la creación de procesos de aprobación basándose en pedidos de usuario desde el portal de autoservicio • La solución debe permitir definir workflows custom con pasos en paralelo. • La solución debe permitir escalamiento de workflows, si no fue autorizado en cierto período de tiempo que el mismo sea escalado a otra persona o nivel. • Los workflows deben soportar el concepto de escalamiento de manera nativa (no mediante codificación Java, Xml, etc.) • La solución de workflow debe estar integrada en el mismo portal de self service y password self service. • La solución debe permitir llamadas a Web services dentro de cada paso del workflow. • Los workflows deben poder ser iniciados por los usuarios que requieren el acceso, recursos, etc. o por otra persona asignada a tal tarea. En este caso la solución debe permitir como mínimo que el recurso pueda ser solicitado por un jefe, para sus subordinados y que puedan definirse grupos de trabajo en los cuales el o los responsables del mismo puedan pedir recursos para sus miembros. (en este caso los grupos de

	trabajo no responden a estructuras jerárquicas del organigrama). • La solución deberá permitir la aprobación o rechazo de múltiples solicitudes en un solo paso. • Un mismo recurso debe poder ser aprovisionado de manera automática (mediante las políticas de los colectores) o mediante workflows. Por ejemplo, el aprovisionamiento de correo debe ser automático para los usuarios efectivos y mediante workflow para los contratados. • La solución debe proveer modelos de casos de uso del Ciclo de vida de Identidades preconfigurados con las tareas correspondientes que aceleren la implementación de la solución, tales como : ✓ Ciclo de Vida de Contratado ✓ Crear Contratado ✓ Crear varios Contratados ✓ Modificar contratados ✓ Cambiar contratados a empleados ✓ Finalizar el contrato de contratados ✓ Extender el contrato de contratados ✓ Cambiar el gerente del contratado ✓ Crear Contratados en forma batch ✓ Ciclo de Vida de Empleado ✓ Crear un empleado ✓ Crear varios empleados ✓ Convertir un empleado en contratado ✓ Dar de baja un empleado ✓ Modificar un empleado ✓ Cambiar el gerente ✓ Crear empleados en forma batch ✓ Autoservicio ✓ Seteo de preguntas de seguridad • La solución debe brindar la capacidad de armar diferentes ciclos de vida de usuarios

	combinando tareas prearmadas de manera tal que forma muy rápida se puedan customizar los workflows que necesita la organización. • Permitir Workflows de aprobación: En serie En Paralelo Teniendo X de Y cantidad de Aprobaciones • Proveer un modelo de escalamiento de aprobaciones por tiempo • La carga masiva de usuarios debe permitir: ✓ Transformar datos antes de cargarlos ✓ Ejecutar un workflow que permita realizar las acciones siguientes a nivel de ABM de usuario. - Aprobar - Rechazar - Reservar - Liberar
	• La solución debe permitir ver en forma gráfica el estado de la ejecución de los workflows, mostrando el flujo de ejecución a nivel de: ✓ Tareas aprobadas ✓ Tareas enviadas
SOLUCIÓN DE GESTIÓN DE CUENTAS PRIVILEGIADAS	• La solución debe proveer una interfaz gráfica web con capacidades avanzadas y evitar en lo posible el uso de scripting. • La solución debe proveer un componente de testeo que permita armar suites de pruebas antes de pasar a producción. • La solución debe ofrecer la posibilidad de reutilizar comandos y otros elementos en múltiples reglas. REGISTRO DE ACTIVIDAD DE USUARIOS • El licenciamiento debe contemplar el cubrimiento de hasta máximo 40 servidores.

