ANEXO TÉCNICO
CONTRATO CA-05-2015

1. OBJETO

Garantizar la disponibilidad, seguridad, desempeño y escalabilidad de los servicios de TI, que sirven de apoyo a la misión y objetivos del Fondo, con la contratación de servicios de infraestructura tecnológica como servicios (IaaS – Infraestructura como servicio) ofrecido por demanda, con la posibilidad de contar con ambientes altamente escalables, capaces de responder de manera más eficiente a las cambiantes necesidades del negocio de **FOGACOOP**.

2. ALCANCE DEL PRESENTE ANEXO

Los servicios de TI establecidos en este documento, conforman los aspectos técnicos, funcionales, administración, soporte y mantenimiento requeridos para la debida prestación de los servicios a proveer por parte del **CONTRATISTA** durante la ejecución del contrato.

3. JUSTIFICACION

FOGACOOP requiere la prestación del servicio de arrendamiento de infraestructura tecnológica, comunicaciones y seguridad que facilite y haga posible la gestión de la información que genera y/o almacena en desarrollo de sus funciones legales.

FOGACOOP requiere la prestación de servicios de:

a) Seguridad Perimetral entre la red pública de Internet y la red del Fondo, manteniendo esquemas de niveles de seguridad adecuados, denegando conexiones y accesos no autorizados.

b) Red inalámbrica integrada a la red corporativa del Fondo garantizando el acceso y movilidad tanto en algunos dispositivos móviles portátiles, como en las distintas áreas para comodidad de los usuarios locales, invitados, contratistas o personal de paso y así evitar los engorrosos cables para conectarse a la red y a Internet. Además garantizar que existan entornos dinámicos de trabajo en donde la conexión deje de ser un problema, en donde siempre se

tiene señal para distintos tipos de tareas que pueden considerarse como necesarias o prioritarias.

c) Servicios de monitoreo de Infraestructura de TI, con una labor continua y permanente de supervisión del estado, disponibilidad y el desempeño de todos los elementos que conforman la infraestructura de red del Fondo desde cualquier lugar, momento y dispositivo. Además de las situaciones críticas como son las interrupciones de servicios, amenazas internas y externas (intrusiones), ataques a dispositivos, tráficos anómalos o comportamientos dentro de la red que requieren de la intervención del encargado para evitar colapsos o saturaciones que puedan poner en riesgo la continuidad de la operación de la infraestructura de TI del Fondo.

d) Servicios de Antivirus EndPoint para la detección de virus informáticos en los microcomputadores y servidores que posee el Fondo, permitiendo contrarrestar cualquier ataque de virus de fuentes externas, al igual que controlar el correo no deseado, evitando de esta manera el contagio y cualquier acción que pueda comprometer la seguridad de la información y la red del Fondo.

e) Servicios de Backup y restauración de información que nos garantice la ejecución automática y que su entorno este protegido contra cualquier fallo de hardware. Importante mencionar que las copias de seguridad es un respaldo de información que nos permite mantener segura la información que consideramos importante y que no estamos dispuestos a perder si nuestros servidores presentan un fallo de hardware.

f) Servicios de Mantenimiento de Cableado Eléctrico y Estructurado, minimizando los riesgos de pérdida de comunicación en (datos, voz, video y control) de nuestros usuarios internos con el **DATACENTER** y el mundo exterior, además del aprovisionamiento y readecuación de cableado eléctrico y estructurado, con un sistema de cableado correctamente diseñado e instalado, que provea al usuario final una infraestructura de cableado con un desempeño predecible así como flexibilidad para acomodar crecimiento y cambio sobre un periodo extendido en el tiempo.

Dicha plataforma no funciona correctamente sin la debida administración, operación, soporte y monitoreo, de conformidad con los requerimientos técnicos establecidos en este contrato, por lo que se hace necesaria igualmente su contratación.

De conformidad con las situaciones planteadas, se requiere el suministro de hardware y software necesario para el diseño, implementación, administración, puesta en marcha, monitoreo, soporte y mantenimiento que permitan mantener en funcionamiento los servicios que garanticen su operación y disponibilidad de manera permanente (7x24x365).

4. ESPECIFICACIONES TÉCNICAS

OBJETIVO

Incluir las condiciones requeridas para los servicios de seguridad perimetral, redes wiffi integrada con la red corporativa, monitoreo de los elementos de red, antivirus y procesos de backup todo lo anterior, como servicio (infraestructura como servicio), y el suministro de mantenimiento preventivo y correctivo de cableado eléctrico y estructurado del fondo, para la operación de **FOGACOOP**.

El contrato incluye el suministro de hardware, software y licenciamiento necesario para el diseño, implementación, administración, puesta en marcha, monitoreo, soporte y mantenimiento que permitan mantener en funcionamiento los servicios provistos garantizando su operación y disponibilidad de manera permanente

Para el cumplimiento del objetivo de la contratación, la propuesta, aclaraciones, acuerdos, actas y demás documentos escritos que soporten el entendimiento entre las partes de este proceso (**FOGACOOP** y **CONTRATISTA**) serán parte integral de este anexo técnico para todos sus efectos, siempre y cuando ello no represente un cambio en el alcance del contrato y en los costos del mismo. A continuación se describen los aspectos técnicos en relación con:

a) Características transversales del servicio a proveer.
b) Especificaciones técnicas de las soluciones provistas.
c) Descripción de las soluciones propuestas.
d) Niveles de servicio mínimos.
e) Test de penetración e identificación de vulnerabilidades.

5. CARACTERISTICAS TRANSVERSALES DEL SERVICIO A PROVEER

El servicio a proveer debe tener las siguientes características, transversales para todos sus componentes:

a) Disponibilidad: El **CONTRATISTA** debe establecer las características y manejo de contingencias con características de alta disponibilidad que impidan la existencia de puntos de falla ó indisponibilidades del servicio provisto por **CONTRATISTA**, relacionado con el suministro del servicio de seguridad perimetral, redes wiffi integrada con la red corporativa, monitoreo de los elementos de red, antivirus y procesos de backup.

b) Escalabilidad: El **CONTRATISTA** debe permitir y responder de manera rápida y oportuna a las demandas de crecimiento ó decrecimiento, para los servicios que se alojarán en la infraestructura provista y que hace parte de la contratación.

c) Gestión de Configuración: El **CONTRATISTA** debe realizar la parametrización de los elementos que conforman las soluciones propuestas según el esquema de operación de **FOGACOOP** y mejores prácticas de casa matriz.

d) Gestión de Cambios y Liberaciones: El **CONTRATISTA** debe realizar cambios a los elementos que conforman las soluciones propuestas, según solicitudes de **FOGACOOP** y de la operación del **CONTRATISTA**, dichas solicitudes deben ser acordadas mediante un tiket y en común acuerdo entre las dos partes.

e) Gestión de la Disponibilidad: El **CONTRATISTA** deberá mantener operando las soluciones propuestas dentro de los niveles de servicio acordados por **FOGACOOP**, gestionando de forma adecuada los mantenimientos preventivos y correctivos anticipando alguna eventualidad que ponga en riesgo la operación de **FOGACOOP**.

f) Gestión de Capacidad: El **CONTRATISTA** deberá realizar gestión y seguimiento acerca de comportamientos de la infraestructura de redes, comunicaciones y soluciones propuestas y contratadas por **FOGACOOP**.

g) Gestión de Continuidad: El **CONTRATISTA** deberá impedir que por causas externas exista una degradación del servicio o afecte la

disponibilidad del mismo, El **CONTRATISTA** debe tomar medidas proactivas y reactivas ante alguna incidencia.

