La entidad designada por la Corporación Colombia Digital que tiene por objetivo de garantizar la disponibilidad y correcto funcionamiento de la plataforma tecnológica requiere modernizar el sistema de gestión institucional a través del fortalecimiento de la infraestructura tecnológica de la comunicaciones, información, y seguridad, través de la transformación digital de la entidad designada por la CCD, esto con el fin de servicio de calidad tanto a los usuarios internos como externos de acuerdo a las siguientes condiciones:

- **Seguridad en el acceso y tráfico de red.**

Esta solución integral de telecomunicaciones permitirá asegurar y fortalecer el procesamiento de información y conectividad de la totalidad de los servicios de TI, prestados a funcionarios ubicados en el nivel central de la entidad que designe la Corporación Colombia Digital, y en el nivel desconcentrado en las Gerencias Departamentales, asegurando siempre la continuidad de la operación hacia el cliente externo e interno.

A continuación, se presenta el principal componente:

Servicios	Componentes
Seguridad	Seguridad en el acceso y tráfico de red.

La solución deberá aumentar la seguridad del tráfico de red y de la información.

ESPECIFICACIONES TÉCNICAS MÍNIMAS GENERALES.

Seguridad en el acceso y tráfico de red .

A través del presente proceso la entidad en materia de seguridad requiere:

RENOVACION DE SOPORTE, DERECHO DE ACTUALIZACIÓN Y GARANTIA DE LOS PRODUCTOS FORTINET FAI-3500F-BDL-331 Y EL FNC-CAVM

La entidad que designe la Corporación Colombia Digital requiere la renovación de soporte, derecho de actualización y garantía de los productos Fortinet FAI-3500F-BDL-331 y el FNC-CAVM por un (1) año de seguridad informática de la entidad designada por la Corporación Colombia Digital, con el objetivo de garantizar la disponibilidad y correcto funcionamiento de la plataforma de seguridad informática actual, estableciendo las acciones necesarias para la resolución de las incidencias presentadas en dicha infraestructura y aportando el nivel de servicio necesario para la administración y utilización de esta de acuerdo a las siguientes condiciones:

FORTINET FAI-3500F-BDL

- Entregar el documento en el cual conste el soporte y garantía de la solución implementada, por parte del proveedor, durante un periodo de un (1) año, posterior al recibo a satisfacción
- Prestar los servicios de soporte, entrega de licenciamiento, hardware y software en las instalaciones de la entidad ubicada en el nivel central.
- La solución debe tener garantía y soporte técnico de fábrica en esquema 7x24x365 durante un (1) año.
- La solución debe contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 1 año en un esquema 7x24x365, incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos

asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono.

- El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil y no hábil por el tiempo contratado
- Se deben incluir actividades de mantenimiento, las cuales se realizarán como mínimo un (1) mantenimiento preventivo al año para minimizar problemas y mantener los sistemas actualizados, cuando este sea requerido por la entidad, durante el periodo de garantía y soporte que es de un (1) año. En cuanto a los mantenimientos correctivos se deben realizar los que sean necesarios con el fin de garantizar la disponibilidad del servicio, durante el periodo de garantía y soporte que es de un (1) año.
- Se deben incluir las actividades necesarias para atender las solicitudes de la entidad que designe la Corporación Colombia Digital durante el contrato, que podrán incluir las siguientes actividades:
    - Cambios de Configuraciones.
    - Acompañamiento en migraciones.
    - Afinamientos
    - Hardening
    - Consultas e implementación de nuevas funcionalidades
- Realizar visitas cada tres (3) meses durante la vigencia del contrato en las cuales se deben validar las configuraciones de los equipos y realizar los ajustes correspondientes en las reglas de configuración y realizar las recomendaciones que se requieran a los administradores de las plataformas.
- Mantener actualizados los niveles de firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante.
- Al finalizar cada visita correctiva y/o preventiva el proveedor deberá generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones, y si hubo cambio de software y/o en la configuración.
    - El horario de atención para el mantenimiento correctivo y preventivo deberá ser de 7x24 en sitio, sin costo adicional para la entidad.
    - Realizar y documentar entre otras, las siguientes actividades:
    - Nuevas configuraciones y migraciones solicitadas por la Entidad.
- Configuración e implementación de la solución, con el resultado de las pruebas incluyendo evidencias (captura de pantallas, fotos).
- Realizar transferencia de conocimientos para cinco (5) funcionarios de la entidad, la cual debe incluir por lo menos temas de administración, configuración y afinamiento de la solución implementada.
- El proveedor debe brindar capacitación oficial de fabricante para cinco (5) funcionarios de la entidad sobre la operación y administración de la solución.
- debe contar con el máximo nivel de membresía del fabricante, para lo cual debe adjuntar el certificado de distribuidor autorizado del fabricante con fecha no mayor a 60 días anteriores al cierre del proceso, donde se evidencie el nivel de membresía. Las certificaciones deben dirigirse a la entidad designada por la Corporación Colombia Digital.

