SELECCIÓN ABREVIADA POR SUBASTA INVERSA No. 9015689 de 2025

OBJETO:

Adquirir licencias soporte y actualización del Antispam Barracuda Cloud

1. Denominación del bien o Servicio

SOFTWARE

2. Denominación técnica del bien o Servicio

SOFTWARE

3. Unidad de medida

UN

4. Descripción General

OBJETIVO GENERAL

Mitigar los riesgos a los que está expuesta la información, por medio de la Adquisición de licencias, soporte y actualización del La solución Barracuda Email Protection Advanced, propendiendo por la protección del servicio de correo electrónico corporativo, esta solución integral de protección del correo electrónico basada en la nube, que permita prevenir, detectar, mitigar y responder de forma automatizada a amenazas avanzadas como phishing, ransomware, suplantación de identidad (BEC), malware, y ataques dirigidos (spear phishing). La solución debe garantizar la continuidad operativa del servicio de correo electrónico en caso de fallas, así como brindar capacidades de respaldo, archivado, y cumplimiento normativo

OBJETIVOS ESPECIFICOS

· Prevenir el ingreso de correos electrónicos maliciosos mediante filtros avanzados de spam, phishing, malware, ransomware y suplantación de identidad, utilizando inteligencia artificial y análisis de comportamiento.

· Detectar amenazas sofisticadas en tiempo real, incluyendo ataques de tipo Business Email

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

Compromise (BEC), spear phishing y ataques sin carga maliciosa (zero payload), utilizando tecnologías de análisis dinámico y sandboxing.

· Proteger las cuentas de correo electrónico contra accesos no autorizados, mediante la detección de anomalías en inicios de sesión, comportamientos sospechosos y posibles secuestros de cuenta (account takeover).

· Automatizar la respuesta ante incidentes de seguridad relacionados con el correo electrónico, permitiendo la identificación, contención y eliminación de correos comprometidos ya entregados a los usuarios.

· Garantizar la continuidad del servicio de correo electrónico, permitiendo a los usuarios enviar y recibir correos aun cuando la plataforma principal (Microsoft 365, Exchange, etc.) se encuentre fuera de servicio.

· Asegurar el cumplimiento normativo y la conservación de evidencias electrónicas, a través de mecanismos de archivado inmutable, retención de correos y capacidades de búsqueda avanzada.

· Centralizar la gestión, monitoreo y auditoría de la seguridad del correo electrónico, a través de una consola administrativa unificada con generación de alertas, reportes e indicadores clave.

1. ESPECIFICACIONES TECNICAS

La Adquisición de las licencias, soporte y actualización de la solución Barracuda Email Protection Advanced, comprende:

1.1 HARDWARE:

· No se requiere porque es una solución as a services

1.2. SOFTWARE Y LICENCIAMIENTO

· Entrega del licenciamiento completo para la solución Barracuda Email Protection Advanced.

· El software debe ser una solución 100% basada en la nube, sin necesidad de instalación local en servidores o dispositivos finales.

· Debe ser compatible con plataformas de correo electrónico Microsoft 365 y Exchange Online incluyendo entornos híbridos.

· Debe contar con filtros avanzados de spam, malware, ransomware y virus, actualizados de forma automática y permanente.

· Debe incluir protección contra ataques de phishing, spear phishing y Business Email Compromise (BEC), con análisis de comportamiento del contenido y el remitente.

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

· La solución debe ofrecer detección de amenazas sin archivos ni enlaces (zero payload), utilizando tecnología de inteligencia artificial y machine learning.

· Debe contar con sandboxing dinámico para el análisis seguro de archivos y enlaces sospechosos antes de su entrega al usuario.

· La solución debe permitir la validación de autenticación de correos electrónicos mediante los protocolos SPF, DKIM y DMARC, con generación de reportes y acciones automáticas de bloqueo o cuarentena.

· Debe incluir protección contra secuestro de cuentas (Account Takeover Protection), con detección de inicios de sesión anómalos y bloqueo automático de cuentas comprometidas.

· Debe contar con una consola centralizada de administración y monitoreo accesible desde la web, con autenticación multifactor (MFA) y gestión basada en roles (RBAC).

· La solución debe ofrecer respuesta automática a incidentes de seguridad, incluyendo la detección, notificación, y eliminación de correos maliciosos entregados a los usuarios.

· Debe incluir funcionalidad de continuidad del correo electrónico (Email Continuity), permitiendo el envío y recepción de correos desde una plataforma alterna en caso de interrupción del servicio principal.

· La solución debe generar reportes automáticos y en tiempo real sobre incidentes, correos bloqueados, usuarios afectados y otras métricas relevantes de seguridad.

· Debe permitir integración con plataformas SIEM mediante API o syslog para la exportación de eventos de seguridad.

· La solución debe operar bajo el protocolo seguro HTTPS (SSL/TLS) y ser accesible desde los navegadores más comunes (Chrome, Edge, Firefox, Safari).

1.3. ESPECIFICACIONES DE LA PLATAFORMA:

· El producto no puede estar en End of Sale en los próximos 3 años.

· Integración con LDAP basada en roles, la solución se debe integrar con toda la clase de servidores de LDAP, tales como: OpenLDAP, Lotus Domino, iPlanet LDAP y Windows Active Directory.

· La solución deberá poder integrarse con un Active Directory de Microsoft, sin necesidad de instalar algún componente en los controladores de dominio. Esta integración permitirá que la administración de la solución se efectué por medio de cuentas de usuarios y grupos de administración basadas en el Active Directory.

· Administración Basada en Roles: Es requisito indispensable que se pueda segregar la

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

administración de la seguridad diferenciando claramente los roles de Seguridad de Sistemas y de otras unidades definidas en el Active Directory. La solución deberá permitir la segregación de funciones de forma granular, permitiendo así definir al alcance o posibilidades de gestión para cada administrador.