h) Gestión de Eventos: El **CONTRATISTA** deberá atender y solucionar todas aquellas acciones de monitoreo y alarmas que generen las soluciones propuestas sin que estos interfiera en la operación de **FOGACOOP**.

i) Gestión de Incidentes: El **CONTRATISTA** deberá dar alcance y solución a los incidentes que sean escalados y estén dentro del alcance de las soluciones propuestas.

j) Gestión de Problemas: El **CONTRATISTA** deberá dar manejo adecuado a los tikets que sean escalados, verificando las causas de los problemas, las soluciones a seguir y el monitoreo para prevenir que se tengan casos constantes con el mismo inconveniente.

k) Gestión de Mejoramiento Continuo: A partir del conocimiento de la operación de las soluciones propuestas y de acuerdo al análisis de los resultados, el **CONTRATISTA** recomendara al fondo el mejoramiento de los procesos que nos ayuden a mejorar el servicio en **FOGACOOP**.

l) Procedimientos de Gestión: El **CONTRATISTA** deberá realizar gestión, operación y administración total de la infraestructura (hardware y software) deberá ser desarrollada aplicando las mejores prácticas de ITIL v3, COBIT como marco de trabajo destinadas a facilitar la entrega de servicios de tecnologías de la información y comunicaciones (TIC) de alta calidad.

m) Gerencia de los Servicios, El **CONTRATISTA** deberá controlar que éstos se mantengan dentro de los rangos contratados por **FOGACOOP** e informando cuando éstos estén llegando al máximo ofertado por el **CONTRATISTA** y contratado por **FOGACOOP**.

6. ESPECIFICACIONES TÉCNICAS DE LAS SOLUCIONES PROVISTAS.

6.1 ESPECIFICACIONES TECNICAS DE LA SOLUCIÓN PERIMETRAL.

6.1.1 OBJETIVO Y ALCANCE:

El presente ITEM tiene por objeto definir las condiciones técnicas y específicas para los **SERVICIOS DE SEGURIDAD PERIMETRAL**, en clúster Activo / Activo, en alta disponibilidad, suministrando el hardware y software necesario para su diseño, implementación, administración, soporte y mantenimiento, asegurando siempre la protección de la red del Fondo, conforme a los requerimientos del Fondo, contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por el **CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.

6.1.2 ESPECIFICACIONES TÉCNICAS:

6.1.2.1. Se debe proveer una solución de Firewall perimetral, que permita un nivel de seguridad apropiada permitiendo al mismo tiempo el acceso a los servicios vitales del Fondo, seguridad con las mejores tasas de desempeño, capacidad de definir políticas de control de acceso, segmentar las redes en zonas de seguridad, aplicar controles en el tráfico que circula entre dichas zonas. Así mismo, se requiere que se complemente con herramientas que atiendan las buenas prácticas en seguridad de la información, mitiguen amenazas de ataques, explotación de virus, identificación, clasificación y detención de tráfico malicioso. De otra parte, las interfaces de la solución de seguridad perimetral, debe soportar el protocolo Giga Ethernet y garantizar el funcionamiento y la implementación de VPN´s de acuerdo a las necesidades del Fondo.

6.1.2.2. La solución debe contar con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluya filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, prevención contra amenazas de virus, spyware y malware, conformando una plataforma de seguridad integrada y robusta.

6.1.2.3. La solución debe contar con un sistema operativo pre-endurecido específico para seguridad que sea compatible con el appliance. Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre

sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows.

6.1.2.4. Debe ser una solución de alta disponibilidad.

6.1.2.5. En Cluster Activo/Activo.

6.1.2.6. Los firewall debe poseer un rendimiento de mínimo 11 Gbps.

6.1.2.7. Con rendimiento (multiprotocolo) de al menos 3.9 Gbps.

6.1.2.8. Debe manejar al menos 350 sesiones (peers) de VPN basadas en IPSec.

6.1.2.9. Debe manejar algoritmos de Encripción 3DES/AES con un desempeño mínimo de 500 Mbps.

6.1.2.10. Debe contar como mínimo con seis (6) interfaces 10/100/1000 (conector RJ45).

6.1.2.11. La solución deberá emplear firmas de protección a nivel aplicación para poder bloquear tráfico no deseado a los servidores del DATACENTER.

6.1.2.12. La solución deberá permitir realizar protección sobre ataques de Denegación Servicios.

6.1.2.13. Compatible con protocolos IPv4 e Ipv6.

6.1.2.14. Debe ser administrable vía SNMP y con en un solo ambiente de administración.

6.1.2.15. Debe permitir definir políticas por lo menos por usuario y por aplicación.

6.1.2.16. Debe permitir integrarle (ahora ó en un futuro) manejo de VLAN's

6.1.2.17. Debe ser integrable y compatible al 100% con equipos firewall (Fortinet 200B).

6.1.2.18. Instalable en RACK Standard.

6.1.2.19. Espacio ocupado en el RACK: 2U

6.1.2.20. El **CONTRATISTA** deberá efectuar al menos un (1) monitoreo, de la solución implementada, trimestralmente, dando las recomendaciones tendientes a mejorar su desempeño y prevenir inconvenientes en el servicio y haciendo entrega del informe sobre las labores efectuadas.

6.1.2.21. El **CONTRATISTA** deberá contar como mínimo con un ingeniero profesional entrenado y certificado por el fabricante en la solución ofrecida. Se debe adjuntar en la propuesta la certificación de los ingenieros, expedida por el fabricante.

6.2 ESPECIFICACIONES TECNICAS DE LA SOLUCIÓN RED INALÁMBRICA.

6.2.1 OBJETIVO Y ALCANCE:

El presente ITEM tiene por objeto definir las condiciones técnicas específicas del suministro del servicio de los **SERVICIOS DE RED INALÁMBRICA INTEGRADA CON LA RED CORPORATIVA**, para las dos (2) sedes con que cuenta la entidad, las cuales se encuentran conectadas mediante un backbone de Fibra óptica y Cableado UTP categoría 6A, cada sede cuenta con un sitio restringido en donde se alojan los equipos de comunicaciones que permiten la conectividad entre las dos (2) sedes.

FOGACOOP cuenta con las conexiones de cableado eléctrico y estructurado necesarios para colocar los elementos suministrados por **EL CONTRATISTA**. **EL CONTRATISTA** debe suministrar el hardware y software necesario para proveer el servicio e integrarlo a la red corporativa del Fondo, incluido el diseño, implementación, administración, soporte y el mantenimiento del servicio, asegurando siempre la protección de la red del Fondo, conforme a los requerimientos del Fondo, contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por **El CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.

6.2.2 ESPECIFIC|ACIONES TÉCNICAS:

6.2.2.1. Se debe realizar al menos el despliegue de dos (2) tipos de redes inalámbricas, diferenciadas según su propósito y características. Los dos (2) tipos considerados son:

a) Red inalámbrica de invitados o contratistas o personal de paso.

El **CONTRATISTA** debe ofrecer una red inalámbrica que les permita a los usuarios invitados, contratista o personal de paso a salir a Internet (o a los recursos internos que el Fondo considere necesarios). Esta red no debe usar cifrado y debe tener un acceso restringido mediante un usuario y una contraseña otorgada por el Fondo. La solución debe realizar las tareas de asignación dinámica de direcciones (DHCP), mientras que las labores de filtrado de paquetes y traducción de direcciones (NAT) las realizara la infraestructura de seguridad perimetral que posee el Fondo.

b) Red inalámbrica corporativa y de acceso a escritorios remotos.