FNC-CAVM

- Entregar el documento en el cual conste el soporte y garantía de la solución implementada, por parte del proveedor, durante un periodo de un (1) año, posterior al recibo a satisfacción
- Prestar los servicios de soporte, entrega de licenciamiento, hardware y software en las instalaciones de la entidad ubicada en el nivel central.
- La solución debe tener garantía y soporte técnico de fábrica en esquema 7x24x365, durante un (1) año
- La solución debe contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 1 año en un esquema 7x24x365, incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono.
- El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil y no hábil por el tiempo contratado
- Se deben Incluir actividades de mantenimiento, las cuales se realizarán como mínimo dos (2) mantenimiento preventivo al año para minimizar problemas y mantener los sistemas actualizados, cuando este sea requerido por la entidad, durante el periodo de garantía y soporte que es de un (1) año. En cuanto a los mantenimientos correctivos se deben realizar los que sean necesarios con el fin de garantizar la disponibilidad del servicio, durante el periodo de garantía y soporte que es de Un (1) año.
- Se deben incluir las actividades necesarias para atender las solicitudes de la entidad designada por la CCD durante el contrato, que podrán incluir las siguientes actividades:
    - Cambios de Configuraciones.
    - Afinamientos.
    - Acompañamiento en migraciones.
    - Consultas e implementación de nuevas funcionalidades
- Realizar visitas cada tres (3) meses durante la vigencia del contrato en las cuales se deben validar las configuraciones de los equipos y realizar los ajustes correspondientes en las reglas de configuración y realizar las recomendaciones que se requieran a los administradores de las plataformas.
- Mantener actualizados los niveles de firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante
- Realizar la re parametrización y configuración de la solución en caso de ser necesaria.
- Al finalizar cada visita correctiva y/o preventiva el proveedor deberá generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones, y si hubo cambio de software y/o en la configuración.
- El horario de atención para el mantenimiento correctivo y preventivo deberá ser de 7x24 en sitio, sin costo adicional para la entidad.
- Realizar y documentar entre otras, las siguientes actividades:
- Nuevas configuraciones y migraciones solicitadas por la Entidad.
- Configuración e implementación de la solución, con el resultado de las pruebas incluyendo evidencias (captura de pantallas, fotos)"

Presentar junto con la oferta, el certificado de distribuidor autorizado del fabricante con fecha no mayor a 30 días anteriores al cierre del proceso, donde se evidencie que es PARTNER EXPERT del fabricante Fortinet, con especialización en Operational Technology y Security Operations, Las certificaciones deben dirigirse a la entidad designada por la CCD.

RENOVACION DE SOPORTE, LICENCIAMIENTO, ACTUALIZACIÓN Y ALTA DISPONIBILIDAD DE PLATAFORMAS FORTINET DE SEGURIDAD INFORMÁTICA EN NUBE DE LA ENTIDAD DESIGNADA POR LA CCD

La entidad designada por la CCD dispone actualmente de plataformas Fortinet de seguridad informática en nube como es el Firewall de Nueva Generación (NGFW) Fortigate VM64-AZURE, destinado a establecer las políticas de acceso y control de comunicaciones perimetrales y segmentación de la red en nube de la entidad designada por la CCD controlando el acceso de la red corporativa.

