**ANEXO 3 Especificaciones Técnicas**

REFERENCIA: Proceso de Contratación N° 15804
OBJETO: Adquisición, Instalación, configuración y soporte de equipos para la red corporativa

1. DISPOSITIVOS QUE SE DEBEN ADQUIRIR: ..... 2
2. CONSIDERACIONES GENERALES ..... 2
2.1. CRONOGRAMA PROPUESTO. ..... 3
2.2. GARANTÍA Y SOPORTE DEL FABRICANTE CISCO ..... 4
2.3. SERVICIO DE SOPORTE DEL CONTRATISTA ..... 4
2.4. PRIORIZACIÓN Y ACUERDOS DE SERVICIO. ..... 5
2.5. TRANSFERENCIA DE CONOCIMIENTO ..... 6
3. SERVICIO DE IMPLEMENTACIÓN. ..... 6
3.1. DESCRIPCIÓN GENERAL. ..... 6
3.2. AUTORIZACIÓN ..... 7
3.3. GESTIÓN DE EQUIPOS DE RED. ..... 7
3.4. POSTURA DE ADMISIÓN (VERIFICACIÓN) ..... 8
3.5. AISLAMIENTO Y CUARENTENA ..... 8
3.6. REMEDIACIÓN ..... 9
4. EQUIPO DE TRABAJO ..... 9

## 1. DISPOSITIVOS QUE SE DEBEN ADQUIRIR:

| EQUIPO | MODELO/PRODUCTO | DESCRIPCIÓN | CANTIDAD |
|---|---|---|---|
| ISE | SNS-3715-K9 | Small Secure Network Server for ISE Applications | 2 |
| ISE | SNTC-24X7X4 | Small Secure Network Server for ISE Appl, (5 años) | 2 |
| ISE | UCSC-PSU1-1050W | Fuente de poder | 2 |
| Licencia | ISE-E-LIC | Cisco Identity nService Engine Essentials Subscription (5 años) | 2700 |
| Licencia | ISE-P-LIC | Cisco Identity Service Engine Premier Subscription (5 años) | 3600 |
| Licencia | L-AC-APX-5Y-S6 | licencia de Cisco AnyConnect (5años) | 3600 |
| Licencia | L-ISE-TACACS-ND= | License TACACS | 2 |
| N/A | N/A | Servicio de implementación y soporte | 1 |

## 2. CONSIDERACIONES GENERALES

A. Los equipos serán instalados la siguiente dirección: Centro Administrativo Departamental (CAD), José María Córdova, Calle 42B 52-106, piso 6 Centro de Computo (Data Center) Medellín, Antioquia, Colombia

B. El contratista debe realizar 2 revisiones lógicas de todos los equipos descritos en este documento por cada año de contrato SNTC, por cada revisión debe incluir:

B.1. Revisión IOS y LOGS, estado de salud general del equipo.

B.2. Por cada revisión se debe entregar un informe técnico, indicando las acciones de mejoras recomendadas las cuales deberá implementar el contratista. Las fechas en que se realizarán las revisiones se deben acordar con el supervisor del contrato.

B.3. El estado de salud para los dispositivos será:

B.3.1. Respaldo de configuración del dispositivo

B.3.2. Uso de CPU, consumo de memoria, Logs de temperatura, protocolos habilitados, consistencia de Backup, Versión de IOS.

B.3.3. Toma de evidencias e informe detallado.

B.3.4. Relacionar vulnerabilidades encontradas.

B.3.5. Recomendaciones sobre mejoraras en la implementación

C. El contratista deberá realizar las recomendaciones que considere necesarias sobre diseño y cambios de configuración para cumplir con los objetivos y requisitos para la óptima implementación de la solución ofertada, las cuales pueden ser aplicadas a la red cableada o inalámbrica, basados en las mejores prácticas

del fabricante Cisco, en todo caso, las recomendaciones de diseño y cambios de red deberán ser aprobadas por el supervisor del contrato.