El **CONTRATISTA** debe ofrecer una red inalámbrica con extensión a la red corporativa del Fondo. Esta red debe contar con cifrado y control de acceso, utilizando como elementos los servidores de controlador de dominio de la infraestructura informática del Fondo. En esta red serán los servidores internos los que otorguen direcciones a los equipos de los usuarios autenticados, mientras que las tareas de traducción de direcciones (NAT) y registro de los accesos las llevarán a cabo la infraestructura de seguridad perimetral que posee el Fondo. Importante mencionar que algunos dispositivos móviles van a tener acceso a máquinas virtuales que residen en un **DATACENTER** bajo el sistema de virtualización (VMWare).

6.2.2.2. La red wifi debe permitir el acceso inalámbrico de los usuarios, invitados, contratistas o personal de paso a aplicaciones y servicios con las máximas prestaciones de seguridad, disponibilidad y rendimiento.

6.2.2.3. La topología de la red propuesta debe contar con al menos una controladora central inalámbrico conectada a la red del Fondo, junto con una serie de puntos de acceso controlados por dicho controlador inalámbrico, que garantizara el servicio a las siguientes zonas del Fondo:

Sede A

a) Centro de Cómputo, costado Norte del Piso.
b) Secretaria General, costado Norte del Piso.
c) Dirección, costado Norte del Piso.
d) Planeación Estratégica, costado Sur del Piso.
e) Sala de Juntas, Costado Oriental del Piso.
f) Gerencia Técnica, Costado Occidental del Piso.

Sede B

a) Oficina de Servicios Corporativos, Costado Oriental del Piso 3.
b) Oficina de Gestión Documental, Ubicación Centro entre Costado Oriental y Occidental del Piso 2.
c) Sala de Capacitaciones, Costado Sur del Piso 1.

6.2.2.4. El diseño de la red se deberá orientar a los usuarios, dispositivos y servicios que el Fondo va a proveer. El objetivo principal es que la red esté al servicio de los usuarios y se adapte a sus necesidades.

6.2.2.5. Facilidad de Gestión: el sistema debe facilitar la gestión y administración de cuentas de usuarios, disponer de interfaces simples e intuitivos y con capacidad de integrar, crear y borrar masivamente las cuentas.

6.2.2.6. Alta Capacidad: se considera fundamental para el correcto funcionamiento de la red que la capacidad de la misma no tenga cuellos de botella y que el flujo de datos sea lo más rápido posible y flexible.

6.2.2.7. Escalabilidad: todos los elementos de la solución deberán permitir ampliar sus funcionalidades, mediante la adición de nuevos dispositivos o módulos a la solución ya existente.

6.2.2.8. Flexibilidad: Las plataformas ofertadas deberán estar preparadas para soportar nuevas tecnologías y servicios de cara al futuro. (comunicaciones unificadas, escritorios virtuales, telefonía IP, entre otros).

6.2.2.9. La solución debe ser abierta, de manera que facilite la incorporación de módulos adicionales de comunicaciones con otras aplicaciones y la integración con otros sistemas. Por tanto, deberá seguir estándares que permitan su interoperatividad con otros fabricantes y otras tecnologías.

6.2.2.10. La solución debe estar dimensionado para soportar entre 50 y 100 conexiones simultáneas.

6.2.2.11. Se deberá proporcionar cobertura en todas las oficinas de las sedes.

6.2.2.12. Se reforzará la cobertura en las Zonas de la sala de juntas y sala de capacitación ya que se tratará de los puntos de mayor concurrencia de usuarios.

6.2.2.13. El **CONTRATISTA** deberá efectuar al menos un (1) monitoreo, de la solución implementada, trimestralmente, dando las recomendaciones tendientes a mejorar su desempeño y prevenir inconvenientes en el servicio y haciendo entrega del informe sobre las labores efectuadas.

6.2.2.14. El **CONTRATISTA** deberá contar como mínimo con un ingeniero profesional, entrenado y certificado por el fabricante en la solución ofrecida. Se debe adjuntar en la propuesta una copia de la certificación de los ingenieros, expedida por el fabricante.

6.2.2.15. El **CONTRATISTA** deberá adjuntar un certificado de distribuidor directo autorizado de la marca de los equipos que conforman la solución ofrecida expedido por el fabricante o su subsidiaria en Colombia, con fecha de expedición no superior a seis (6) meses, contados a partir de la fecha de presentación de la oferta.

6.2.2.16. El **CONTRATISTA** deberá contar como mínimo con un ingeniero profesional, entrenado y certificado en directorio activo Windows Server 2012. Se debe adjuntar en la propuesta una copia de la certificación del ingeniero.

6.2.2.17. Las características mínimas que deberá cumplir la controladora inalámbrica serán las siguientes:

a) Número mínimo de puntos de acceso soportados seis (6). Tres (3) puntos para la sede A y tres (3) puntos para la sede B.
b) Capacidad de ampliación por licencia software hasta 100 usuarios.
c) Soporte de equipos 802.11a/b/g/n/ac.
d) Autoconfiguración automática y centralizada de los puntos de acceso.
e) Asignación automática de canales 802.11 para evitar interferencia.
f) Balanceo de carga.
g) Detección y corrección de huecos en la cobertura.
h) Control dinámico de potencia.
i) 802.11i (WPA2), WPA y WEP.
j) Protocolo 802.11x con soporte para EAP-TLS, EAP-TTLS, PEAP, EAP-FAST.
k) Detección de puntos de acceso no autorizados.
l) Capacidades de IDS/IPS.
m) Listas de control de acceso.
n) Integración en entorno RADIUS AAA.
o) Roaming mejorado.
p) Soporte para VLAN y calidad de servicio (QoS).
q) Soporte CAPWAP.

r) Validación de usuario y contraseña contra base de datos de usuarios locales, Active Directory, LDAP o Radius
s) Varios interfaces para Uplink Gigabit (10/100/1000 BASE T, 1000 BASE SX).
t) Interfaz de gestión web (https). Posibilidad de varios SSID.
u) Posibilidad de varias VLAN.
v) Los estándares que debe cumplir el controlador son los siguientes: IEEE 802.3, 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE T, 1000 BASE-SX, 1000 BASE-LH, IEEE 802.1Q Vtagging, IEEE 802.1A Link Aggregation, IEEE 802.11a, 802.11b, 802.11b, WMM/802.11e, 802.11h, 802.11n, DHCP, BOOTP, SNMP v1,v2,v3, Telnet, RMON, Syslog, http y CAPWAP.

6.2.2.18. Los puntos de acceso deberán cumplir con las siguientes especificaciones y estándares:

a) Duales (802.11a/n y 802.11g/n/ac) simultáneos.
b) Compatibilidad 802.11n Draft 2.0.
c) Tasa de datos de hasta 300 Mbit/s.
d) Software CAPWAP.
e) Antenas duales integradas.
f) Encriptación AES por hardware (sin pérdida de rendimiento).
g) Certificados WPA y WPA2 compatibles con 802.11i.
h) Diseño estético.
i) Soporte de alimentación por cable de red (PoE).
j) Interfaz 10/100/1000 BASE-T.

6.2.2.19. El software de gestión de usuarios deberá tener las siguientes características:

a) Soporte de múltiples servidores de autenticación externos, incluyendo la base de datos de usuarios locales, Active Directory, LDAP, RADIUS y Proxy.
b) Módulo de generación de informes y consultas: por usuario, globales en el sistema, globales en un período de tiempo, etc.
c) Funcionamiento como servidor de autenticación 802.1X: soporte PEAP, TLS, TTLS.
d) Integración con plataformas existentes de gestión mediante API abierta.
e) El software deberá permitir su instalación en una máquina física o virtual.