	• La solución deberá proveer la posibilidad de grabar las sesiones privilegiadas en Windows, Linux y Unix para hasta máximo 40 servidores. • La solución debe permitir la captura de todas las acciones realizadas por usuarios privilegiados y su posterior reproducción y análisis incluyendo tanto lo que ingresa el usuario como lo que devuelve el sistema. En el caso de Unix/Linux la solución debe ofrecer la captura de todas las acciones realizadas por los usuarios (incluyendo las que no requieren privilegios) y su posterior reproducción y análisis AUDITORÍA Y REVISIÓN • La solución debe contar con capacidades de auditoría otorgando una herramienta de análisis forense con registros indelebles. • La solución debe contar con una herramienta o módulo que permita definir la reglas para seleccionar los eventos que serán tomados como muestra para la revisión de auditoría. • La solución debe proveer un mecanismo de notificación para los usuarios involucrados en la revisión indicando que existen eventos pendientes de análisis.
CONEXIÓN REMOTA	• La solución deberá proveer un bastión para la autenticación de usuarios privilegiados vía (SSH Gateway), donde los usuarios puedan aparecer logueados en el equipo a partir de un check out de una clave, sin necesariamente conocer la contraseña y sin perder la capacidad de grabar la sesión. • La solución debe permitir el bloqueo del usuario o desconexión en base al nivel de riesgo de los comandos ejecutados.
GOBIERNO DE IDENTIDADES	• La solución debe permitir definir reglas de negocio/compliance en forma fácil, mediante

	una interfaz en la que no sea necesario programar
	• Las reglas de negocio deben permitir especificar controles de: ✓ Segregación de funciones ✓ Restricciones de negocio tales como ubicación, función de trabajo, propiedad de datos y otros criterios ✓ Políticas entre sistemas ✓ Ejecución de transacciones
	• La solución debe soportar la asignación y monitoreo de riesgos a cualquier combinación de permisos de acceso
	• La solución debe permitir la certificación automática para: ✓ Usuarios ✓ Roles
	• La solución debe poder identificar las cuentas relevantes y ejecutar certificaciones de solo un subconjunto de datos, por ej.: ✓ Permisos que violan una política de segregación de funciones ✓ Combinaciones de permisos de accesos potencialmente riesgosas basado en análisis de patrones ✓ Recursos con "links" directos a los usuarios ✓ Cuentas huérfanas ✓ Permisos que cambian entre fechas
	• La solución debe poder alertar de violaciones a las políticas durante el contexto de una campaña de certificación.
	• La solución debe permitir integrarse con los sistemas de aprovisionamiento para una remediación automática.

	• La solución debe mostrar mediante reportes y tableros de control el estado de cumplimiento de la organización.
	• La solución debe brindar la facilidad que los administradores especifiquen en forma automatizada el lanzamiento de correos de recordatorio y alertas.
	• La solución debe brindar la facilidad que los administradores requieran la justificación mediante un comentario de la certificación de acceso de un usuario que está violando una política de cumplimiento.
	• La solución debe brindar la facilidad que los gerentes de negocio puedan certificar el acceso de los usuarios en forma amigable. Por favor ejemplifique un proceso de certificación.
	• La solución debe poder identificar los recursos con más violaciones de reglas SOD de manera poder evaluar la situación.
ADMINISTRACION DE ROLES	• La solución debe permitir el descubrimiento de roles usando técnicas eficientes y rápidas (por ej.: usando análisis basado en patrones). Brinde ejemplos de experiencias de descubrimiento de roles en clientes.
	• La solución debe permitir técnicas combinadas según un enfoque: ✓ Top Down ✓ Bottom Up ✓ Hibrido
	• La solución debe proveer metodologías de descubrimiento de roles 'out-of-the-box' fácilmente customizables mediante parámetros.
	• La solución debe permitir visualizar en forma fácil los diferentes tipos de asociaciones existentes entre usuarios, roles y recursos.