· Administración delegada.

· Personalización de la configuración si es necesario.

· La solución deberá permitir monitoreo en tiempo real.

· La solución deberá poder realizar respaldos y restauraciones de las configuraciones.

· Las políticas, los cuadros de mando, informes y más deberán estar disponibles en una consola o menú gráfico, para reducir el tiempo y la experiencia necesaria para lograr resultados.

· Compatibilidad con los diferentes navegadores de internet (Internet Explorer 10 y superior, Chrome, Mozilla Firefox, Opera, Edge, Safari).

1.4. ESPECIFICACIONES TÉCNICAS DEL PRODUCTO O SERVICIO A ADQUIRIR:

· La solución debe permitir la creación y gestión de políticas locales de filtrado y control de correos electrónicos, diferenciando entre usuarios, grupos, dominios y tipos de contenido.

· Debe permitir el establecimiento de reglas de retención y eliminación para cumplimiento de normativas institucionales o sectoriales.

· Debe ofrecer funcionalidades de cifrado de correos electrónicos salientes, configurables por el administrador, según criterios como tipo de contenido o destinatario.

· Debe permitir la creación de listas blancas y negras locales, administradas por el equipo de TI, sin depender de reglas globales del fabricante.

· La solución debe ofrecer control de datos sensibles (DLP # Data Loss Prevention) para prevenir el envío de información confidencial o restringida a través del correo electrónico.

· Debe contar con un registro de auditoría (logs) accesible por el administrador, donde se registren todos los eventos de entrada, salida, detección, bloqueo, y acciones administrativas.

· Debe integrarse con sistemas de autenticación locales (ej. Active Directory, Azure AD) para aplicar políticas diferenciadas según el perfil del usuario.

· La solución debe contar con análisis dinámico (sandboxing) para examinar archivos adjuntos y enlaces sospechosos en entornos aislados antes de ser entregados al usuario final.

· Debe utilizar tecnologías de inteligencia artificial (IA) y machine learning (ML) para identificar

patrones de comportamiento inusuales en correos electrónicos, evitando ataques de tipo zero-day y amenazas no identificadas por firmas tradicionales.

· Debe incluir capacidades de detección de suplantación de identidad (spoofing), mediante verificación de encabezados, dominios, autenticación (SPF, DKIM, DMARC), y análisis de relaciones previas entre remitente y destinatario.

· La protección debe incluir detección de amenazas sin carga maliciosa (zero payload attacks), tales como correos que utilizan únicamente ingeniería social.

· La solución debe permitir la remediación automática de correos maliciosos entregados, eliminándolos del buzón del usuario, bloqueando al remitente y rastreando usuarios afectados.

· Debe incluir una consola forense que permita investigar campañas maliciosas, rastrear su origen, ver la propagación y aplicar acciones correctivas.

· El sistema debe proteger contra secuestro de cuentas (Account Takeover Protection - ATO) detectando comportamientos anómalos, accesos desde ubicaciones sospechosas, y cambios inusuales en patrones de envío.

1.5. PROTECCIÓN ANTIMALWARE:

· Protección de phishing y suplantación de sitios web.

· Debe permitir proteger a los usuarios de virus, spyware, troyanos, scams, malware, phishing, botnets, gusanos que infecten los equipos de cómputo.

· Evaluación en tiempo real de los contenidos, guiones y otros potenciales componentes de amenaza.

· La solución deberá permitir la detección de malware entrante y saliente de la red.

· Las firmas deberán ser actualizadas automáticamente o bajo demanda de los administradores.

· La solución deberá permitir la detección heurística proactiva.

· Debe poseer módulo de cuarentena de malware.

1.6. SERVICIO DE ACTUALIZACIÓN

El proponente deberá garantizar, por un período mínimo de 12 meses, el suministro, operación y soporte de la solución Barracuda Email Protection Advanced, cumpliendo con los siguientes requisitos:

· Licenciamiento y Accesos

· Licenciamiento activo por mínimo 12 meses para la solución Barracuda Email Protection Advanced.

· Acceso completo al módulo Advanced Threat Protection (ATP) por al menos 12 meses.

· Acceso a todas las funcionalidades de administración y configuración desde la consola en la nube de Barracuda.

· Protección contra malware avanzado, exploits de día cero y ataques dirigidos.

· Análisis de archivos adjuntos y enlaces mediante sandboxing en la nube.

· Uso de inteligencia artificial, aprendizaje automático y algoritmos de detección para clasificación de amenazas.

· Respuesta automática y análisis forense de incidentes.

· Protección basada en comportamiento y análisis en tiempo real de amenazas emergentes.

· Funcionalidades Esenciales de Seguridad.

· Protección contra spam, virus, spoofing, ataques de denegación de servicio y ataques de directorio.

· Filtrado de correo electrónico saliente.

· Filtrado por usuario, grupo o dominio.

· Bloqueo de archivos adjuntos por tipo y extensión.

· Aplicación automática de políticas sin intervención del usuario.

· Actualizaciones automáticas y continuas de firmas, listas negras y políticas de seguridad.

· Actualizaciones automáticas y en tiempo real, sin necesidad de intervención manual.

· Migración a nuevas versiones estables sin costo adicional durante la vigencia del contrato.

· Soporte técnico completo para actualizaciones de firmware o funcionalidades nuevas.

· Notificación previa de cambios mayores por parte del contratista y soporte del fabricante.

· Mantenimiento continuo sobre la última versión estable disponible.

· Administración y Monitoreo

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

· Acceso completo a la consola de gestión en la nube de Barracuda.

· Visualización de registros, trazabilidad de eventos, auditoría y generación de reportes gráficos.

· Acceso a análisis de incidentes y funciones de remediación.