D. El contratista deberá realizar las recomendaciones de configuración de los equipos diferentes a la solución ISE, así como el acompañamiento en la implementación de las mismas.
E. El Departamento de Antioquia realizará el despliegue de las configuraciones recomendadas para el óptimo funcionamiento de la solución conforme al a lo expuesto en el punto anterior.
F. El contratista deberá suministrar las conexiones físicas y lógicas como son conexiones de red (patch cord UTP), patch cord fibra óptica, eléctricas (cable de poder) y las demás necesarias para el óptimo funcionamiento de la solución contratada. La entidad proporcionará el espacio físico y los 4 puntos eléctricos de energía regulada 120V.
G. El contratista deberá proporcionar 4 patch cord de 5 metros categoría 6A Panduit para conectar los equipos ISE.
H. El contratista deberá correr un protocolo de pruebas acordado con El Departamento de Antioquia con el fin de garantizar el correcto funcionamiento de los servicios a implementar.
I. El despliegue del agente Cisco AnyConnect se podrá realizar a través de una GPO o a través de alguna de las herramientas con que cuenta la entidad para este fin. El contratista será responsable junto con el Departamento de Antioquia del despliegue del agente Cisco AnyConnect en los dispositivos finales.
J. El contratista deberá entregar un informe final sobre la solución implementada, debe incluir los diagramas de conexión, direcciones IP, políticas implementadas y toda la información técnica.
K. El Departamento de Antioquia suministrará toda la información relevante y necesaria para la implementación de solución ofertada.
L. El Departamento de Antioquia suministrará el espacio en sus gabinetes para la implementación de los appliances de Cisco ISE.
M. El Departamento de Antioquia proporcionará acceso remoto a la red de GOBERNACIÓN DE ANTIOQUIA a través de una conexión VPN a los equipos en caso de ser requerido, luego de la implementación.
N. El Departamento de Antioquia realizará la programación de las ventanas de mantenimiento para la ejecución del plan de implementación.
O. El Departamento de Antioquia proporcionará los certificados SSL que se requieran para la implementación del ISE.

### 2.1. CRONOGRAMA PROPUESTO.

El contratista deberá presentar un cronograma de trabajo y actividades que se desarrollaran semana por semanas, indicando mínimamente:

A. Entrega de plan de proyecto: Debe incluir los lineamientos básicos y normas a trabajar durante el desarrollo del proyecto.
B. Tiempos de pedido.
C. Entrega de equipos en el sitio.
D. Periodo de ingeniería de detalle y planeación de las migraciones.

E. Periodo de implementación.
F. Periodo de estabilización.
G. Periodo de ajustes a la plataforma.
H. Periodo de documentación y cierre final.

El cronograma de actividades para la ejecución del contrato permitirá una visión integral y detallada de las tareas a realizar, los plazos estimados para su ejecución y la secuencia adecuada de las actividades. Con el fin de lograr una planificación eficiente, asegurando que todas las etapas del proyecto se lleven a cabo de manera oportuna y coordinada, ya que se establece una línea de tiempo clara y se establecen expectativas realistas en cuanto a la finalización del proyecto.

## 2.2. GARANTÍA Y SOPORTE DEL FABRICANTE CISCO

A. El contratista debe brindar el servicio de Smartnet Total Care, de reemplazo y garantía de partes Cisco (7*24*4 soporte en sitio) de la solución adquirida
B. El contratista debe aportar el certificado que entrega el fabricante CISCO en el cual se evidencia que los equipos y licencias están cubiertos por un contrato de soporte y garantía, indicando fecha de inicio y fecha de terminación del periodo.
C. El contratista debe realizar a todo costo la actualización de software y firmware del sistema operativo que se requiera para el correcto funcionamiento de los equipos relacionados durante el periodo de la garantía.
D. El contratista debe asesorar e implementar nuevas configuraciones sobre los equipos de red CISCO-ISE durante el tiempo de soporte y garantía.
E. El contratista debe tener en cuenta que en caso de activarse un RMA (por sus en inglés) tendrá la obligación de gestionar todo el proceso de garantía, incluyendo el montaje/desmotaje, envío, configuración y puesta en funcionamiento del equipo con características técnicas iguales o superiores. Además, el contratista realizará disposición final del equipo defectuoso. En ningún caso el Departamento de Antioquia cubrirá gastos de envió de las partes o equipos defectuosos.