	• La solución debe poder asociar los resultados de las diferentes metodologías de descubrimiento de roles utilizadas.
	• La solución debe proveer de reportes que muestren el grado de cubrimiento de permisos de acceso.
	• La solución debe ser escalable y permitir acomodar millones de usuarios y decenas de millones de permisos de accesos.
	• La solución debe brindar una administración basada en web que se pueda integrar al workflow de la solución.
	• La solución debe poder detectar cambios de permisos de acceso a nivel negocio que requieran cambios en el modelo de roles Por ej: Si se agregan 10 usuarios a un Nuevo rol X y resulta que el rol X es similar al rol Y ya definido, el sistema debe ser capaz de detectar las similitudes y asistir al administrador en resolver las redundancias y reusar los roles.
	• La solución debe permitir automatizar los procesos de negocio para aprobación de roles, autoservicio de roles y modificación de roles.
	• La solución debe permitir la exploración y la importación de cuentas y roles en las siguientes aplicaciones: ✓ Active Directory/Sun One Directory/eDirectory/Oracle ID ✓ Oracle, MS SQL ✓ SAP,Siebel CRM,Oracle Business
	• La solución deber poder mostrar y/o reportar sobre los permisos de acceso y/o roles que hayan sido asignados a un usuario.
	• La solución deber poder mostrar y/o reportar sobre los usuarios/roles que tengan un acceso asignado a un recurso especifico o a un permiso de acceso.

	• La solución debe proveer reportes de privilegios /roles y certificaciones: ✓ Certificación de Privilegios de usuarios ✓ Campaña de certificación de usuarios ✓ Campaña de certificación de recursos ✓ Campaña de certificación de roles ✓ Estado de avance de certificaciones ✓ Requerimiento de cambios de privilegios de usuarios
	• La solución debe poder mostrar en un tablero de control el estado en que se encuentran las certificaciones.
ADMINISTRACION Y APROVISIONAMIENTO DE USUARIOS	• La solución debe permitir el descubrimiento de roles usando técnicas eficientes y rápidas (por ej: usando análisis basado en patrones). Brinde ejemplos de experiencias de descubrimiento de roles en clientes.
	• Crear, actualizar y eliminar cuentas de usuario en cualquier entorno de la empresa, incluidos sistemas y aplicaciones legados o basados en web.
	• Permitir el almacenamiento de cuentas administradas por la solución en un directorio corporativo.
	• Permitir la definición de una identificación de usuario global (UID global) que permita la asociación y mapeo de Identidades de usuarios a través de distintos 'endpoints' y fuentes autoritativas en base a reglas prestablecidas (Funcionalidad de Autodescubrimiento y correlación de cuentas de usuario).
	• Soportar la Administración y Aprovisionamiento de Identidades para los siguientes tipos de comunidades de usuarios: ✓ Empleados ✓ Contratados ✓ Socios de negocio

	✓ Usuarios Externos
	• Poder escalar a nivel de Administración y Aprovisionamiento según el tipo de comunidad de usuarios: de cientos a miles de usuarios (internos) a cientos de miles o millones de usuarios (externos).
	• Permitir delegación granular en forma temporal con: Fecha de inicio de la delegación Fecha de finalización de la delegación
	• Permitir la delegación dinámica de una tarea de aprobación de manera tal de reasignar la tarea a otro usuario dinámicamente según reglas preestablecidas.
	• Permitir cargar en forma masiva la información de usuarios desde más de una fuente autoritativa al mismo tiempo. ✓ RRHH propio ✓ Oracle ✓ SAP ✓ Peoplesoft ✓ Etc..
	• Permitir la carga masiva de usuarios aplicando reglas y realizando transformaciones de datos para normalizar el modelo de datos de usuarios y aplicaciones administradas.
	• Permitir el Aprovisionamiento de Usuarios basado en Roles (RBAC: Role Based Access Control).
	• Permitir que el modelo RBAC de administración de roles también soporte la capacidad de manejar roles anidados.
	• Permitir el Aprovisionamiento basado en reglas dinámicas (ABAC: Attribute Based Access Control) de manera de poder realizar la asignación de permisos basado en atributos del usuario.