· Alcance del Servicio.

· Soporte técnico 24/7 en español para incidentes críticos.

· Soporte preventivo y correctivo sin costos adicionales.

· Capacitación inicial remota al personal administrador de la entidad.

· Entrega de documentación técnica y de administración.

· Sin cobros adicionales por licencias, módulos o actualizaciones especificadas en este documento.

NOTAS:

Todos los trabajos de actualización deben ser notificados y documentados oportunamente por el proveedor mínimamente 15 días antes, quien informará al Distrito Especial de Ciencia, Tecnología e Innovación de Medellín si requiere su apoyo para recibir el acompañamiento correspondiente.

Las nuevas funcionalidades integradas en las actualizaciones deben ser notificadas y documentadas al Supervisor del Contrato mínimamente 15 días antes, después de que se haya completado la actividad.

1.7. SOPORTE

· El servicio de soporte debe ser prestado por personal certificado en #Barracuda Advanced Email Security" y debe ser residente en el Área Metropolitana del valle de Aburra.

· La atención que se realice por #Los medios de comunicación por donde se puede solicitar un soporte", por parte del contratista deberá prestarse de lunes a viernes en horario de 8:00 a.m. a 6:00 p.m.

· La atención que se realice por #Los medios de comunicación por donde se puede solicitar un soporte", por parte del fabricante deberá garantizarse 7x24.

· El tiempo máximo de respuesta telefónica para asuntos críticos después del reporte: 4 horas.

· El tiempo de respuesta en sitio sí se determina que el problema no puede ser resuelto por #Los medios de comunicación por donde se puede solicitar un soporte", es decir de manera

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

remota, el ingeniero asignado se desplazará a las oficinas del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, en un tiempo máximo de Cuatro (4) horas.

· Soporte en sitio comprende actualizaciones, reinstalaciones, parametrizaciones y adecuaciones necesarias que requiera el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín.

· Las actualizaciones deberán ser realizadas por el contratista en caso de que el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, lo requiera.

· El servicio de soporte y mantenimiento debe ser soportado por personal certificado en la solución.

· El soporte de la herramienta deberá iniciar a partir de finalizada la instalación e implementación de la solución, la cual no debe durar más de 15 días calendario.

· El servicio de soporte y mantenimiento para los incidentes reportados debe ser atendido según los ANS (Acuerdos de Nivel de Servicio) descritos a continuación.

· Las actividades de actualización que se requieran, se deberán programar en horarios previamente autorizados por el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín (horarios no laborales) y estos serán desarrollados por el contratista, quien deberá entregar el plan de trabajo respectivo.

· No se pueden cerrar los requerimientos (Casos de Soporte # Tickets) hasta que el Supervisor del Contrato lo autorice.

· Realización de visitas que sean necesarias para solucionar incidentes.

· Los hallazgos o mejoras detectados en la herramienta donde el fabricante debe escalar el requerimiento a su área de desarrollo porque generan dificultades en el servicio, bajando la credibilidad del producto y calidad del servicio, deben ser solucionados de acuerdo con la definición de un plan de atención concertado entre las partes, que detalle las actividades, responsables y tiempos, para brindar una respuesta adecuada, coherente con los acuerdos de nivel de servicio definidos.

· El tiempo que se demore el fabricante solucionando alguna falla en el software que ocasione indisponibilidad del servicio contratado, al escalar a su área de desarrollo, debe compensarlo en tiempo sobre el vencimiento de las licencias y el soporte; es decir, la fecha de terminación del contrato se debe correr los días que se tardaron en entregar la solución definitiva.

· Las actividades de actualización que se requieran, se deberán programar en horarios previamente autorizados por el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín (horarios no laborales) y estos serán desarrollados por el contratista, quien deberá entregar el plan de trabajo respectivo.

· Si la solución o herramienta posee problemas que no puede ser resuelto por los #Los medios de comunicación por donde se puede solicitar un soporte", debe atenderse en sitio tiempo completo (24x7), hasta que entreguen una solución real, confiable y estable; de acuerdo a lo establecido en los Acuerdos de Niveles de Servicio (ANS).

1.8. REPORTES:

La solución deberá incluir un módulo de reportes avanzado, sin costo adicional, que cumpla con las siguientes capacidades técnicas:

· El sistema debe ofrecer reportes estándar, así como permitir la creación de informes personalizados con filtros dinámicos, agrupación de datos por múltiples criterios (ej. remitente, dominio, nivel de amenaza), y selección de columnas visibles.
· Los reportes deben presentarse mediante gráficos dinámicos tipo barra o línea, con capacidad de alternar entre vistas diarias, semanales o mensuales, según el periodo analizado. El usuario debe poder definir el formato visual más adecuado para el análisis.

· La herramienta debe generar informes específicos sobre:
o Volumen de correos fraudulentos por tipo (phishing, suplantación, estafa, secuestro de conversaciones, extorsión).
o Principales destinatarios internos de dichos mensajes.
o Remitentes y dominios más utilizados para intentos de suplantación.
o Servicios legítimos más suplantados (p. ej. Google, Amazon, etc.).
o Asuntos más frecuentes en correos fraudulentos.

· El sistema debe permitir trazabilidad completa de eventos de seguridad, incluyendo información detallada de quién, qué, cuándo, cómo y desde dónde, para soporte en procesos de investigación de incidentes.

· Se debe permitir la generación de reportes históricos con selección de rangos de fechas personalizables.

· Informes deben ser exportables en formatos estándares como .CSV, .PDF y .TXT. El sistema debe permitir exportar hasta 10,000 registros por informe.

· Se deberá contar con funcionalidad para programar la generación y envío automático de reportes a través de correo electrónico, según frecuencias configurables (diaria, semanal, mensual).