Con el NGFW se realiza control del acceso a internet, red en nube de la entidad designada por la CCD, control de aplicaciones hacia internet, publicaciones web, control de navegación de dispositivos, herramienta fundamental para evitar accesos no deseados, denegando o permitiendo el tráfico de protocolos específicos que transmiten información dentro de la red, control total de las comunicaciones internas hacia el exterior (internet) y comunicaciones internas desde el exterior (internet) hacia la red corporativa; adicionalmente controla los túneles seguros entre dos firewall (VPN site to site) y conexiones seguras entre clientes hacia el firewall (VPN client to site); siendo uno de los elementos de seguridad más importantes de la entidad designada por la CCD, brindando un alto nivel de seguridad para la infraestructura tecnológica y la información de la Entidad.

Adicionalmente, se cuenta con un Firewall de Aplicaciones Web (WAF) Fortiweb VM para la protección de aplicaciones web publicadas en la nube de la entidad designada por la CCD contra ataques dirigidos a vulnerabilidades conocidas y desconocidas teniendo en cuenta la reputación de IP, la protección DDoS, la validación de protocolos, las firmas de ataque de aplicaciones, la mitigación de bots entre otros aspectos.

Esta solución de seguridad informática fue adquirida en el año de 2022 con un término de garantía y soporte de la solución por tres años, el cual vence en el año 2025.

Es así, que la entidad designada por la CCD requiere renovar el licenciamiento y soporte de su infraestructura de Firewall de nueva generación Fortigate, así como del Fortiweb, con el objetivo de garantizar la disponibilidad y correcto funcionamiento de la plataforma de seguridad informática actual, estableciendo las acciones necesarias para la resolución de las incidencias presentadas en dicha infraestructura y aportando el nivel de servicio necesario para la administración y utilización de esta.

1. Especificaciones técnicas

<table>
<tr><th>ITEM</th><th>DESCRIPCIÓN</th></tr>
<tr><td>1</td><td>ACTUALIZACION DEL SOFTWARE DE SEGURIDAD FORTINET</td></tr>
<tr><td>1.1</td><td>Actualizar el licenciamiento con servicios de soporte, mantenimiento y actualización, de la plataforma de seguridad FORTINET en la cual se encuentran los equipos tecnológicos de firewall de nueva generación Fortigate VM08V y Fortiweb VM 8 CPU ubicados en el data center en nube (suscripción de Azure a nombre de la la entidad designada por la CCD) de la entidad designada por la CCD.
<table>
<tr><td>Modelo</td><td>Serial</td><td>Fecha vencimiento de soporte y licencias</td></tr>
<tr><td>FortiGate VM08V</td><td>FGVM8VTM22000328
FGVM8VTM22000386</td><td>21 de abril de 2025</td></tr>
<tr><td>FortiWeb VM 8 CPU</td><td>FVVM08TM22000335
FVVM08TM22000336</td><td>21 de abril de 2025</td></tr>
</table>
Componentes actuales de la plataforma de seguridad Fortinet en nube:</td></tr>
<tr><td>1.2</td><td>Instalación, implementación y puesta en marcha de soporte y actualización del licenciamiento requerido para el correcto funcionamiento de las plataformas indicadas.</td></tr>
<tr><td>1.3</td><td>Entregar y contemplar dentro de su propuesta todas licencias, appliance virtuales, software, soporte y servicios necesarios para dar cumplimiento a las condiciones técnicas establecidas en el presente documento.</td></tr>
<tr><td>1.4</td><td>Las renovaciones son requeridas por un periodo de un (1) año en un esquema 7 x 24 ante fabricante y por lo menos con las mismas funcionalidades actuales de las plataformas para los seriales mencionados, garantizando las suscripciones de seguridad de los equipos durante el tiempo contratado e incluyendo acceso a soporte técnico de fábrica en esquema 7x24.</td></tr>
<tr><td>1.5</td><td>El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil y no hábil por el tiempo contratado.</td></tr>
<tr><td>1.6</td><td>Se deben incluir actividades de mantenimiento, las cuales se realizarán como mínimo dos (2) mantenimientos preventivos durante el año para minimizar problemas y mantener los sistemas actualizados, y/o cuando este sea requerido por la entidad, durante el periodo de garantía y soporte que es de un (1) año. En cuanto a los mantenimientos correctivos se deben realizar los que sean necesarios con el fin de garantizar la disponibilidad del servicio, durante el periodo de garantía y soporte que es de un (1) año. Estos mantenimientos deben ser realizados por personal</td></tr>
<tr><td>1.7</td><td>Se deben incluir las actividades necesarias para atender las solicitudes de la entidad designada por la CCD durante el periodo de garantía</td></tr>
</table>