## 2.3. SERVICIO DE SOPORTE DEL CONTRATISTA

A. El contratista debe disponer de diferentes métodos de atención para solicitudes de soporte (matriz de escalamiento) que permita solicitar asistencia técnica para solución de problemas técnicos que se presenten en la solución instalada, durante el tiempo de soporte:
   A.1. Portal de soporte
   A.2. Correo electrónico
   A.3. Línea de atención
   A.4. Línea de atención especializada (en horario no hábil)
   A.5. Diferentes métodos para recibir soporte:
   A.6. Sesiones virtuales.

B. El contratista deberá contar con una matriz de escalamiento para gestionar los incidentes. En esta matriz se deben incluir los perfiles profesionales descritos en el numeral 4 EQUIPO DE TRABAJO.
C. Si el contratista realiza cambios en su planta de personal que modifique la matriz de escalamiento debe informar por escrito a la entidad cuales son los cambios y se debe enviar las certificaciones respectivas que cumplan con el mismo perfil.
D. El contratista debe realizar el soporte en sitio, donde se encuentra el dispositivo, en caso que el acceso remoto no sea efectivo para diagnosticar y/o solucionar el incidente, se desplazará un agente calificado al sitio en donde se reporta el problema, para agilizar su diagnóstico y solución. Los gastos de transporte y viáticos para atender los incidentes y demás actividades referentes al contrato serán asumidos por el contratista.
E. El contratista debe enviar por vía e-mail el registro y procedimiento realizado en el soporte solicitado.

## 2.4. PRIORIZACIÓN Y ACUERDOS DE SERVICIO.

| TIEMPO DE FALLA | TIEMPO DE RESPUESTA | TIEMPO DE RESTAURACIÓN | TIEMPO DE SOLUCIÓN | TIEMPO DE ENTREGA DE INFORME CONTADOS A PARTIR DE LA APLICACIÓN DE LA SOLUCIÓN DEFINITIVA |
|---|---|---|---|---|
| Prioridad 1 | 15 min | 2 horas | 4 horas | 24 horas |
| Prioridad 2 | 1 hora | 7 horas | 2 días | 48 horas |
| Prioridad 3 | 2 horas | 23 horas | 3 días | 48 horas |
| Prioridad 4 | 4 horas | NA | 5 días | NA |

**A. PRIORIDAD 1.**

A.1. La red esta caída y el servicio se encuentra interrumpido.
A.2. El equipo de ingenieros del Departamento de Antioquia como el contratista dedican tiempo completo en la resolución del caso 7x24.
A.3. El Departamento de Antioquia proporcionará el personal en sitio mientras se supere el incidente.
A.4. El contratista deberá enviar a sitio a un agente, en caso de que el soporte remoto no sea efectivo.

**B. PRIORIDAD 2.**

B.1. El servicio de la red está severamente afectado y su nivel de prestación es inaceptable.
B.2. El equipo de ingenieros del Departamento de Antioquia como el contratista dedican tiempo completo en la resolución del caso 7x24.
B.3. El contratista deberá enviar a sitio a un agente, en caso de que el soporte remoto no sea efectivo.

**C. PRIORIDAD 3.**

C.1. El desempeño de la red se encuentra degradado. El servicio es prestado con una calidad menor a la normal.

C.2. El equipo de ingenieros del Departamento de Antioquia como el contratista dedican a resolver el incidente en horario laboral (8x5)

**D. PRIORIDAD 4.**

D.1. El servicio no se encuentra afectado

D.2. Las solicitudes serán sobre nuevas configuraciones que se requieren implementar en la solución instalada.

### 2.5. TRANSFERENCIA DE CONOCIMIENTO

La transferencia se realizará en cinco (5) sesiones de cuatro (4) horas de transferencia de conocimiento (charla), exclusivamente en modo presencial, la entidad dispondrá de un espacio adecuado para la transferencia de conocimiento. El alcance de esta actividad es el siguiente:

A. Presentación del estado final de las soluciones.
B. Presentación de las experiencias de configuración y solución de problemas durante la implementación.
C. Transferencia para administración de la solución
D. Configuración básica de los equipos.
E. Transferencia en el esquema actual del cliente
F. Transferencia en casos comunes de soporte
G. Entrega y explicación de documentación de configuración e implementación del proyecto.

La transferencia de conocimiento será acordada con el supervisor del contrato.