· El usuario debe poder guardar reportes personalizados bajo su perfil para su reutilización, y establecer un informe como predeterminado para acceso rápido.

1.9. INSTALACION:

· La instalación, configuración y puesta en marcha de la solución deberá ser realizada en sitio por personal certificado por el fabricante, con experiencia comprobable en implementaciones similares.

· El proceso debe completarse hasta que la solución esté en plena operación productiva.

· El proceso de transición desde la plataforma actual hacia la nueva solución deberá contemplar:
o Creación y activación de cuentas administrativas en la consola de gestión en la nube correspondiente.
o Alta y verificación de dominios, incluyendo validación de conectividad.
o Habilitación de los puertos requeridos para el tráfico de correo electrónico y sincronización de usuarios mediante servicios de directorio (LDAP, Active Directory, Entra ID u otros).
o Migración completa de configuraciones y políticas: listas blancas/negras, reglas de remitentes/destinatarios, filtros de contenido y archivos adjuntos.
o Sincronización de usuarios para habilitar mecanismos de autenticación centralizada (ej. SSO).
o Actualización de registros de enrutamiento de correo (MX o equivalentes).
o Verificación integral del flujo de correo entrante y saliente, así como pruebas funcionales completas.
o Documentación detallada del proceso de transición y respaldo de la configuración original para fines de auditoría o reversión.
o Integración de la solución con la infraestructura disponible.
o Realización y validación de pruebas de integración.
o La etapa de implementación no podrá exceder un (1) mes.

NOTA:
· Todas las actividades anteriores se deben realizar en las instalaciones de la Alcaldía de Medellín, sin costo para esta.

1.10. GARANTIA DE LA SOLUCIÓN

· La solución debe garantizar la disponibilidad del servicio de la solución SaaS, con un compromiso de entrega de mensajes de correo electrónico con una disponibilidad mínima del 99.9% cada mes calendario, siempre que la suscripción no haya sido suspendida por ninguna razón. Este compromiso se aplica a la capacidad de entregar mensajes de correo electrónico desde y hacia los servidores de Barracuda, exceptuando situaciones que no estén bajo el control de Barracuda, como problemas de infraestructura local o fallos en la conexión a Internet.
· La solución debe contar con un compromiso de disponibilidad del 99.9% para acceder a la consola de gestión de la plataforma, exceptuando tiempos de mantenimiento programado, emergente o interrupciones solicitadas por el cliente.
· La solución debe contar con la migración a nuevas versiones del software y actualizaciones dentro del plazo acordado, siempre conforme a las políticas del fabricante.
· Garantía de 1 año a partir del momento de la entrega a satisfacción, una vez que la solución esté completamente operativa y en producción.
· En caso de requerirse reemplazos, Barracuda debe realizar el envío inmediato tras la notificación formal de del distrito de Medellín, y todos los costos de envío, nacionalización y otros gastos relacionados serán cubiertos por el contratista.
· En caso de que se necesite escalar un problema al área de desarrollo de Barracuda, el tiempo que demande resolver la falla debe ser compensado, extendiendo la fecha de finalización del

contrato, ajustando el vencimiento del licenciamiento y la atención de requerimientos e incidentes.

1.11. ENTREGABLES

· El contratista debe entregar documento formal indicando la forma como se escalarán los casos de soporte acorde a los ANS descritos anteriormente, plazo para entrega: 8 días calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Si se presentan cambios en la configuración del equipo, el contratista debe entregar documento con la modificación, plazo para entrega: un (1) mes calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· El contratista debe entregar documento que evidencia el suministro de las licencias, esto deberá realizarse dentro de los 8 primeros días posteriores a la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Constancia del personal certificado en la solución expedida directamente por el fabricante, se debe entregar inmediatamente se realice la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Entrenamiento en el manejo de la herramienta, con una duración de 24 horas dictadas a mínimo diez (10) personas, con su respectivo certificado de asistencia, en las instalaciones de la Alcaldía de Medellín, plazo treinta (30) días calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Certificación canal autorizado, plazo ocho (8) días calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Certificación de garantía de un (1) año para el software, plazo ocho (8) días calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Manuales y documentación actualizada de la última versión para la administración, configuración, parametrización e instalación de la solución implementada en la Alcaldía de Medellín, plazo ocho (8) días calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Plan de contingencia para la plataforma, plazo un (1) mes calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· El contratista deberá suministrar datos de contacto para soporte y un instructivo de cómo generar los casos, plazo ocho (8) días calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II. Para este punto, cabe aclarar que si algún canal para generar un soporte cambia, este documento debe ser actualizado inmediatamente.
· Plan de trabajo y metodología de implementación de la solución, el cual contenga el reporte de las acciones a tomar, se debe entregar inmediatamente se realice la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Diagramas de la plataforma y su integración con terceros de ser necesarios, plazo un (1) mes calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Diagramas de flujo de diseño del sistema, plazo un (1) mes calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Cronograma de servicio de soporte preventivo incluida en la solución, plazo un (1) mes calendario a partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.
· Documento que certifique fecha de inicio y terminación del soporte; esto de acuerdo al ítem: #Los 12 meses de soporte iniciaran a partir de implementación y puesta en marcha de la plataforma, previa autorización del Supervisor". Plazo inmediatamente finalice la implementación de

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

la plataforma.

· El contratista debe entregar Cronograma de servicio de mantenimiento preventivo incluida en la solución, plazo para entrega: 8 días calendario partir de la marcación electrónica de inicio en la plataforma transaccional Secop II.

El mantenimiento preventivo, tiene como objetivo verificar el estado de la solución, configuraciones, actualizaciones y mejores prácticas, por lo tanto, debe contener como mínimo:

· Verificación de la solución
· Revisión de políticas y configuraciones
· Recomendaciones e informe de la visita

Toda la documentación, capacitación, información, manuales y demás textos deben ser en español.