6.3 ESPECIFICACIONES TECNICAS DE LA SOLUCIÓN DE GESTIÓN Y MONITOREO.

6.3.1 OBJETIVO Y ALCANCE:

El presente ITEM tiene por objeto definir las condiciones técnicas específicas del suministro del servicio de los **SERVICIOS DE MONITOREO DE INFRAESTRUCTURA DE TI**, de los elementos que conforman la plataforma tecnológica de red y de comunicaciones, incluida su instalación, configuración, administración y monitoreo de la misma, el **CONTRATISTA** debe suministrar el hardware y software necesario para proveer el servicio, incluido el diseño, implementación, administración, soporte y el mantenimiento del servicio. El **CONTRATISTA** deberá efectuar al menos un (1) monitoreo mensual de la solución implementada, dando las recomendaciones tendientes a mejorar su desempeño y prevenir inconvenientes en el servicio y haciendo entrega del informe sobre las labores efectuadas, garantizando siempre la independencia de la función asignada y el mejoramiento y prevención de malos hábitos que aporten a posibles soluciones y situaciones de anomalía en dos niveles (Estratégico y Técnico), conforme a los requerimientos del Fondo, contenidos en la propuesta, al igual que los ofrecimientos efectuados por el **CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.

6.3.2 ESPECIFICACIONES TÉCNICAS:

6.3.2.1. El **CONTRATISTA** debe ofrecer una solución de gestión y monitoreo de elementos que conforman la plataforma tecnológica de red y de comunicaciones del Fondo, con el fin de evitar que estos lleguen a funcionar incorrectamente sin que se degrade el rol y las funciones asignadas, mediante un monitoreo efectivo y continuo se debe realizar la recolección y el análisis de datos con el fin de anticipar problemas en la red.

6.3.2.2. La solución debe involucrar todas las herramientas e infraestructura de monitoreo.

6.3.2.3. La gestión sobre la infraestructura, debe ofrecer al Fondo la posibilidad de análisis de rendimiento de ancho de banda, canales de comunicaciones, servicios de red, protocolos utilizados por los usuarios, consumo de aplicaciones, entre otros y toma de acciones preventivas y/o correctivas.

6.3.2.4. El **CONTRATISTA** debe realizar la gestión y optimización del ancho de banda, canales de comunicaciones, servicios de red y todo tipo de tráfico que circula entre el Fondo y el **DATACENTER** y especialmente la conexión a Internet, el cual termina siendo importante controlar su uso, para administrarlo adecuadamente según las necesidades del Fondo.

6.3.2.5. El **CONTRATISTA** debe realizar el monitoreo del tiempo de respuesta de las aplicaciones de principio a fin para posteriormente, analizar el rendimiento de la aplicación en toda la infraestructura de la red.

6.3.2.6. Las herramientas de monitoreo deben ser propiedad del **CONTRATISTA**.

6.3.2.7. El **CONTRATISTA** debe monitorear el desempeño de toda la infraestructura de tecnología de red y comunicaciones (servidores, switches, routers puntos de acceso (AP) y periféricos, etc.), que se encuentran en las instalaciones del fondo.

6.3.2.8. El **CONTRATISTA** debe entregar un informe mensual (general) de gestión y monitoreo (incluidos los soportes).

6.3.2.9. El **CONTRATISTA** debe entregar un informe trimestral (detallado) de gestión y monitoreo (incluidos los soportes).

6.4 ESPECIFICACIONES TECNICAS DE LA SOLUCIÓN DE ANTIVIRUS ENDPOINT.

6.4.1 OBJETIVO Y ALCANCE:

El presente ITEM tiene por objeto definir las condiciones técnicas específicas del suministro del servicio de los **SERVICIOS DE ANTIVIRUS ENDPOINT** para los servidores y microcomputadores del Fondo, la cual se encuentra compuesta por (72 licencias para los equipos del Fondo), el **CONTRATISTA** debe suministrar el hardware y software necesario para proveer el servicio, se debe suministrar el servicio de diseño, implementación, administración, incluido el licenciamiento, las actualizaciones y el soporte del producto instalado, conforme a los requerimientos del Fondo, contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por el **CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.

6.4.2 ESPECIFICACIONES TÉCNICAS:

6.4.2.1. El **CONTRATISTA** debe ofrecer una solución de Antivirus EndPoint, que permita protección de software malicioso con motor de antivirus de alto desempeño para escanear los archivos a medida que pasan a través de los equipos o dispositivos (servidores, routers, switches puntos de acceso (AP) y todos los componentes que provee la solución), permitiendo inspeccionar los archivos de cualquier tamaño y formato, manteniendo altos niveles de desempeño, ofreciendo flexibilidad y permitiendo balancear entre los requerimientos de desempeño y seguridad del entorno.

6.4.2.2. La solución propuesta debe brindar seguridad a la infraestructura y servicios informáticos comunes de todos los usuarios, contratistas y los equipos informáticos, que forman parte de la red del Fondo.

6.4.2.3. El **CONTRATISTA** deberá realizar el diseño e implementación de reglas de filtrado antivirus para la red, web, control de navegación e integración con el Microsoft Active Directory, el cual deberá garantizar disponibilidad del servicio.

6.4.2.4. El **CONTRATISTA** deberá realizar el diseño e implementación de reglas de filtrado antivirus para la red, web, control de navegación e integración con el Microsoft Active Directory, el cual deberá garantizar disponibilidad del servicio.

6.4.2.5. El motor de exploración deberá utilizar distintas tecnologías de detección antivirus: exploración de firmas y exploración heurística. La exploración de firmas busca un conjunto de código hexadecimal característico de cada virus y la exploración heurística busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos. Además, deberá tener integrada una tecnología de Servicio de Mapeo, que permita acceder por debajo del sistema operativo para un análisis y una reparación completo.

6.4.2.6. La solución propuesta debe brindar acciones posteriores a la detección, con capacidad para tomar distintas acciones cuando sea detectado un virus o un ataque, limpiar el archivo infectado.

6.4.2.7. La solución propuesta debe brindar exclusiones en la exploración con capacidad para excluir de la exploración archivos, carpetas, procesos, etc. o moverlos a cuarentena, no tomar acción, eliminar el archivo, etc.

6.4.2.8. La solución propuesta debe brindar capacidad para exploración de mensajes de correo electrónico utilizando Microsoft Outlook, detección de virus y programas no deseados.

6.4.2.9. La solución propuesta debe ser capaz de detectar y eliminar diferentes tipos, tales como: adware, spyware, jokeprograms, Keyloggers, trackware, hacktools, remoteaccesstools, dialers, etc.

6.4.2.10. La solución propuesta debe ser capaz de instalarse en clientes de forma remota desde una consola de administración centralizada, de forma transparente para el equipo cliente y con la capacidad de retrasar/suprimir la necesidad del reinicio de este equipo cliente, dependiendo de la tecnología a implementar.

6.4.2.11. La solución propuesta debe tener la capacidad de programar tareas de exploración, actualización, etc.

6.4.2.12. La solución propuesta debe tener la capacidad para retrasar/dejar en modo espera las búsquedas de virus en caso de que el equipo portátil se encuentre sin alimentación eléctrica directa.

6.4.2.13. La solución propuesta debe crear bitácoras por cada uno de los eventos tales como: historial de riesgos, historial de exploraciones, historial de eventos e historial de ataques al antivirus, disponible tanto en el cliente como en la consola de administración.