	y soporte que es de un (1) año, que podrán incluir las siguientes actividades: • Cambios de Configuraciones. Acompañamiento en • migraciones. • Consultas e implementación de nuevas funcionalidades.
1.8	Garantizar la continuidad del soporte y licenciamiento de la actual plataforma de seguridad Fortinet en nube de la entidad designada por la CCD, en tanto se hace la implementación de la plataforma objeto del presente proceso de contratación.
2.	**SERVICIOS DE SOPORTE**
2.1	Prestar los servicios de soporte, entrega de licenciamiento, hardware y software en las instalaciones de la entidad designada por la CCD ubicada en el Nivel Central (Bogotá).
2.2	Realizar las Actividades necesarias para la puesta en marcha de plataforma de seguridad Fortinet, basadas en la actualización del licenciamiento y/o actualización de la misma.
2.3	Realizar la planeación de cada una de las actividades, validadas en conjunto con la entidad.
2.4	Configuración y alistamiento del software y/o hardware a la última versión estable aprobada por el fabricante para todas las plataformas renovadas e implementadas.
2.5	Pruebas de Servicio de las plataformas renovadas.
2.6	Entregar de los documentos en donde conste la actualización del licenciamiento de la plataforma de seguridad de la entidad, con sus respectivos soportes, al supervisor del contrato.
2.7	Entregar el documento en el cual conste el soporte y actualización de la plataforma renovada e implementada, por parte del contratista, durante un periodo de *un (1) año* a partir de la finalización de la implementación de la renovación solicitada.
2.8	Atención de incidentes sobre las plataformas ofertadas en un esquema 7x 24.
2.9	Consultas a través de llamadas telefónicas, correo electrónico.
2.10	Sesiones remotas y atención en sitio (en caso de requerirse) en horario hábil y no hábil. Todo con respecto a las plataformas ofertadas y objeto del presente contrato.
2.11	Realizar visitas cada 3 meses durante la vigencia del contrato en las cuales se deben validar las configuraciones de los equipos y realizar los ajustes correspondientes en las reglas de configuración y realizar las recomendaciones que se requieran a los administradores de las plataformas.

2.12	Realizar y documentar entre otras, las siguientes actividades (2.13, 2.14, 2.15, 2.16) durante un periodo de un (1) año , previa coordinación con el supervisor del contrato o quien designe la Entidad.
2.13	Revisar la consistencia de los backups realizados a la solución implementada. Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma, en forma escrita.
2.14	Configurar, afinar y revisar los logs y reportes de las plataformas.
2.15	Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante y, de ser necesario, compatibles con la plataforma de seguridad Fortinet OnPremise de la entidad.
2.16	Nuevas configuraciones y migraciones solicitadas por la Entidad.
2.17	El horario de atención para el mantenimiento correctivo y preventivo deberá ser de 7x24 en sitio, sin costo adicional para la entidad.
2.18	Al finalizar cada visita correctiva y/o preventiva el contratista deberá generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones, y si hubo cambio de software y/o en la configuración.
2.19	Contemplar todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones, sin costo adicional para la entidad.
2.20	Realizar transferencia de conocimientos para cuatro (4) funcionarios de la Entidad, la cual debe incluir por lo menos temas de administración, configuración y afinamiento de las plataformas renovadas, como mínimo cuarenta (40) horas; el plan presentado para este requerimiento debe ser aprobado por el supervisor o quien designe.
2.21	Incluir cuatro (4) cupos para la capacitación sobre la instalación y configuración de la solución de seguridad licenciada, mínimo de 48 horas de capacitación, que deben ser dictados por canal autorizado por el fabricante y en instalaciones autorizadas por el fabricante. Todas las capacitaciones presenciales deberán ser impartidas por instructores certificados y con material certificado. (Todos los costos relacionados con las capacitaciones presenciales deberán ser cubiertos en su totalidad por el contratista).