	• Permitir el aprovisionamiento out of the box a los sistemas siguientes Sistemas Operativos tales como: ✓ Windows 20xx ✓ UNIX/Linux ✓ Z/OS (Mainframe : RACF,TSS,ACF2) ✓ OS400 Bases de Datos que incluyan aplicaciones tales como: ✓ SQL ✓ Oracle ✓ DB2 ✓ Otros Groupware que incluyan aplicaciones tales como: ✓ MS Exchange ✓ Lotus Notes ✓ MS Lync Servicios de Directorios tales como: ✓ Active Directory ✓ NDS ✓ SUNONE ✓ LDAP genérico Sistemas de control de acceso remoto (VPN) como: ✓ Kerberos ✓ RSA ID y PKI ✓ CA AuthMinder Entornos basados en la Nube soportando aplicaciones SaaS tales como: ✓ Google Apps ✓ Office 365 ✓ SalesForce Otros Aplicaciones Web que soporten el standard SCIM (System for Cross-domain Identity Management) tales como: ✓ Service Now ✓ Microsoft Azure ✓ Zendesk

	Aplicaciones de Negocio (ERP,CRM) tales como : ✓ Microsoft Dinamics ✓ SAP ✓ Siebel ✓ Oracle applications ✓ PeopleSoft Aprovisionar activos físicos tales como: ✓ Computadoras ✓ TE ✓ Otros
	• La solución debe tener flexibilidad de aprovisionar usuarios de fuentes de identidades donde no tenga un conector predefinido. Por ej.: Aplicaciones desarrolladas internamente (InHouse) La solución debe permitir la construcción de conectores a aplicaciones internas o comerciales no soportadas por un conector 'out of the box'.
	• La solución debe simplificar el desarrollo de conectores mediante herramientas tipo 'wizard', evitando la necesidad de programar en lenguaje de programación, para aplicaciones que definen usuarios y permisos en: ✓ Directorios LDAP (JNDI) ✓ Bases de datos RDMBS (ODBC/JDBC) ✓ Aplicaciones que exponen su estructura de usuarios y permisos vía 'web services'.
	• La solución debe permitir el diseño y especificación de los workflows en forma gráfica, sin necesidad de programar en lenguaje de scripting para poder definir los workflows.
	• Tener la Capacidad de cambiar el camino de aprobación teniendo en cuenta en el resultado de los pasos intermedios basado en reglas.
	• Permitir formular Políticas de Identidades basadas en lógica de negocio que permitan la ejecución de cambios de negocio cuando se

	cumple una condición o se evalúa una regla determinada: Los cambios de negocio pueden ser: ✓ Asignar o revocar roles ✓ Asignar o revocar membresías de grupos ✓ Actualizar atributos de un perfil de usuario
	• Permitir que una política de identidades se aplique en forma selectiva a un grupo de usuarios determinados, de manera de evitar que todo el universo de usuarios y solo se aplique a un 10 % de usuarios solamente.
	• Permitir formular Políticas de Identidades Preventivas que eviten que un usuario reciba privilegios que resulten en un conflicto de interés (SOD: Segregation of Duties).
	• Estas políticas deben ser ejecutadas antes que la tarea de aprovisionamiento sea ejecutada, permitiendo que el administrador chequee las violaciones a las políticas antes de asignar o cambiar atributos de un perfil, si existe una violación el administrador puede limpiar la violación antes de submitir la tarea.
	• Permitir la construcción de Políticas de Identidades complejas sin necesidad de programar, Mediante una herramienta tipo 'Wizard' que pueda ser manejada por el administrador en forma simple.
	• Tener la capacidad de sincronizar cuentas: ✓ Hacia Afuera: Desde la definición central de la organización en el sistema de Adm. De Identidades a los sistemas administrados a través de políticas de identidades y roles. ✓ Hacia Adentro: Desde los sistemas administrados hacia el sistema de Adm. De Identidades detectando cambios a través de un proceso de sincronización reversa.