1.12. ACUERDOS DE NIVELES DE SERVICIO (ANS)

De acuerdo con su naturaleza, los incidentes de soporte con el hardware y/o software se pueden clasificar como: Críticos, mayores, medianos o menores; por lo tanto, la atención será regida bajo las siguientes prioridades:

· Prioridad 1 (Critico): La red está #caída" o el impacto sobre su operación es crítico. Todas las partes involucradas se comprometen a dedicar recursos de tiempo completo 24x7 (las 24 horas del día, los 7 días de la semana), de acuerdo al nivel adquirido, para resolver la situación. Máximo una (1) hora después de reportado el incidente por alguno de los medios de comunicación, un ingeniero experto y certificado en la tecnología debe comunicarse con el personal encargado de los equipos en cuestión de la Subsecretaria de Tecnología y Gestión de la Información del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, para otorgar la solución del problema remotamente, si el caso lo amerita debe ser escalado para que en el transcurso de las siguientes cuatro (4) horas a un ingeniero experto y certificado en esta tecnología otorgue solución del problema en sitio.

· Prioridad 2 (Mayor): La operación de los canales está severamente degradada o aspectos importantes de la operación del negocio se ven afectados negativamente por el desempeño inadecuado de estos. Todas las partes involucradas se comprometen a dedicar recursos de tiempo completo 24x7 (las 24 horas del día, los 7 días de la semana), durante las horas de oficina estándares para resolver esta situación. Máximo cuatro (4) horas después de reportado el incidente por alguno de los medios de comunicación, un ingeniero experto y certificado en la tecnología debe comunicarse con el personal encargado de los equipos en cuestión de la Subsecretaria de Tecnología y Gestión de la Información del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, para otorgar la solución del problema remotamente, si el caso lo amerita debe ser escalado para que en el transcurso de las siguientes veinticuatro (24) horas un ingeniero experto y certificado en esta tecnología otorgue solución del problema en sitio.

· Prioridad 3 (Media): El desempeño operativo de los canales está deteriorado, mientras que las operaciones del negocio funcionan normalmente. Las partes comprometen recursos durante las horas de oficina normales (lunes a viernes de 8:00 a.m. a 6:00 p.m.), para restaurar el servicio a niveles satisfactorios. Máximo setenta y dos (72) horas después de reportado el incidente por

alguno de los medios de comunicación, un ingeniero experto y certificado en la tecnología debe comunicarse con el personal encargado de los equipos en cuestión de la Subsecretaria de Tecnología y Gestión de la Información del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, para otorgar la solución del problema remotamente, si el caso lo amerita debe ser escalado para que en el transcurso de las siguientes noventa y seis (96) horas un ingeniero experto y certificado en esta tecnología otorgue solución del problema en sitio.

· Prioridad 4 (Menor): Se requiere información o asistencia sobre las capacidades de los productos, o sobre Instalación o configuración. Las partes se comprometen a entregar recursos durante las horas de oficina normales (lunes a viernes de 8:00 a.m. a 6:00 p.m.), para entregar la información o el soporte requerido. Máximo en noventa y seis (96) horas debe ser atendido y solucionado el requerimiento.

En caso de presentarse retrasos en el cumplimiento de los acuerdos de niveles de servicio detallados anteriormente, que sean atribuibles al contratista y que a juicio del supervisor del contrato pongan en riesgo la continuidad en la prestación del servicio, se procederá a plasmar en informe de supervisión la situación presentada, con el fin de iniciar el correspondiente proceso administrativo sancionatorio a que haya lugar, de conformidad con la normatividad que rige la materia.

1.13. MEDIOS POR DONDE SE PUEDE SOLICITAR UN SOPORTE TÉCNICO REQUERIDO POR EL DISTRITO ESPECIAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN DE MEDELLÍN

Los soportes se pueden solicitar y prestar atención por los siguientes medios de comunicación:

· Soporte correo electrónico: Respuesta a través de un buzón de correo electrónico de soporte informado con anticipación, y deberá ser atendido de acuerdo a la criticidad del problema que están descritos en los Acuerdos de Nivel de Servicio (ANS), si el buzón es modificado, éste deberá ser informado con anterioridad al cambio.

· Soporte telefónico: Si el número telefónico o los números telefónicos informados cambian, estos deben ser especificados con anterioridad, y deberá ser atendido de acuerdo a la criticidad del problema que están descritos en los Acuerdos de Nivel de Servicio (ANS).

· Soporte remoto: Para conectarse remotamente con el hardware, deberá contar con previa autorización por parte del Líder de Infraestructura Tecnológica, con el fin de garantizar la seguridad y control en el acceso.

· Soporte por chat: Deberá ser atendido de acuerdo a la criticidad del problema que están descritos en los Acuerdos de Nivel de Servicio (ANS), si el chat es modificado, éste deberá ser informado con anterioridad al cambio.

· Soporte en sitio: Deberá ser atendido de acuerdo a la criticidad del problema que están descritos en los Acuerdos de Nivel de Servicio (ANS).

1.14. OTRAS CONSIDERACIONES.

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

Las siguientes consideraciones deben estar incluidas:

· Las especificaciones técnicas requeridas son mínimas, por lo tanto, se pueden ofertar mejores características.
· Se debe especificar en sus manuales, datasheets y documentos relacionados si certifica cada ítem de la propuesta.
· La instalación deberá realizarse por personal certificado en la herramienta.
· Las actualizaciones que surjan durante el contrato y sean necesarias para garantizar el uso eficiente de la herramienta serán entregadas y prestadas por el contratista bajo su responsabilidad y sin costo adicional, así mismo de informarlas a la mayor brevedad para realizar su instalación ya sea remotamente bajo las condiciones del numeral anterior (medios por donde se puede solicitar un soporte técnico) o en sitio.