<table>
<tr><td>3.</td><td>ACTIVIDADES GENERALES</td></tr>
<tr><td>3.1</td><td>El contratista debe realizar las actividades necesarias para el cabal cumplimiento del objeto del contrato, de acuerdo con su experiencia para la entrega a satisfacción de la solución.</td></tr>
<tr><td>3.2</td><td>El tiempo máximo para la ejecución del contrato, incluidas las actividades técnicas, es de 60 días contados a partir de la firma del acta de inicio del
contrato.</td></tr>
<tr><td>4.</td><td>CERTIFICACIONES DEL FABRICANTE</td></tr>
<tr><td>4.1</td><td>Presentar junto con la oferta, el certificado de distribuidor autorizado del fabricante con fecha no mayor a 30 días anteriores al cierre del proceso, donde se evidencie que es EXPERT del fabricante Fortinet, con especialización en Public Cloud Security. Las certificaciones deben dirigirse a la entidad designada por la CCD.</td></tr>
<tr><td>4.2</td><td>Presentar con la entrega de la oferta certificación del fabricante, no menor a 30 días antes del cierre del proceso donde se evidencie que cuenta con mínimo 2 ingenieros certificados NSE4 y NSE5 o superiores de la misma certificación.
Las certificaciones deben dirigirse a la entidad designada por la CCD.</td></tr>
<tr><td>5.</td><td>ACUERDO DE NIVELES DE SERVICIO</td></tr>
<tr><td>5.1</td><td>DEFINICIONES:

Incidente: Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo. Problema: Evento que se presenta en la operación de las plataformas de seguridad informática, que produce un comportamiento o resultado diferente al esperado. Se debe tener claro que no es error del código del software sino es la falta de parámetros o prototipos no declarados o definidos en las plataformas. Servicio: Medio para entregar valor a la Entidad con resultados que proporcionen una utilidad y una garantía a las plataformas de seguridad informática (hardware y software).

Se definen las siguientes prioridades para incidentes y problemas, acordes a los niveles de servicio:
<table>
<tr><th rowspan="2">TIPO DE SOLICITUD DE SOPORTE TÉCNICO</th><th rowspan="2">Asignar responsable o reactivar estado</th><th colspan="3">HORAS HABILES</th></tr>
<tr><th colspan="3">Solución</th></tr>
<tr><th></th><th></th><th>Prioridad 1</th><th>Prioridad 2</th><th>Prioridad 3</th></tr>
<tr><td>Incidente o Problema</td><td>15 minutos</td><td>2</td><td>4</td><td>8</td></tr>
</table>
NS Prioridad 1: Sin acceso al servicio. Afecta la operación de la entidad designada por la CCD. NS Prioridad 2: Caída del servicio con conexión alterna disponible, Intermitencias en el servicio, degradación, servicio lento.
NS Prioridad 3: Impacto leve sobre el servicio que no afecta la operación del sistema.