	• Poder realizar una sincronización reversa detectando cualquier tipo de cambio realizados en forma directa en las aplicaciones integradas por fuera del proceso normal de Adm. de Identidades tales como creación de cuentas nuevas, atributos modificados, etc.
	• La detección de cambios realizados por afuera de la herramienta de Adm. De Identidades debe poder ejecutar las acciones siguientes: ✓ Aceptar ✓ Borrar ✓ Suspender ✓ Enviar a flujo de aprobación. etc.
	• Poder realizar la sincronización de usuarios del Active Directory (AD), con información de usuarios de aplicaciones en la nube.
	• Tener la capacidad para gestionar las altas y bajas de cuentas en forma mediante la lectura de archivos csv o txt.
	• La solución debe poder definir los umbrales de riesgo que pueden asumir los usuarios y solicitar aprobación de los accesos solicitados si el umbral de riesgo es elevado.
	• La solución debe poder alertar en caso de que las solicitudes de accesos superen los umbrales de riesgo definidos por la JEP.
	• La solución debe poder evaluar el riesgo de la combinación de accesos en tiempo real, por ejemplo, Si un usuario solicita el acceso a la aplicación ERP y también a la aplicación de Nómina; la solución debe evaluar en línea si estos accesos se pueden otorgar al usuario solicitante y no son accesos que generan riesgo a la JEP.
	• La solución debe proveer un único punto de ingreso a todas las aplicaciones de los usuarios,

	evitando múltiples ingresos de credenciales a los usuarios.
	• La solución debe poder modificar en forma masiva los atributos de un usuario basado en un atributo filtro, tal como departamento, ciudad, fecha de ingreso, fecha de egreso etc. Por ej.: Se quiere modificar todos los usuarios que pertenecen a un departamento determinado.
	• La solución debe permitir la notificación de correos electrónicos basado en Políticas, es decir que basado en la información del evento y/o de la fecha, se configurará dinámicamente el cuerpo del mensaje, el remitente y el receptor.
	• Mostrar en forma online las modificaciones realizadas por los administradores directamente desde la Consola de las Aplicaciones, por fuera del proceso normal de Adm. de Identidades tales como creación de cuentas nuevas, atributos modificados, etc.
	• Tener la capacidad para programar las altas y bajas de cuentas basadas en un calendario de tiempo, con una fecha efectiva de arranque y fecha efectiva de terminación.
	• Tener la capacidad de buscar usuarios en el directorio basado en diferentes atributos de usuarios tales como ID de usuario, apellido, primer nombre, etc.
	• Esta capacidad que generalmente tienen los administradores debe poder ser delegada a los usuarios finales (i.e, funcionalidad de 'paginas blancas').
	• Los usuarios deberán poder ver la información con filtros de acuerdo con su rol, de manera que un usuario final pueda ver su nombre, oficina y dirección, mientras que el gerente del mismo vea además sus roles.

	Tener la capacidad de definir un ID de usuario único durante la creación de la cuenta de una identidad en la aplicación integrada basada en una lógica predefinida que debe considerar las siguientes situaciones de conflicto: ✓ Que el usuario este previamente definido en cuyo caso deberá generar una ID de usuario única. ✓ Que el usuario haya sido retirado o deshabilitado en cuyo caso se deberá prevenir la reutilización del mismo usuario.
	• La solución debe proveer flexibilidad en la administración de permisos, permitiendo un control granular de cambios a nivel de: ✓ Roles de negocio ✓ Cambios en las cuentas ✓ Cambios en los atributos de las cuentas ✓ Cambios en los valores de los atributos de las cuentas.
	• La interfaz del usuario debe poder ser customizada en forma simple y fácil, permitiendo diferentes 'skins' de acuerdo al tipo de usuarios que este ingresando a la interfaz, etc.
	• Permitir que el proceso de registro obligue al usuario final a dar como leída y aceptada, las condiciones de acceso a la organización, pudiendo ser un formulario de aceptación o una política de seguridad global aprobada.
	• Permitir que el proceso de registro permita establecer diferentes métodos de verificación de identidad: ✓ Validación de Respuestas a los atributos ingresados en la pantalla de registro que son validados vía web Services contra sistemas internos/externos de validación. ✓ Validación del usuario en forma posterior por parte de un administrativo.