1.15 ITEMS DEL PROCESO - CANTIDADES PROYECTADAS

Se requiere una (1) solución integral de protección del correo electrónico basada en la nube, que permita prevenir, detectar, mitigar y responder de forma automatizada a amenazas avanzadas como phishing, ransomware, suplantación de identidad (BEC), malware, y ataques dirigidos (spear phishing). La solución debe garantizar la continuidad operativa del servicio de correo electrónico en caso de fallas, así como brindar capacidades de respaldo, archivado, y cumplimiento normativo.
Todos sus componentes y garantía.
· Todos sus componentes de software y licencias.
· Todos los servicios de instalación e implementación en sitio.
· Soporte de la solución.
· Entrenamiento de la solución.

Por lo tanto, la propuesta económica debe venir discriminada en los siguientes ítems:

1. Licenciamiento por 1 año del AntiSpam Barracuda Cloud Email Protection Advanced para 16.000 correos
2. Soporte y Actualizaciones por 1 año

1.16 TRANSFERENCIA DE CONOCIMIENTO

Desarrollar cuatro (4) sesiones de transferencia de conocimiento y sensibilización para mínimo (10) funcionarios de la entidad, la cual debe ayudar a identificar el funcionamiento y manejo de la Plataforma La solución Barracuda, también debe ayudar a identificar situaciones sospechosas que puedan mitigar el contagio software malicioso en la plataforma tecnológica; estas sesiones pueden ser virtuales y serán agendadas por el supervisor del contrato de manera trimestral; previa concertación con el proveedor.

Se deberá dar cumplimiento a una reunión cuatrimensual, mínimo de dos (2) horas cada una, en las cuales el proveedor indique si se han generado nuevas características en la solución, la mejor manera de aprovecharlas, brindando orientación frente al tratamiento de amenazas, las modificaciones definidas por el fabricante para su tratamiento y relacionar las mejores prácticas a seguir para mitigar el riesgo.

Adicionalmente, se deberá plantear acciones de mejora a las plataformas existentes en el Distrito y el conglomerado público para generar sinergia en los procesos y en los sistemas de la entidad, dando cumplimiento Decreto 0310 de 2022, por el cual se reglamenta el Acuerdo 016 de 2020 "Modelo de compras públicas socialmente responsable”

REQUISITOS HABILITANTES TÉCNICOS:

EXPERIENCIA GENERAL DEL PROPONENTE:

Para la verificación de la experiencia se tomarán los contratos ejecutados por el proponente, ya sea individualmente o en consorcio o unión temporal que estén registrados en el RUP, de los cuales el proponente deberá relacionar en el formato Experiencia del Proponente, aquellos con los que pretende acreditar las condiciones exigidas en este pliego. No se tendrán en cuenta para la evaluación los contratos que no estén registrados en el RUP.

Para ser considerado hábil el proponente deberá acreditar hasta cinco (5) contratos ejecutados, debidamente certificados en el Registro Único de Proponentes, identificados en el clasificador de bienes y servicios en el tercer nivel, en al menos uno tres (3) de los códigos mencionados a continuación, cuyo objeto y/o alcance y/o actividades contemplen la solución barracuda. La sumatoria de ellos deberán ser iguales o superiores a 100% del presupuesto oficial expresado en salarios mínimos mensuales legales vigentes SMMLV.

Código	Descripción
43222500	Equipo de seguridad de la red
43233200	Software de seguridad y protección
81111801	Seguridad de ordenadores, redes o internet
81112200	Mantenimiento y soporte de Software
81112500	Servicios de alquiler o arrendamiento de licencias software

EXPERIENCIA GENERAL PROPONENTE PLURAL:

El proponente plural deberá acreditar experiencia en las condiciones indicadas anteriormente, mediante contratos debidamente certificados en el Registro Único de Proponentes (RUP) en los códigos solicitados.

El valor a acreditar por cada uno de los integrantes del consorcio, unión temporal u otra forma de asociación permitida por la ley, deberá corresponder a su porcentaje de participación en la forma asociativa y expresada en Salarios Mínimos Mensuales Legales Vigentes (SMMLV). En todo caso, cada integrante deberá acreditar como mínimo un (1) contrato, independientemente del número de integrantes de la forma asociativa. Si el proponente plural se conforma por un número mayor al número de contratos solicitados, el proponente informará cuales de los contratos aportados se deberán tener en cuenta para la verificación de la experiencia, sin perjuicio en todo caso de que, a cada uno de los integrantes de la forma asociativa, le corresponde acreditar un (1) contrato que

corresponda a su porcentaje de participación en el correspondiente proponente plural.

EXPERIENCIA GENERAL DIFERENCIAL:

Con fundamento en el Artículo 2.2.1.2.4.2.18 respecto de las Mipyme, del Decreto 1082 de 2015, adicionado por el artículo 3 del del Decreto 1860 de 2021, las Entidades Estatales establecerán condiciones habilitantes diferenciales que promuevan y faciliten la participación en los procedimientos de selección competitivos. En este sentido, para el presente proceso se establece el criterio diferencial descrito a continuación únicamente para la experiencia general.

Cabe aclarar que la aplicación de tal criterio diferencial no regirá en las convocatorias limitadas a Mipymes que se realicen conforme a los artículos 2.2.1.2.4.2.2 y 2.2.1.2.4.2.3 del Decreto 1860 de 2021.

EXPERIENCIA PARA MIPYME

De acuerdo con el artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, adicionado por el artículo 3 Decreto 1860 de 2021, el proponente individual o plural que cuente con la calidad de Mipyme deberá acreditar experiencia en las condiciones indicadas en la Experiencia General, no obstante, podrá acreditar experiencia hasta un contrato adicional al exigido, además, la sumatoria de estos contratos deberá ser igual o superior a 10% menos de lo exigido frente al presupuesto oficial expresado en salarios mínimos mensuales legales vigentes SMMLV.