6.4.2.14. La solución propuesta debe escanear y bloquear en tiempo real cualquier acceso e instalación de cualquier spyware, adware, malware, key logger, herramientas de administración remota, Dialer, trackware, hack tools, etc.; no solamente por escaneo en demanda.

6.4.2.15. La solución propuesta debe escanear llaves del registro y eliminar las llaves creadas por los spyware sin afectar la estructura del registro a nivel de sistema operativo.

6.4.2.16. La solución propuesta debe poder instalarse en los siguientes sistemas operativos: Windows XP SP1+ 32-bit/64-bit SP2, Windows 7 32-bit/64-bit, Windows 8, Windows Server 2003 32-bit/64-bit y Windows Server 2008 32-bit/64-bit.

6.4.2.17. La solución propuesta debe presentar un icono en el área de notificación de la barra de tareas, con posibilidad de ser ocultado por el administrador.

6.4.2.18. La solución propuesta debe integrar de forma transparente las tecnologías principales de antivirus, antispyware, firewall, prevención de intrusos, control de dispositivos y control de acceso a los recursos de Hardware del equipo.

6.4.2.19. La solución propuesta debe ofrecer una única interfaz integrada para administrar todas las tecnologías, con posibilidades de administración local o por la consola.

6.4.2.20. La solución propuesta debe contar con protección basada en comportamiento, que protege contra las amenazas de día cero y amenazas nunca antes vistas.

6.4.2.21. La solución propuesta debe mostrar puntuaciones en base a comportamientos buenos y malos de las aplicaciones desconocidas, para determinar una detección más precisa del software malicioso.

6.4.2.22. La solución propuesta debe ser capaz de detectar virus conocidos y desconocidos a través de comportamiento o patrones similares a los de un virus en todos los archivos (HEURISTICA).

6.4.2.23. La solución propuesta debe brindar análisis de aplicaciones, control de acceso a los archivos ejecutables, y evitar la ejecución de las mismas.

6.4.2.24. La solución propuesta debe permitir a los administradores restringir ciertas actividades consideradas sospechosas o de alto riesgo. Así mismo, el administrador debe ser capaz, por política interna del Fondo, de controlar la ejecución de aplicaciones mediante el código hash de las mismas.

6.4.2.25. La solución propuesta debe permitir al administrador controlar por usuario qué periféricos pueden conectarse a un equipo y cómo se usan.

6.4.2.26. La solución propuesta debe tener la capacidad de bloquear los equipos o servidores para impedir que se conecten las unidades thumbdrive, grabadoras de CD, impresoras y otros dispositivos USB, incluyendo teléfonos celulares y dispositivos bluetooth.

6.4.2.27. La solución propuesta debe igualmente contar con la capacidad no solo de bloquear en su totalidad un dispositivo, sino de restringir parcialmente actividades en los periféricos, tales como memorias USB; haciendo que sean de solo lectura, o que no permita la ejecución de aplicaciones desde dichos periféricos. Adicionalmente el administrador puede definir si restringe el acceso a

todos los dispositivos USB o sólo restringe el acceso de acuerdo al identificador del dispositivo.

6.4.2.28. La solución propuesta debe tener la capacidad de generar y programar reportes de amenazas encontradas en la red o en los equipos.

6.4.2.29. La solución propuesta debe tener la capacidad de crear reportes personalizados de los sucesos más sobresalientes de riesgos de seguridad del Fondo.

6.4.2.30. La solución propuesta debe tener la capacidad de monitorear la distribución de un ataque, riesgo de seguridad e infección, así como verificar el nivel de actividad de esta en la red.

6.4.2.31. La solución propuesta debe administrar desde la consola central los dispositivos y las aplicaciones.

6.4.2.32. Es requisito que la solución de antivirus se encuentre en la Gartner para Endpoint-Protection-Platforms.

6.4.2.33. El **CONTRATISTA** deberá realizar la transferencia de conocimientos de la solución Implementada con una duración de al menos dos (2) horas.

6.4.2.34. El **CONTRATISTA** deberá efectuar al menos un (1) monitoreo, de la solución implementada, trimestralmente, dando las recomendaciones tendientes a mejorar su desempeño y prevenir inconvenientes en el servicio y haciendo entrega del informe sobre las labores efectuadas.

6.4.2.35. El **CONTRATISTA** deberá contar como mínimo con un ingeniero profesional, entrenado y certificado por el fabricante en la solución ofrecida. Se debe adjuntar en la propuesta una copia de la certificación de los ingenieros, expedida por el fabricante.

6.4.2.36. El **CONTRATISTA** ofrecerá el soporte técnico especializado para realizar las siguientes actividades:

a) Transferir el conocimiento al personal del Fondo para actualizar versiones y problemas de infección.
b) El conocimiento que se dé al personal del Fondo, deberá contemplar la actualización de versiones, aplicación de parches, y puesta a punto en la configuración para aplicaciones, sistemas operativos y bases de datos que cubran las vulnerabilidades tecnológicas conocidas al momento.

c) Capacitación que asegure las mejores prácticas en la utilización del software licenciado.
d) Una vez iniciado el servicio si se presenta una solicitud urgente de atención el tiempo de respuesta no deberá exceder de 4 horas. La solicitud podrá realizarse vía correo electrónico y/o vía escrita. El tiempo máximo de 4 horas de darse por enterado el proveedor, se contabilizará a partir de la notificación, ya se escrita o por correo electrónico.

6.5 ESPECIFICACIONES TECNICAS DE LA SOLUCIÓN DE BACKUP Y RESTAURACIÓN DE INFORMACIÓN.

6.5.1 OBJETIVO Y ALCANCE:

El presente ITEM tiene por objeto definir las condiciones técnicas específicas del suministro del servicio de los **SERVICIOS DE PROCESOS DE BACKUP Y RESTAURACIÓN DE INFORMACIÓN**, suministrando el hardware y software necesario para su diseño, implementación, administración, puesta en marcha, soporte y mantenimiento, incluido la ejecución de los procedimientos de copias de seguridad y de recuperación de la misma, garantizando que se ejecuten correctamente y que el entorno esté protegido contra la pérdida de datos o los intervalos de continuidad, conforme a los requerimientos del Fondo, contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por el **CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.

6.5.2 ESPECIFICACIONES TÉCNICAS:

6.5.2.1. El **CONTRATISTA** debe ofrecer una solución de backup y restauración de información, garantizando que se ejecuten correctamente y que el Fondo se encuentre protegido contra la pérdida de datos o intervalos de interrupciones en la continuidad del servicio.

6.5.2.2. La solución propuesta debe ser instalada y configurada en las instalaciones del Fondo.

6.5.2.3. El **CONTRATISTA** debe suministrar el hardware y software que permita hacer respaldo y recuperación de información del Fondo.

6.5.2.4. La solución propuesta debe permitir la restauración de la información, una vez validado el correcto funcionamiento del medio y la integridad física del mismo, se debe entregar en cintas o en medio magnético CD – ROM, DVD o cualquier otro formato que defina el Fondo, para ser enviadas a custodia externa.

6.5.2.5. La solución propuesta debe ser interoperable con la infraestructura de tecnológica que posee el Fondo, servidores físicos con sistemas operativos, Solaris 10, Windows Server 2003 32-bit/64-bit y Windows Server 2008 32-bit/64-bit.

6.5.2.6. La solución propuesta debe ser compatible con productos de respaldo estándar en el mercado.

6.5.2.7. La solución propuesta debe estar en capacidad de realizar compresión por software para aumentar la capacidad total almacenada.