	• La solución debe proveer formularios HTML prearmados para la registración de usuarios
	• La solución debe tener un sistema de administración de contraseñas flexible que permite establecer políticas de: ✓ Composición ✓ Reutilización ✓ Expiración ✓ Reinicio ✓ Autoservicio ✓ Propagación ✓ Integración
	Permitir asignar a un usuario la contraseña por primera vez y luego solicitar que la cambie con la primera sesión inicial.
	• Permitir soportar políticas de composición de contraseñas basado en un diccionario de contraseñas no permitidas.
	• La solución debe permitir limitar la cantidad de veces que se intenta reiniciar una contraseña.
	• La solución debe brindar un mecanismo de preguntas variables para validar la autenticación
	• La solución debe permitir soportar políticas de reutilización flexibles y debe permitir guardar la información de las contraseñas utilizadas para evitar su uso recurrente basadas en: ✓ Datos de los atributos del perfil de usuario ✓ Contraseñas del Diccionario ✓ Cantidad mínima de días antes de reusar una contraseña ✓ Cantidad mínima de contraseñas antes de volver a reusar la contraseña ✓ Porcentaje de diferencia con respecto a la contraseña anterior

	• La solución debe proveer un mecanismo de propagación de cambio de contraseñas a todas las plataformas integradas.
	• La solución debe brindar un mecanismo para atrapar cambios de contraseñas cuando se realizan puntualmente en las aplicaciones integradas.
	• La solución debe contar con una aplicación móvil que permita desde un dispositivo móvil (Smartphone,Iphone o Ipad) realizar las tareas siguientes : ✓ Reinicio de Contraseñas ✓ Cambio de Contraseñas ✓ Responder a solicitudes de aprobación ✓ Visualización de información a nivel gerencial para aprobar ✓ La solución debe permitir la aprobación de tareas de flujos de trabajo desde un dispositivo móvil Nota : Como mínimo debe soportar IOS y Android.
	• El Catálogo de Permisos debe describir los permisos en forma comprensible e intuitiva para solicitarlos (Por ejemplo: Acceso a SAP CRM en lugar de 'SAP_View:RZS50).
	• La solución debe permitir el manejo de un Catálogo de permisos granulares de manera tal que permita solicitar: ✓ Roles ✓ Membresía de grupos ✓ Atributos de usuario ✓ La solución debe soportar un Modelo de Permisos que permita presentar y agrupar los mismos en forma lógica de manera que el usuario final pueda navegar fácilmente para solicitar los permisos que necesita. ✓ Las agrupaciones lógicas deberían ser al menos las siguientes:

	✓ Aplicaciones ✓ Grupo de Aplicaciones ✓ Roles ✓ Grupo de Roles ✓ Permisos de Negocio
	• La solución debe permitir que los Administradores puedan agregar, modificar y borrar accesos que son presentados a los usuarios como un Catálogo de Permisos.
	• La solución debe permitir la generación de un Tablero de Control Analítico que permita visualizar las estadísticas relacionadas con un permiso tal como el nivel de servicio (SLA) o el número de requerimientos para un permiso en un período de tiempo determinado. Por ej.: un administrador quiere ver cuánto tiempo lleva otorgar a los usuarios los accesos a la red. El Tablero de control debe mostrar la cantidad de requerimientos en un periodo de tiempo, cuanto tiempo llevó cada uno, cuáles fueron los grupos que lo solicitaron y otra información similar.
	• La solución debe permitir visualizar el scoring de riesgo asociado con el permiso solicitado
	• La solución debe permitir la aceptación o rechazo de un Requerimiento de Acceso basado en una evaluación de riesgo entre el permiso solicitado y los permisos existentes.
	• La solución debe permitir actualizar en forma dinámica el scoring de riesgo asociado con el permiso solicitado basado en los privilegios del usuario, atributos del usuario y factores contextuales, simulando en tiempo real los cambios de scoring de riesgo en contexto con los requerimientos de acceso.
	• La solución debe permitir la configuración de acciones especiales para manejar requerimientos

	con un nivel de scoring de riesgo fuera de norma.
	• La solución debe poder recomendar al usuario final cuales son los roles que deberían incluir en la Solicitud de requerimiento de acceso basado en los siguientes conceptos: ✓ Quién es el usuario (ej. usuario pertenece al Dpto de Finanzas) ✓ Qué permisos tiene actualmente el usuario (por ej.: Permiso de 'Aprobación de Gastos') ✓ Cuales ítems se encuentran incluidos en el carrito de compras.
	• La solución debe poder requerir un Segundo factor de autenticación cuando se requieren los siguientes elementos: ✓ Login ✓ Solicitud de Requerimiento de Acceso específico ✓ La solución debe poder integrarse desde su interfaz gráfica con otras aplicaciones en forma transparente a través de 'links' a URLs externas y/o estáticas.