ANS CON CALCULO MENSUAL</td></tr>
</table>

	Se definen tres niveles de servicio (NS) para restablecer servicios o cerrar requerimientos, con los siguientes tiempos de solución: La entidad designada por la CCD registra el incidente o solicitud clasificado con base en la tabla de prioridades establecidas. Una vez la entidad designada por la CCD haga el registro en el sistema, el Contratista dispondrá de 15 minutos para atender y analizar el caso y responder sobre la clasificación, solicitud de información y/o aclaraciones. En el caso en que la entidad designada por la CCD reporte incidencias que contengan temas diferentes, el contratista, dentro de los 15 minutos otorgados para dar respuesta e iniciar la atención del soporte, atenderá uno de ellos e informará a la entidad designada por la CCD para que se realicen el o los nuevos registros. Una vez la entidad designada por la CCD responda a las inquietudes del contratista, éste dispondrá de otros 15 minutos contados a partir de la respuesta dada por la entidad designada por la CCD, para reactivar la incidencia y continuar con el proceso. Los tiempos establecidos en los ANS, se suspenden cuando un incidente reportado se encuentre en estado “SE NECESITAN MAS DATOS o EN VERIFICACION CLIENTE”. EL soporte técnico contratado se prestará en los tiempos establecidos para la solución de fallas y su incumplimiento ameritará la siguiente sanción: La diferencia que se genere entre el tiempo definido en la tabla de prioridades y el efectivamente utilizado para la atención y/o solución de las fallas, deberá ser compensado por parte del contratista, de la siguiente manera: Las horas por incumplimiento de los ANS se penalizarán con horas de acompañamiento en las actividades que defina la entidad designada por la CCD, tales como: - transferencia de conocimiento técnico y funcional, parametrizaciones y acompañamiento en la operación. El tiempo de incumplimiento debe constar en los informes mensuales de ejecución del contrato, debidamente aprobadas por las partes, y por cada hora incumplida, el contratista pagará una (1) hora en cualquiera de las actividades mencionadas en el párrafo anterior, las cuales se pueden acumular, precisando que su cumplimiento se dará durante la ejecución del contrato.

Además de lo anterior, el contratista deberá cumplir con los siguientes requerimientos:

1. Ejecutar soluciones técnicas sobre incidentes y/o problemas presentados en la plataforma instalada; para lo cual se tendrá atención de las solicitudes presentadas por la entidad designada por la CCD. Para ello se debe tener en cuenta lo establecido en los acuerdos de niveles de servicio – ANS.
2. Desarrollar el objeto del Contrato, en las condiciones de calidad, oportunidad, y

obligaciones definidas en el Contrato, incluyendo las Especificaciones Técnicas y el Pliego de Condiciones.

3. Continuación Pliego Definitivo de Condiciones del contrato para suscribir la renovación de soporte, licenciamiento, actualización y alta disponibilidad de plataformas Fortinet de seguridad informática en nube de la entidad designada por la CCD.
4. Reemplazar los dispositivos que se requieran para mejorar capacidad y eficiencia de la plataforma de seguridad.
5. Responder las solicitudes presentadas por la entidad designada por la CCD relacionadas con la plataforma instalada de seguridad.
6. Contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros), requerida para que el personal asignado al proyecto pueda cumplir sus funciones.
7. Entregar a satisfacción la actualización del licenciamiento e implementación de la plataforma de Fortinet, objeto del presente proceso de contratación.
8. Garantizar la continuidad del soporte y licenciamiento de la actual plataforma de seguridad Fortinet en nube de la entidad designada por la CCD, en tanto se hace la implementación de la plataforma objeto del presente proceso de contratación.
9. Mantener actualizada la plataforma de seguridad Fortinet de la entidad.
10. Garantizar el soporte técnico de la modalidad de 7 x 24 por un (1) año .
11. Realizar visitas técnicas cada tres (3) meses durante el término de la garantía relacionada con el uso de los servicios conexos a la suscripción contratada, en las cuales se deben validar las configuraciones de los equipos, hacer los ajustes correspondientes en las reglas de configuración y realizar las recomendaciones pertinentes a la entidad designada por la CCD.
12. Entregar un reporte mensual detallado de las actividades desarrolladas, e incidentes solucionados durante la vigencia del contrato, y aquellos requeridos por el supervisor del contrato.
13. Documentar de manera técnica lo referente a las actualizaciones y la respectiva transferencia de conocimiento de los cambios realizados, entregando a la supervisión del contrato (o a quien éste designe) una copia en medio digital de los documentos de instalación y de control de cambios establecidos por la Oficina de Sistemas e Informática de la entidad designada por la CCD.
14. Proveer los medios y las herramientas idóneas para realizar las actividades contratadas.
15. Las demás que se deriven o sean inherentes al objeto y naturaleza del contrato y que garanticen su cabal cumplimiento.
16. Las demás inherentes al objeto del contrato y que por ley le correspondan

ACTIVIDAD	RESPONSABLE	FIRMA
Elaboró	Juan Felipe Lizarazo Jerez/ ingeniero apoyo Técnico	
Revisó	Pablo Sandoval / director Operativo y Técnico	