6.5.2.8. La solución propuesta debe permitir el backup de archivos abiertos.

6.5.2.9. La solución propuesta debe poseer un software de gestión vía GUI o WEB para su administración.

6.5.2.10. La solución propuesta debe estar en capacidad de trabajar y estar soportada por fabricantes de productos de software de respaldo, reconocida y de trayectoria en el mercado.

6.5.2.11. La solución propuesta debe incluir el software de backup (consola central de administración para Windows y agentes de backup).

6.5.2.12. La solución propuesta debe ser compatible con un (1) servidor de Dell, Modelo PowerEdge R620, con sistema operativo Windows 2012 Server Standard Procesador Intel® Xeon® 6C E5-2640, 2.50GHz, Memoria RAM RDIMM de 16 gigabytes (GB), Capacidad total de almacenamiento de 1.2 Teras Bytes (TB) (Con el rol de servidor de Aplicaciones y Archivos).

6.5.2.13. La solución propuesta debe tener como mínimo una unidad de tape (Lto3), con capacidad de las cintas de al menos 400 GB no comprimida.

6.5.2.14. El **CONTRATISTA** debe proveer 24 cintas para unidad de tape (Lto3).

6.5.2.15. El **CONTRATISTA** deberá ejecutar todas las labores de instalación, configuración, estabilización y demás elementos que sean necesarios para cumplir

con los requerimientos técnicos y funcionales especificados, de tal forma que se conforme una solución completa, integrada y enteramente operacional.

6.5.2.16. El **CONTRATISTA** deberá como actividad de inicio, hacer el levantamiento de información con las gerencias y entregar al Fondo un documento con el detalle de la información a respaldar y custodiar, que servirá a la entidad de soporte para establecer y determinar cuáles medios magnéticos serán migrados, de acuerdo a las políticas actuales de retención.

6.5.2.17. El **CONTRATISTA** deberá ejecutar procesos de restauración de la información en cualquier momento debido a daños o pérdida de la misma, la cual se debe realizar de acuerdo con los procedimientos definidos en cualquier día y momento.

6.5.2.18. El **CONTRATISTA** debe presentar una planilla de programación de backups a un año, la cual será revisada y aprobada.

6.5.2.19. El **CONTRATISTA** deberá revisar periódicamente la integridad y consistencia de la información respaldada de los Backups realizados, diligenciando una planilla de programación de pruebas de restauración, la cual será revisada y aprobada por el Fondo.

6.5.2.20. El **CONTRATISTA** deberá tener total confidencialidad en la información suministrada y firmar un acuerdo de confidencialidad donde se comprometa al manejo confidencial de la información, contenida en los medios magnéticos de propiedad de la entidad.

6.5.2.21. El **CONTRATISTA** deberá garantizar la entrega y recibo de medios magnéticos a custodia externa, mediante contenedores o tulas especiales con precinto de seguridad.

6.5.2.22. El operador encargado de la administración de los backups, ejecutará las siguientes actividades:

a) Monitorear la infraestructura utilizada en la función operativa de backups.
b) Verificar diariamente la consola de administración de la herramienta de backups.
c) Llevar registro diario en bitácora de los backups ejecutados.
d) Realizar cambios en la política, instalaciones, configuración y/o creación de nuevos agentes, actualización, con el apoyo del proveedor cuando sea requerido.

e) Tramitar soporte ante el proveedor en caso de fallas de acuerdo con el alcance del contrato de soporte del fabricante.
f) Control y seguimiento de la ejecución de los respaldos.
g) Realizar las actividades de restauración de las cintas de acuerdo con lo previsto en este documento.

Actividades Administrativas.

a) Informar oportunamente al Fondo, la necesidad de proveer cintas regulares cada vez que sea necesario.
b) Verificar que las cintas se encuentren correctamente etiquetadas (es decir, se debe verificar que la cinta tenga su label correspondiente, marca legible por el lector óptico).
c) Preparar envío de cintas para entregar en custodia externa al proveedor.
d) Informar oportunamente al autorizado ante el proveedor de custodia externa del Fondo, la necesidad de nuevos de transportes.
e) Supervisar las actividades del operador encargado del manejo de las cintas.
f) Resguardar las cintas en el gabinete asignado, mientras son llevadas para custodia externa
g) Mantener un inventario de las cintas recibidas (nuevas) y las que estén en operación (Gabinete y custodia externa).
h) Proveer los materiales, herramientas, hardware y software requeridos para los backups.

6.5.2.23. En el momento de efectuar restauraciones por demanda o periódicas, el operador encargado de la administración de los backups generará el informe respectivo, el cual deberá contener la siguiente información como mínimo:

a) Fecha de ejecución.
b) Información restaurada.
c) Origen y Destino de la información restaurada.
d) Verificación de la restauración.
e) Validar si la restauración fue exitosa.
f) Validar si el tamaño y cantidad de archivos reportados en el backups corresponde a lo restaurado.
g) Nombre de las carpetas o archivos restaurados.
h) Ubicación de la restauración.
i) Descripción de Problemas (si aplica).
j) Descripción Plan de Acción a ejecutar por fallas en la restauración (si aplica).

6.5.2.24. Todos los servicios inherentes a la toma de los Backups, tal y como se

define en este Anexo, deben realizarse de la manera estipulada en tiempos y frecuencia, mensualmente se deben entregar al Fondo, las siguientes mediciones:

a) Eventos ó incidencias presentadas en la infraestructura física y lógica de la solución de backups.
b) Inconsistencias detectadas en los medios utilizados (daños en cintas, sobredimensionamientos, etc.).
c) Cantidad de cintas utilizadas en el período.
d) Cantidad de cintas enviadas a custodia externa.
e) Inventario de cintas nuevas, en operación y custodia externa.
f) Informe que contenga la identificación de cada cinta, el contenido de la información respaldada, la fecha, el(los) servidor(es) al(os) que pertenece.

6.5.2.25. Los informes mensuales presentados al Fondo, consolidan los indicadores de gestión, identificando el estado de la calidad y el progreso de las actividades correspondientes asociadas al servicio, así como las incidencias y problemas presentados durante el período. Los informes de gestión de backups, contendrán la siguiente información:

a) Movimiento mensual de cintas, monitoreo y gestión de infraestructura y comportamiento mensual de backups.
b) Consolidación de incidencias registradas en la herramienta de gestión.
c) Mediciones de indicadores de desempeño.
d) Inventario de cintas.
e) Informe que contenga la identificación de cada cinta, el contenido de la información respaldada, la fecha, el(los) servidor(es) al(os) que pertenece.

6.6 ESPECIFICACIONES TECNICAS PARA EL SUMINISTRO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE CABLEADO ELÉCTRICO Y ESTRUCTURADO DEL FONDO.

6.6.1 OBJETIVO Y ALCANCE:

El presente ITEM tiene por objeto definir las condiciones técnicas específicas **SUMINISTRO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE CABLEADO ELÉCTRICO Y ESTRUCTURADO DEL FONDO.** Suministrando los servicios de mantenimiento preventivo y correctivo de cableado eléctrico y estructurado del Fondo, con el fin de poder prevenir y resolver los problemas relacionados con cableado eléctricos y estructurados y las redes de comunicaciones de voz y datos de forma más rápida y eficiente posible. Dicho

mantenimiento se realizará, o bien acorde a las solicitudes de ampliación y/o reparación por parte del Fondo, o bien a las deficiencias que se presenten a la hora de realizar las inspecciones del mantenimiento preventivo, conforme a los requerimientos del Fondo, contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por el CONTRATISTA, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.