3.3 ESPECIFICACIONES MINIMAS SOLUCION SESION UNIFICADA

Especificaciones Técnicas Mínimas de Solución	
La solución debe estar integrada a la de IGA	
Cliente	Si la solución de inicio de sesión único es una aplicación WEB, esta no solo debe permitir la visualización de datos, sino el procesamiento de los mismos a través de la WEB.
Navegadores	El sistema debe permitir el acceso desde los navegadores conocidos en el mercado, que sea de distribución libre y no tenga costo para la entidad (Ejemplo: Internet Explorer, Firefox Mozilla y Chrome, etc.)

Integración con Sistema Operativo	Si la solución de Sesión de inicio unificada cuenta con elementos de software, estos deberán instalarse en sistema operativo Windows Server 2016 o superior.
Integración con motores de base de datos	El sistema debe permitir trabajar con cualquiera de los motores de bases de datos existentes: SQL Server 2017 o superior, Oracle,etc.
Idioma	La solución de inicio de sesión inicio unificada, las ayudas, documentación y los sitios de soporte deben operar y entregarse, como mínimo en idioma español o inglés.
Logs	La solución ofrecida debe llevar un registro de las transacciones de los usuarios
Integridad	La solución debe proveer información integral, real, confiable y oportuna de los datos registrados en ella.
	La solución no debe limitar la cantidad de Sistemas de Información, Aplicativos o Servicios Informáticos en los que la Entidad requiera implementar la autenticación mediante Single-Sign-On.
	La solución de sesión de inicio unificada ofrecida debe permitir como mínimo la autenticación Single-Sign-On con los Servicios Informáticos, Sistemas de Información y Aplicativos en producción de la Entidad sin impacto negativo, garantizando su correcto funcionamiento en forma transparente y sin importar si se encuentran en ambiente Web o Cliente/Servidor.
	La solución debe permitir la integración con el Directorio activo de la Entidad.
	La solución no debe limitar la cantidad de Sistemas de Información, Aplicativos o Servicios Informáticos a los que accede un usuario o licencia de usuario.
	La solución debe permitir la configuración de políticas de seguridad de las contraseñas una vez sean gestionadas por el Gestor de Identidades y cuando no existan en la Base de Datos del Sistema de Información o Aplicativo. Como mínimo debe permitir la definición de longitud, periodicidad de cambio y complejidad.
	Las contraseñas de conexión a cada Sistema de Información, Aplicativo o Servicio informático deben ser almacenadas de

	manera segura, debidamente encriptadas y no deben ser conocidas por el administrador de la solución.
	La solución debe permitir conocer registros de auditoría en donde se pueda encontrar la siguiente información: intentos fallidos indicando usuario, fecha, hora y dirección IP, información del último cambio de contraseña realizado, la fecha, la hora de realización y la dirección IP de la maquina desde la cual se realizó el cambio.
	La solución de Sesión de inicio unificada debe ser compatible con los Sistemas Operativos Microsoft Windows 7, Windows 8, Windows 8.1 y Windows 10.
	La solución deberá soportar la opción de restablecimiento de contraseña por parte del usuario.
Administración	La solución debe ser administrada y mantenida de manera centralizada
	La configuración y parametrización de la solución debe ser fácil, intuitiva y amigable.
	La solución de Sesión de inicio unificada debe permitir la creación de usuarios con perfiles y roles diferentes para la administración y operación.
	La solución de Sesión de inicio unificada ofrecida debe permitir remover y configurar nuevos Servicios Informáticos, Sistemas de Información y Aplicativos para el uso de autenticación mediante Single-Sign-On.
	La solución no debe causar impacto negativo en el desempeño de los Servicios Informáticos, Sistemas de Información y Aplicaciones de la Entidad que se autentiquen mediante Single-Sign-On.
Seguridad	La solución debe garantizar la integridad, confidencialidad y la disponibilidad de la información una vez esta almacenada.
	La solución debe permitir la administración de roles y perfiles para cumplir con el principio de autorización.
	La solución debe permitir el acceso y la administración de usuarios para cumplir con el principio de autenticación. La autenticación de usuarios en el sistema debe ser directa y automática con Directorio Activo (bajo un esquema Single Sign On).