## 3. SERVICIO DE IMPLEMENTACIÓN.

### 3.1. DESCRIPCIÓN GENERAL.

A. Implementación desde cero (sin migración de configuración) de dos (2) appliance ISE SNS 3715.
B. Se permitirá la importación de bases de datos de usuarios y dispositivos, previa autorización del supervisor del contrato.
C. Configuración HA e Integración con Active Directory (on-premises)
D. Implementación de 2700 licencias Cisco ISE Essential (ISE-E-LIC), utilizando autenticación MAB y 802.1X, generando los grupos necesarios para su funcionamiento.
E. Implementación de 3600 licencias Cisco ISE Premier (ISE-P-LIC), utilizando autenticación 802.1X, configurando toma de postura con al menos las siguientes condiciones: verificar sistema operativo, verificar parches, verificar antivirus, verificar que el PC pertenezca al dominio, verificar software de inventario.
F. Configuración de políticas de acceso y reglas de la solución ISE de autenticación y autorización.
G. Configuración de Políticas, DACL, asignación dinámica de VLANs, MAB para tráfico WIFI y tráfico Cableado.
H. Configuración de reglas de perfilado utilizando las mejores prácticas recomendadas por el fabricante que sean aplicables al contexto del proyecto y la infraestructura de red de la entidad.
I. Configuración de SNMP hacia Herramienta de Monitoreo Departamento de Antioquia.

J. Configuración de autenticación TACACS en el ISE para dispositivos del Departamento de Antioquia.
K. Configuración de respaldos de manera programada periódicamente de la infraestructura ISE.
L. El contratista debe implementar la solución de autenticación de dispositivos y usuarios a la red utilizando el protocolo IEEE 802.1X, haciendo uso de autenticación encadenada utilizando las mejores practicas recomendadas por el fabricante que sean aplicables al contexto del proyecto y la infraestructura de red de la entidad.
M. El contratista debe implementar la solución para lograr la correcta integración con una base de usuarios de AD (Active Directory) para login único de usuarios (Single Sign On). Las credenciales de usuario utilizadas al momento de la autenticación de Windows deben ser utilizadas en la autenticación de usuario en la solución de control de acceso de forma automática, sin que el usuario deba ingresar nuevamente sus credenciales.
N. Configuración de mejores prácticas recomendadas por el fabricante para la implementación del proyecto.

### 3.2. AUTORIZACIÓN

A. El contratista debe implementar asignación de VLAN asignada por el servidor de control de acceso.
B. El contratista debe implementar asignación de dominio de voz para teléfonos IP (Voice Domain).
C. El contratista debe implementar asignación de parámetro de re-autenticación 802.1X
D. El contratista debe implementar con la funcionalidad de configurar dinámicamente los puertos de acuerdo al tipo de dispositivo detectado en el puerto
E. El contratista debe implementar la personalización de atributos de autorización
F. El contratista debe implementar el agrupamiento de atributos de autorización
G. El contratista debe implementar la creación de perfiles de usuarios.

### 3.3. GESTIÓN DE EQUIPOS DE RED.

A. El contratista debe implementar la gestión de la autenticación, autorización y contabilidad en dispositivos de red como switches, ruteadores, firewalls, equipos de red inalámbrica y adicionales por medio del protocolo estándar TACACS+.
B. La gestión de AAA por medio de TACACS+ deberá permitir la autorización granular de los comandos que un administrador de red puede ejecutar en un equipo de red configurado con este protocolo.
C. El contratista debe implementar los perfiles de autorización de comandos predefinidos (out-of-the-box) para la gestión de controladores inalámbricos, ruteadores y switches, de tal manera que no se tengan que construir listas de comandos desde cero.
D. El contratista debe implementar la generación de bitácoras para auditorías de autenticaciones, autorizaciones y comandos ejecutados en los dispositivos de red configurados con TACACS+.
**D.1.** Se deberá soportar la función de proxy de protocolo TACACS+