6.6.2 ESPECIFICACIONES TÉCNICAS:

6.6.2.1. Para el mantenimiento, instalación, readecuación y documentación de nuevos puntos de la infraestructura de cableado estructurado estará conformado por elementos que cumplan con el estándar TIA/EIA, y demás normas, cumpliendo con los procedimientos de instalación, marcación, certificación y conexión a tierra, y demás que sean necesarios para el correcto funcionamiento.

6.6.2.2. Los elementos de la infraestructura de cableado estructurado ofrecidos por el **CONTRATISTA** deberán ajustarse a lo estipulado en las normas y estándares, y las características de fabricación, instalación y pruebas se ajustarán a la última versión de la siguiente norma (ANSI/EIA/TIA-568B.2-10 - Documento principal que regula todo sistema de cableado estructurado para edificios comerciales. TIA/EIA TSB-67 - Especificación del desempeño de transmisión en el campo de prueba del sistema de cableado UTP. TIA/EIA TSB-72 - Guía para el cableado de fibra óptica. ANSI/EIA/TIA-568B.2-10; Category 6A.

6.6.2.3. Para readecuaciones o nuevos puestos de trabajo, el servicio estará compuesto por canaleta, los patchcords, conectores tipo RJ 45, adaptadores, tomas, jacks y la respectiva certificación que permitan la conexión de los puestos de trabajo (equipos finales) a los gabinetes de comunicaciones y tableros control eléctrico, indiferente si estas son de datos y/o de voz y/o eléctrico.

6.6.2.4. Para cableado horizontal (cable UTP, jacks, faceplate) que conecta cada salida de información al respectivo centro de cableado.

6.6.2.5. Para cableado vertical, se compone de cables de fibra óptica, UTP y cable multipar telefónico que unen los centros de cableado del Fondo, tanto para la parte de datos como de voz, con los centro de cableado principal de cada sede.

6.6.2.6. Para administración, tanto para voz como datos comprende todos los elementos de conectividad que permiten administrar el sistema, es decir, los equipos y elementos pasivos (patch panel, patch cord, Fibra, face place y tomas eléctricas) que se encuentra ubicados en los gabinetes de comunicaciones y en cuanto a eléctrico todo lo concerniente a parte eléctrica, para la conexión de equipos activos a la red.

6.6.2.7. El centro de procesamiento (comunicaciones), es el sitio donde se ubican los equipos centrales para los sistemas de información, datos y los sistemas telefónicos.

6.6.2.8. Eléctrico, hace referencia a todo lo concerniente a parte eléctrica regulada, para la conexión de equipos activos a la red.

6.6.2.9. Los patch cord de fibra y de UTP suministrados por el **CONTRATISTA** deben ser de fábrica.

6.6.2.10. El **CONTRATISTA** debe cumplir el tiempo de solución de los requerimientos o reparaciones del bien, de acuerdo a lo siguiente:

a) Para mantenimiento de un punto triple (voz, datos y eléctrico) categoría 6 o superior, el tiempo máximo para ser atendido y solucionado no debe superar las 8 horas hábiles.
b) Para instalación de un punto triple con canaleta (voz, datos y eléctrico) categoría 6 o superior, el tiempo máximo para ser atendido y solucionado no debe superar las 36 horas hábiles.
c) Para mantenimiento de un punto doble (voz y datos), el tiempo máximo para ser atendido y solucionado no debe superar las 4 horas hábiles.
d) Para mantenimiento de un punto eléctrico, el tiempo máximo para ser atendido y solucionado no debe superar las 4 horas hábiles.
e) Para instalación de un punto eléctrico con canaleta, el tiempo máximo para ser atendido y solucionado no debe superar las 24 horas hábiles.
f) Para instalación de un punto sencillo con canaleta (voz o datos) categoría 6 o superior, el tiempo máximo para ser atendido y solucionado no debe superar las 24 horas hábiles.
g) Para instalación de un punto doble con canaleta (voz o datos) categoría 6 o superior, el tiempo máximo para ser atendido y solucionado no debe superar las 32 horas hábiles.
h) Para mantenimiento y organización de gabinete, el tiempo máximo para ser atendido y solucionado no debe superar las 8 horas hábiles.

i) Para conectorización y certificación por hilo de fibra óptica monomodo y/o multimodo, el tiempo máximo para ser atendido y solucionado no debe superar las 16 horas hábiles.
j) Para certificación de cableado, el tiempo máximo para ser atendido y solucionado no debe superar las 8 horas hábiles.

6.6.2.11. El **CONTRATISTA** prestará los trabajos o servicios dentro de los tiempos y horarios que se le señalen.

6.6.2.12. El **CONTRATISTA** debe realizar actividades de mantenimiento correctivo a las instalaciones de cableado eléctrico y estructurado, en al menos a:

a) Reparación de averías.
b) Sustitución de elementos deteriorados.
c) Etiquetado e identificación de las instalaciones.
d) Actualización de la documentación.
e) Elaboración de presupuestos a petición del Fondo.

6.6.2.13. Todos los trabajos realizados deberán quedar documentados mediante parte de trabajo emitido por el personal del **CONTRATISTA**, independientemente del informe de certificación del cableado cuando este proceda. Los trabajos contendrán, como mínimo, los datos siguientes:

a) Fecha de ejecución.
b) Naturaleza de los trabajos.
c) Tiempo empleado en los mismos.
d) Personal que los ha ejecutado.
e) Valoración.

6.6.2.14. El **CONTRATISTA** debe suministrar el personal requerido de manera obligatoria para prestar el servicio, con una experiencia mínima de tres (3) años certificada en proyectos de diseño, implementación y mantenimiento de cableado estructurado y eléctrico.

6.6.2.15. El **CONTRATISTA** debe verificar con una periodicidad anual de las tierras existentes de potencia y comunicaciones, acometidas eléctricas, tableros, circuitos y tomacorrientes. Así como también de las grapas, sistemas, varillas de anclajes, distribución, tuberías conduit, canaletas, bandejas portacables y ductos eléctricos en general, y como resultado entregar un informe de la revisión.

6.6.2.16. El **CONTRATISTA** debe mantener la documentación actual de la infraestructura de cableado eléctrico y estructurado (entrega de planos, documentación de los elementos de configuración que componen el cableado eléctrico y estructurado de las sedes de acuerdo a los requerimientos del Fondo).

6.6.2.17. Descripción de cantidades de cableado estructurado y eléctrico instalado actual.

Sede A.

a) Tomas Reguladas. → 75
b) Tomas Normales. → 78
c) Datos y Voz. → 66

Sede B.

a) Tomas Reguladas. → 46
b) Tomas Normales. → 46
c) Datos y Voz. → 45

6.6.2.18. El sistema eléctrico existente de potencia está conformado por las acometidas desde los armarios principales hasta cada una de las dos (2) sedes del Fondo.

6.6.2.19. El sistema de corriente regulado de la Sede B, se toma desde el tablero regulado existente Piso 2, alimentando una UPS de 10 KVA, la cual se encuentra en instalada en el cuarto de cableado de esta sede y en la Sede A se tiene un tablero regulado en el piso 2 para alimentar una UPS de 20 KVA, la cual se encuentra en centro de cómputo.

6.6.2.20. Las demás instalaciones se encuentran en buen estado y se implementaron con materiales y mano de obra de primera calidad y de acuerdo con las norma vigente 2050 de ICONTEC y el RETIE del Ministerio de Minas y Energía.

7. DESCRIPCIÓN DE LAS SOLUCIONES PROPUESTAS.

A continuación de relacionan los componentes de hardware, software, licenciamiento y accesorios necesarios para la puesta en marcha de la soluciones objeto de contratación.