	La solución debe cumplir con estándares internacionales para el cifrado de la información como FIPS-140-2 nivel 2 con el fin de proteger los datos que se transmiten y los datos almacenados.
Conexión	La solución sesión de inicio unificada ofrecida debe integrarse con el Directorio Activo de Windows Server 2016 con posibilidad de migrar a Windows Server 2019 si la JEP lo requiere, de manera transparente, sin causar impacto negativo y no debe requerir modificaciones a la configuración establecida y con la plataforma MS SharePoint de la JEP
Usabilidad	Debe proveer una capa de presentación mediante un entorno grafico amigable.

4. CAPACITACION

- El personal que haga parte de la oferta del servicio de Mesa de Ayuda en la modalidad de BPO deberá contar con transferencia de conocimiento en el uso de la herramienta ofertada al momento de inicio de la prestación del servicio y así mismo todo el personal adicional que ingrese o sustituya al personal inicial durante la duración del proyecto.
- Adicionalmente a la transferencia de conocimiento que el proveedor haga al personal contratado para la prestación del servicio de mesa de ayuda, el proveedor deberá durante la vigencia brindar un máximo de seis (6) sesiones en todos los módulos que comprende la herramienta, al personal que indique la JEP y un curso ITIL para máximo 11 personas de la entidad.
- El requisito anterior puede ser suplido con la disponibilidad permanente, durante la vigencia del contrato, mediante el acceso sin restricciones a una plataforma que permita la auto capacitación del personal que disponga la JEP.

5. USO Y APROPIACIÓN Y GESTIÓN DEL CAMBIO DEL PROYECTO

- El proyecto debe tener dentro de sus entregables la ejecución de un plan de gestión del cambio (implementación y operación por fases) para facilitar el Uso y Apropiación de las dos herramientas adquirida. Este plan debe incluir y describir modelo de servicio, modelo de soporte, mejores prácticas, procedimientos, recursos y herramientas que serán utilizadas para lograr el objetivo.

- Este plan debe estar basado en una estrategia para concientizar a funcionarios y usuarios sobre las oportunidades que se presentan con el uso del nuevo servicio de TI a implementar, mejorando su productividad y calidad de vida (al hacer uso consciente de sistemas de información, dispositivos, herramientas de comunicación sincrónicas y asincrónicas, construcción de documentos en línea, herramientas para compartir o enviar archivos o acceso a la información) que el proyecto implementará.

El proveedor debe identificar como entradas:

- Necesidades de Apropiación.
- Los Procesos de la organización que se van a afectar con el proyecto.
- Competencias individuales y grupales requeridas para el uso o gestión del nuevo servicio de TI o solución.
- Restricciones identificadas.

El plan de gestión del cambio debe incluir:

- Incorporación del Cambio dentro de la JEP.
- Estrategia y acciones específicas de comunicación y divulgación.
- Cambio incorporado en los procesos.
- Plan propuesto para la Gestión de mejoramiento continuo en la adopción del cambio.
- Indicadores de uso propuesto.

NOMBRE DEL PROPONENTE:
_____

FIRMA DEL REPRESENTANTE LEGAL:
_____

Nombre del Representante Legal:
_____

C.C.:
_____

NOTA: El proponente con la firma del presente documento declara expresamente que se compromete a cumplir con la totalidad de las especificaciones técnicas aquí señaladas y conoce la totalidad del anexo.