**D.2.** Se requiere soporte de TACACS+ sobre IPv6

### 3.4. POSTURA DE ADMISIÓN (VERIFICACIÓN)

A. El contratista debe implementar la solución para la verificación de postura de estaciones de usuario en las siguientes formas:
B. Agente Instalado: Agente que se instala en la estación del usuario, encargado de la recolección de información referente a postura. El agente deberá encargarse sólo de la verificación de postura de la estación. Todo el control de nivel de acceso a la red, control de tiempo concedido y control de ancho de banda deberán ser efectuados a través del Dispositivo de Aplicación de Políticas.
C. El contratista debe implementar el Agente Any Connect para la verificación de los siguientes ítems:
   C.1. Sistema Operativo Instalado
   C.2. Verificación del Service Pack Instalado
   C.3. Llaves de Registro de Windows
   C.4. Archivos existentes en la estación del usuario
   C.5. Estatus de los servicios en ejecución en la máquina
   C.6. Existencia de Software Antivírus y AntiSpyware Instalado
   C.7. Fecha de la última actualización del Antivírus
   C.8. Estatus del software Antivírus (Habilitado o Deshabilitado)
   C.9. Verificación de Hotfixes de Windows Instalados
   C.10. Inventario de Aplicaciones instaladas
   C.11. Estado de cifrado de disco duro
   C.12. Puertos USB
D. El contratista debe implementar la solución para la verificación de la última versión de antivirus provista. La solución deberá ser capaz de verificar cuál es la última firma disponible y su fecha respectiva.
   D.1.1. Cortex - Palo Alto Networks
   D.1.2. Sophos
   D.1.3. Kaspersky
   D.1.4. ClamAV

### 3.5. AISLAMIENTO Y CUARENTENA

A. El contratista debe implementar el aislamiento y cuarentena de usuarios deberá ser orquestado a través del Sistema de Control de Acceso.
B. El contratista debe implementar la solución que permita el aislamiento de las estaciones incluso si éstas cuentan con dirección IP configurada de forma estática.
C. El contratista debe implementar el aislamiento a través de una lista de acceso descargable centralmente desde el Sistema de Control de Acceso.

### 3.6. REMEDIACIÓN

En caso del que el usuario no cumpla con los requisitos de seguridad de la estación, el contratista debe implementar la solución para proveer mecanismos de actualización en las formas siguientes:

A. Manual: El agente instalado deberá guiar al usuario en el proceso de actualización de la estación (proveyendo hipervínculos para los parches, actualización del software de antivirus, actualizaciones de WSUS) de modo que la estación cumple con las políticas de seguridad.
B. Automático: El agente instalado deberá realizar todo el proceso de forma automática.
C. La solución deberá soportar la configuración de las siguientes formas de remediación:
   C.1. Distribución de enlace web
   C.2. Distribución de archivos
   C.3. Integración con WSUS y SCCM
   C.4. Integración con Antivirus y Antispyware
D. La solución deberá proveer integración con el servidor WSUS para la instalación de parches de seguridad de Windows. El agente instalado deberá comunicarse con WUA (Windows Update Agent) para verificar si existe alguna actualización pendiente. En caso de ser necesaria alguna actualización, el agente instalado deberá iniciar una actualización utilizando WUA según el mecanismo de actualización configurado (Manual o Automático). Dicha actualización deberá ser transparente para el usuario y utilizar las APIs presentes en el agente WUA.
E. La solución deberá proveer integración con los Software de Antivirus y Antispyware listados en esta especificación. En caso de requerirse alguna actualización, el agente instalado deberá iniciar una actualización del software Antivirus y Antispyware según el mecanismo de actualización configurado (Manual u Automático). Dicha actualización deberá ser transparente para el usuario y utilizar las APIs presentes en los softwares Antivirus e Antispyware.

## 4. EQUIPO DE TRABAJO

El contratista deberá contar con el personal calificado, de acuerdo a lo requerido por la Entidad, el cual deberá estar en sitio de trabajo para la ejecución del proyecto cuando el supervisor lo solicite. El contratista debe contar durante la ejecución del contrato, con el siguiente personal que debe cumplir con los siguientes perfiles:

A. **LÍDER TÉCNICO**:
   A.1. certificación vigente: Cisco CCNP Security, con certificación de concentración (300-715 SISE).
   A.2. Estudios requeridos: profesionales de ingeniería de Sistemas, Eléctrica, Electrónica, de Telecomunicaciones, Telemática, Informática o afines entendidas como aquellas que comparten núcleo básico de conocimiento. El título debe ser expedido por una institución educativa reconocida por el Sistema Nacional de Información de la Educación Superior – SNIES– del Ministerio de Educación Nacional.
   A.3. Experiencia: Participación en mínimo 2 proyectos de implementación de equipos Cisco ISE. la cual deberá demostrarse mediante certificaciones laborales o certificaciones de contratos y/o actas de liquidación de contratos en los cuales se evidencie la experiencia requerida

A.4 Funciones:

- Levantamiento de información y requerimientos técnicos.
- Diseñar la solución que permita el control de acceso a la red según las necesidades de la entidad.
- Planear la implementación de la solución teniendo en cuenta las limitantes que pueda tener la entidad.
- Implementar la solución cumpliendo con el diseño realizado.
- Realizar ajustes post implementación.
- Monitorear la solución implementada.

B. **AGENTE TÉCNICO**:

B.1. Certificación vigente: Cisco CCNA

B.2. Titulo requerido: estudiantes universitarios con mínimo sexto semestre de carreras profesionales de ingeniería de Sistemas, Eléctrica, Electrónica, de Telecomunicaciones, Telemática, Informática o afines entendidas como aquellas que comparten núcleo básico de conocimiento

B.3. Experiencia: 2 años de experiencia en implementaciones de redes y/o seguridad.

B.4. Funciones:

- Apoyo y acompañamiento al levantamiento de información y requerimientos técnicos.
- Apoyo y acompañamiento para diseñar la solución que permita el control de acceso a la red según las necesidades de la entidad.
- Apoyo y acompañamiento para planear la implementación de la solución teniendo en cuenta las limitantes que pueda tener la entidad.
- Apoyo y acompañamiento para implementar la solución cumpliendo con el diseño realizado.
- Apoyo y acompañamiento para ealizar ajustes post implementación.
- Apoyo y acompañamiento para monitorear la solución implementada.

C. **ROL GERENTE DE PROYECTO:**

C.1. Certificación vigente: PMP y/o Scrum Master

C.2. Estudios requeridos: profesionales de ingeniería de Sistemas, Eléctrica, Electrónica, de Telecomunicaciones, Telemática, Informática o afines entendidas como aquellas que comparten núcleo básico de conocimiento. El título debe ser expedido por una institución educativa reconocida por el Sistema Nacional de Información de la Educación Superior –SNIES– del Ministerio de Educación Nacional.

C.3. Experiencia profesional en al menos un (1) proyecto de implementación de equipos de red, o equipos de seguridad perimetral debidamente terminado, como Gerente, Coordinador, Articulador, Líder y/o Director de Proyectos, que incluya revisión de la situación actual, diagnóstico o caracterización, planeación, implementación, pruebas y monitoreo.

C.4. Funciones:

- Actividades a realizar en la ejecución del contrato:
- Asegurar el cumplimiento del cronograma, planes y acuerdos definidos durante el proyecto, los cuales se deben mantener dentro del alcance, tiempos, recursos, riesgos y calidad del proyecto.
- Apoyar técnicamente de forma transversal a todas las áreas que impactan la ejecución del proyecto
- Apoyar el diseño técnico y la gestión estratégica del proceso de implementación, así como las actividades de configuración, pruebas y monitoreo.
- Documentar detalladamente las actividades realizadas durante la ejecución del proyecto.
- Asegurar la comunicación efectiva entre los miembros del equipo de trabajo, con el supervisor del contrato y los profesionales de la mesa de servicios de TI de la Gobernación de Antioquia.

Consideraciones:

a) La experiencia del Ingeniero y los operarios, se deberá soportar mediante certificaciones expedidas por las entidades o empresas a las cuales se les prestó el servicio o para la cual se ejecutaron los trabajos, las cuales deberán cumplir con los siguientes requisitos:

1. Las certificaciones deberán ser expedidas por la empresa o la persona contratante del servicio.
2. Nombre o razón social del contratante.
3. Nombre o razón social del contratista.
4. Objeto y/o alcance
5. Número o identificación del contrato.
6. Fecha de iniciación del contrato (Día, Mes, Año)
7. Fecha de terminación del contrato. (Día, Mes, Año).
8. Funciones.
9. Nombre y firma de quien expide la certificación.