ACREDITACIÓN DE CONDICIÓN DE MIPYME

Para que un proponente, singular o plural, pueda acceder a criterios diferenciales para Mipyme en el presente proceso, deberá acreditar su condición de la siguiente manera:

i. Las personas naturales, mediante el formato Acreditación de Mipyme expedido por ellos y un contador público, adjuntando copia del registro mercantil, en el que se certifique el cumplimiento de los criterios para ser Mipyme, de conformidad con en el artículo 2.2.1.13.2.2 del Decreto 1074 de 2015.

ii. Las personas jurídicas mediante formato Acreditación de Mipyme expedido por el representante legal y el contador o revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación, en el que se certifique el cumplimiento de los criterios para ser Mipyme, de conformidad con en el artículo 2.2.1.13.2.2 del Decreto 1074 de 2015.

En todo caso, las Mipyme también podrán acreditar esta condición con la copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al cierre del proceso.

Para los casos de propuestas presentadas por Consorcios o Uniones Temporales, solo se aplicarán los criterios diferenciales si por lo menos uno de los integrantes acredita la calidad de Mipyme y tiene una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal.

NOTA 1: Las entidades sin ánimo de lucro, diferentes a las establecidas en el Decreto 142 de 2023 no serán consideradas para la aplicación de este criterio diferencial, toda vez que el Decreto 142 de 2023 definió dicho tratamiento únicamente para las cooperativas y entidades de la economía solidaria, las asociaciones conformadas por sujetos de especial protección constitucional, asociaciones de pequeños productores locales y productores locales agropecuarios cuyos sistemas productivos pertenezcan a la Agricultura. Campesina, Familiar y Comunitaria, catalogadas como Mipymes. Así de acuerdo con la normativa vigente, las entidades sin ánimo de lucro que no se encuentren en la anterior categoría no serán consideradas para la aplicación de este criterio diferencial, toda vez que no persigue el reparto de utilidades entre sus miembros, sino que su objeto está destinado a realizar una actividad de interés general sin esperar a cambio un reparto de ganancia en proporción a sus utilidades.

AVAL DE LA PROPUESTA.

El representante legal o apoderado del proponente individual persona jurídica o el representante legal o apoderado de la estructura plural, debe acreditar que posee título en la rama de la INGENIERÍA DE SISTEMAS, INGENIERÍA INFORMÁTICA, INGENIERÍA ELECTRÓNICA, INGENIERÍA TELECOMUNICACIONES, INGENIERÍA EN TELEMÁTICA, INGENIERÍA SISTEMAS DE INFORMACIÓN o INGENIERÍA EN DESARROLLO DE SOFTWARE, para lo cual adjuntará copia de la tarjeta profesional y del certificado de la vigencia de matrícula profesional expedida por el COPNIA o Consejo Profesional en la respectiva rama de la ingeniería, según corresponda, con una vigencia no superior de 6 meses contados a partir de la fecha de cierre del Proceso de Contratación. El requisito de la tarjeta profesional se puede suplir con el registro de que trata el artículo 18 del Decreto - Ley 2106 de 2019.

En caso de que el representante legal o apoderado no posea título de una de las profesiones mencionadas, la oferta debe ser avalada por un ingeniero en las profesiones requeridas, para lo cual debe adjuntar los documentos solicitados.

CERTIFICACIÓN PROFESIONAL EN INGENIERÍA.

El representante legal del proponente deberá entregar documento donde se certifique que se cuenta con mínimo un (1) profesional en la rama de la INGENIERÍA DE SISTEMAS, INGENIERÍA INFORMÁTICA, INGENIERÍA ELECTRÓNICA, INGENIERÍA TELECOMUNICACIONES, INGENIERÍA EN TELEMÁTICA, INGENIERÍA SISTEMAS DE INFORMACIÓN o INGENIERÍA EN DESARROLLO DE SOFTWARE; vinculado o por prestación de servicios a su empresa que atienda lo respectivo al objeto y deberá también entregar constancia expedida directamente por el fabricante de que este profesional o profesionales vinculado (s) o contratista (s) está certificado en La solución Barracuda.

Para ello, el proponente deberá diligenciar y firmar el formato compromiso de cumplimiento profesional en ingeniería y presentarlo con su propuesta.

CERTIFICADO FABRICANTE # DISTRIBUIDOR.

El proponente individual o uno de los integrantes del proponente plural deberá aportar certificado

emitido directamente por el fabricante de la solución La solución Barracuda no superior a un año de la fecha de cierre del proceso, en el cual exprese que el proponente es distribuidor autorizado y que el certificado este vigente.

CERTIFICADO DE MESA DE AYUDA Y VINCULACION DEL PERSONAL REQUERIDO

Certificación del proponente que se cuenta con una mesa de ayuda, ubicada en el Área Metropolitana del Valle de Aburra, con personal certificado en la solución residente en el Área Metropolitana del Valle de Aburra; este certificado se solicita, con el fin de que cuando no se puede realizar conexión remota por algún inconveniente y el caso de soporte lo amerite se debe otorgar solución del problema en sitio, de acuerdo a los ANS descritos.

Para ello, el proponente deberá diligenciar y firmar el Formato compromiso mesa de ayuda y vinculación de personal requerido y presentarlo con su propuesta.

CUMPLIMIENTO FICHA TÉCNICA.

El proponente deberá aportar el documento en mención, con lo cual se compromete con el cumplimiento de las especificaciones técnicas del bien o servicio de características técnicas uniformes y de común utilización.