Solución de Seguridad Perimetral.	
Descripción:	Next Generatión Firewall (NGFW).
Marca:	SOPHOS UTM SG 210 HW Appliance.
Modelo:	SG 210.
Cantidades:	Dos (2).
Especificaciones técnicas de hardware:	Catalogo técnico (contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por el **CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.
Software:	Gestión y Sistema Operativo.
Licenciamiento:	Incluido.
Accesorios:	N/A.
Otros:	N/A.

Solución de Red Inalámbrica.	
Descripción:	Acces Point.
Marca:	CISCO – MERAKI.
Modelo:	MR-34.
Cantidades:	Seis (6) AP's, Una (1) controladora.
Especificaciones técnicas de hardware:	Catalogo técnico (contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por el **CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.
Software:	Gestión.
Licenciamiento:	Incluido.
Accesorios:	N/A.
Otros:	N/A.

Solución de Monitoreo de Infraestructura de TI.	
Descripción:	Solución de Monitoreo Infraestructura IT.
Marca:	IBOSS.
Modelo:	Enterprise 2160.
Cantidades:	Uno (1).
Especificaciones técnicas de hardware:	Catalogo técnico (contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por el **CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.
Software:	Gestión.
Licenciamiento:	Incluido.
Accesorios:	N/A.
Otros:	N/A.

Solución de Antivirus EndPoint.	
Descripción:	Solución de Antivirus EndPoint.
Marca:	SOPHOS.
Modelo:	SOPHOS ENDPOINT ANTIVIRUS.
Cantidades:	Setenta y Dos (72) licencias.
Especificaciones técnicas de hardware:	Catalogo técnico (contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por el **CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.
Software:	Gestión y Antivirus.
Licenciamiento:	Incluido.
Accesorios:	N/A.
Otros:	N/A.

Solución de Procesos de Backup.	
Descripción:	Librería y Software de Backup.
Marca:	Hewlett Packard.
Modelo:	Librería MSL 2024, HP Data Protector.
Cantidades:	Una (1) Librería.
Especificaciones técnicas de hardware:	Catalogo técnico (contenidos en las condiciones de participación, al igual que los ofrecimientos efectuados por el **CONTRATISTA**, en la propuesta presentada el 06 de Julio de 2015 y las aclaraciones efectuadas por dicha sociedad del 16 de julio de 2015.
Software:	Licencias de HP Data Protector para un (1) drive y ene (n) servidores. Agente para base de datos y correo electrónico MS Exchange.
Licenciamiento:	Incluido.
Accesorios:	N/A.
Otros:	N/A.

8. NIVELES DE SERVICIO MÍNIMOS.

El **CONTRATISTA** deberá compensar a **FOGACOOP** pagando una suma determinada mediante un porcentaje del valor del pago pactado en relación con la cuenta de control respectiva a cargo del contratista, cuando exista una falla durante un número de horas al mes (y su respectiva proporción mensual) sobre uno o varios de los servicios prestados, lo cual impide que estén disponibles en toda su extensión de forma ininterrumpida y estable para los usuarios del Fondo, dentro del horario establecido y por tanto afectan la prestación del servicio por causa imputable a la operación y a la plataforma computacional comprometida por el oferente; lo anterior implica la aplicación de penalizaciones y descuentos.

8.1 PARA LOS SERVICIOS DE SEGURIDAD PERIMETRAL

NIVEL DE SERVICIO	DISPONIBILIDAD	DESDE (<)	HASTA (>=)	DESCUENTO	
Disponibilidad General para los Ítem No. 1- servicios de Seguridad Perimetral.	99,9%	100%	99,90%	0%	Si la Disponibilidad es menor del 99.00% la penalización será el 100% del valor mensual del servicio afectado
		99,90%	99,75%	5%	
		99,75%	99,00%	30 %	

8.2 PARA LOS SERVICIOS DE SERVICIOS DE RED INALÁMBRICA INTEGRADA CON LA RED CORPORATIVA, LOS SERVICIOS DE MONITOREO DE INFRAESTRUCTURA DE TI, LOS SERVICIOS DE ANTIVIRUS ENDPOINT, LOS SERVICIOS DE PROCESOS DE BACKUP Y RESTAURACIÓN DE INFORMACIÓN Y EL SUMINISTRO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE CABLEADO ELÉCTRICO Y ESTRUCTURADO DEL FONDO.

NIVEL DE SERVICIO	DISPONIBILIDAD	DESDE (<)	HASTA (>=)	DESCUENTO	
Disponibilidad General de los servicios para los Ítem No. 2, 3, 4 y 5:	99,75%	100%	99,75%	0%	Si la Disponibilidad es menor del 99.00% la penalización será el 100% del valor mensual del servicio afectado
		99,75%	99,5%	5%	
		99,5%	99,0%	30 %	

NOTA: La disponibilidad es el porcentaje del tiempo en el cual la solución está disponible, medido durante un período determinado. El tiempo de indisponibilidad del servicio se empieza a contar a partir del momento en que se registra una falla, y se considera tiempo indisponible cuando una falla aparece por un período de un (1) minuto consecutivo. La disponibilidad del servicio se calcula con base en la siguiente fórmula:

FORMULA	EXPLICACIÓN DE LA FORMULA
D=(X / Y) x 100	• D: Porcentaje de disponibilidad del enlace. • X: Número de minutos en las cuales el Servicio estuvo disponible durante el mes, según el reporte de disponibilidad. • Y: Número de minutos al mes que debería estar disponible el Servicio, es decir veinticuatro (24) horas por sesenta (60) minutos, multiplicado por el número de días del periodo en cuestión.

9. TEST DE PENETRACIÓN E IDENTIFICACIÓN DE VULNERABILIDADES.

El **CONTRATISTA** deberá realizar hasta dos (2) test de penetración y vulnerabilidades a las soluciones de **SEGURIDAD PERIMETRAL y RED INALÁMBRICA INTEGRADA CON LA RED CORPORATIVA**, cada seis (6) meses, durante la ejecución del contrato. El test, consiste en realizar pruebas de penetración externas controladas e identificación de vulnerabilidades a las soluciones propuestas, a través de expertos en test de penetración y vulnerabilidades, quienes evaluarán la seguridad y los controles ubicados en el perímetro, emulando las posibilidades de acceso a la red con las que podría contar un intruso desde Internet.

El objetivo de este servicio es identificar las vulnerabilidades a las que están expuestos los servicios presentados por **FOGACOOP** a través de la RED, validando la posibilidad que tendría un intruso real de explotarlas, lo cual permitirá establecer los planes de acción para mitigar los riesgos. Los test de penetración y vulnerabilidades no deben generar situaciones explicitas de negación del servicio.

La realización de test de penetración y vulnerabilidades debe estar enmarcadas, como mínimo, en metodologías y mejores prácticas reconocidas mundialmente.

El **CONTRATISTA** debe indicar el procedimiento, actividades y cronograma aproximado mediante los cuales se ejecutarán el test de penetración y vulnerabilidades. Adicionalmente, éste deberá indicar, como mínimo una semana antes del inicio de cada prueba, una dirección o conjunto de direcciones IP públicas fijas, desde las cuales se realizarán el test de penetración y vulnerabilidades.

Como entregables de la aplicación de cada test de penetración y vulnerabilidades, el **CONTRATISTA** deberá proporcionar a **FOGACOOP** un informe final y documentación que soporte los hallazgos encontrados, los riesgos asociados y las recomendaciones técnicas para su mitigación. No obstante lo anterior, en caso de encontrarse vulnerabilidades críticas, se debe recomendar e indicar a **FOGACOOP** cómo proceder para mitigar los riesgos de manera inmediata sin necesidad de esperar el informe final.