OBLIGACIONES DE LAS PARTES

OBLIGACIONES DEL CONTRATISTA

1. Cumplir con el soporte técnico y mantenimiento del sistema y plataforma de La solución Barracuda de acuerdo a las especificaciones esenciales.
2. Atender los requerimientos solicitados por el supervisor del contrato, en el tiempo de respuesta establecido en los Acuerdos de Niveles de Servicio (ANS).
3. Comunicar al supervisor del contrato sobre algún cambio en el esquema de licenciamiento y este no podrá afectar los compromisos financieros adquiridos.
4. Definir los planes de acción a implementar que se deriven de algún cambio en el esquema de licenciamiento. El contratista deberá hacerle seguimiento a estos planes de acción.
5. Garantizar la prestación del servicio con las especificaciones de tipo técnico establecidas en el estudio previo, el contrato y los demás documentos del proceso que hacen parte integral del mismo.
6. Aceptar y firmar el acuerdo de confidencialidad entregado por del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín.
7. Cubrir las garantías contractuales estipuladas en el contrato y garantizar la ampliación y modificación de las mismas en caso de ser necesario.
8. Cumplir con el objeto contractual dentro del plazo establecido para la ejecución del mismo.
9. Garantizar la disponibilidad en la atención durante la vigencia del contrato.
10. Contar con un Coordinador o Administrador quien será el enlace con el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, para prestar atención personalizada a los requerimientos y/o dudas que se presenten en el desarrollo del contrato, según los canales de soporte descritos en las especificaciones técnicas.

Centro Administrativo Distrital - CAD - Calle 44 Nro 52-165
Línea Única de Atención a la Ciudadanía (57)6044444144
www.medellin.gov.co
MEDELLIN - Colombia

11. Velar por conservar las configuraciones de que recomiende el fabricante y por un uso óptimo de la plataforma en cuanto a sus funcionalidades.
12. Validar periódicamente el licenciamiento y las mejoras a este, con el propósito de que el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, no viole en ningún momento un incumplimiento por ello.
13. Abstenerse de hacer uso, bajo ninguna circunstancia de las bases de datos o cualquier otro tipo de información que contengan datos sensibles, a la cual tendrá acceso con ocasión de este contrato, salvo cumplimiento de las excepciones señaladas en el artículo 6 de la Ley 1581 de 2012.
14. Permanecer a paz y salvo en el pago de aportes al sistema de seguridad social integral, parafiscales y contratación de aprendices, durante todo el tiempo de ejecución del contrato y acreditar estar a paz y salvo cada vez que se lo requiera el Supervisor de la Entidad, por cuanto es un requisito previo para los pagos de acuerdo a lo dispuesto en el artículo 23 de la Ley 1150 de 2007.
15. Presentar el Certificado y/o constancia de la autoevaluación de estándares mínimos del SGSST expedida por su ARL vigente, donde se acredite el nivel de cumplimiento de la resolución 0312 de 2019 y su respectivo plan de mejoramiento.
16. Implementar la solución y configuración de cada uno de los componentes técnicos especificados dentro de los términos establecidos, en un plazo máximo de un (1) mes calendario, a partir de la entrega del equipo.
17. Los doce (12) meses de soporte, iniciaran a partir de implementación y puesta en marcha de la plataforma, previa autorización del Supervisor.
18. Las demás que se deriven de la naturaleza del contrato y que garanticen su cabal y oportuna ejecución.

OBLIGACIONES DEL CONTRATISTA REFERENTE AL CUMPLIMIENTO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO (SG-SST)

El contratista debe cumplir las disposiciones contempladas en el Decreto 1072 de 2015 y la Resolución 0312 de 2019 y las demás disposiciones vigentes en materia de Seguridad Social y Seguridad y Salud en el Trabajo. Esta obligación será verificada por los supervisores o interventores según aplique, con los siguientes documentos:

1. La Autoevaluación del SGSST o autoevaluaciones del año en curso. Conforme a los resultados de la autoevaluación que aporte el contratista, éste asume unas obligaciones que están expresas en el artículo 28 Resolución 0312 de 2019, las cuales serán verificadas por el supervisor según sea el caso.

2. Plan de Trabajo del SG-SST acorde a la autoevaluación o autoevaluaciones del año en curso.

3. En los contratos donde el contratista deba dotar de elementos de protección personal, el supervisor debe constatar en campo dicha obligación, y solicitar al contratista formato de entrega de los elementos de protección personal que lleve la firma de los trabajadores que están prestando sus servicios en el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, dejando todas las evidencias en el informe parcial de supervisión, y debe ser revisada en cada pago.

OBLIGACIONES DEL DISTRITO ESPECIAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN DE

MEDELLÍN

1. Cancelar al contratista el valor del contrato, de acuerdo a la forma de pago establecida. Previa presentación de las facturas o documentos equivalentes debidamente legalizados con todos los soportes que aseguren que los bienes o servicios fueron recibidos a entera satisfacción por parte del supervisor.
2. Asignar supervisor para vigilar el desarrollo y ejecución del contrato.
3. Suministrar la información que requiera EL CONTRATISTA de manera oportuna en ocasión a la ejecución del presente contrato.
4. Informar y acompañar la solución de los incidentes o soportes.
5. Verificar el cumplimiento del pago de salarios, honorarios y demás obligaciones laborales, así como los aportes al sistema de seguridad social integral conforme a lo señalado en el artículo 50 de la Ley 789 de 2002 y normas reglamentarias.
6. Velar por el Cumplimiento de las disposiciones contempladas en el Decreto 1072 de 2015, la Resolución 0312 de 2019 y las demás disposiciones vigentes relacionadas con el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) por parte del contratista.
7. Verificar el Certificado y/o constancia de la autoevaluación de estándares mínimos del SGSST expedida por su ARL vigente, donde se acredite el nivel de cumplimiento de la resolución 0312 de 2019 y su respectivo plan de mejoramiento.