MINISTERIO DE EDUCACIÓN PÚBLICA

DIRECCIÓN DE INFORMÁTICA DE GESTIÓN

MANUAL DE ESTÁNDARES INFORMÁTICOS

CÓDIGO: DVM-A-DIG-MAN-08

Noviembre, 2021

TABLA DE CONTENIDOS

1 HISTORIAL DE REVISIONES

Fecha actualización	Versión	Descripción	Responsable
2007	1		Francini Padilla Campos.
2012	4		Kattia Paniagua Alfaro. Delia Calderón Calvo. Pablo Ariel Mora Segura.
2019	5	Se le agregan los estándares de equipos con características mínimas, según las necesidades del MEP.	Shirley Calvo Bolívar. Marianella Cascante Otárola. Tanya Carrera Molina. German Peraza Castro. Ronny Rojas Vargas. Alberto Contreras Cruz. Marlon Vasquez Vásquez.
2021	6	Se ajusta este documento tomando en cuenta las mejores prácticas definidas en el Código Nacional de Tecnologías Digitales (CNTD) en relación con la adquisición, desarrollo y gestión de las tecnologías y los servicios digitales en el sector público costarricense; así como con los lineamientos estipulados por la Contraloría General de la República en las Normas de Control Interno para el Sector Público, en lo que respecta a la vinculación del Sistema de Control Interno (SCI) con la Calidad y el compromiso superior.	Ana Chacón Guevara. Tahyli Mondragón Fonseca. Marlon Vásquez Vásquez. German Peraza Castro. Ronny Rojas Vargas. Jenny Navarro Blanco. Maximo Varela Castro. Ana Marcela Barrantes Arias.

2 INTRODUCCIÓN

La Dirección de Informática de Gestión (DIG) del Ministerio de Educación Pública (MEP), es la unidad organizacional responsable de la administración de la plataforma tecnológica para brindar servicios eficientes, innovadores y seguros; que garanticen información integra, disponible y confiable para la toma de decisiones. Todo bajo procesos de gestión basados en las mejores prácticas establecidas en el marco internacional de gobernanza de TI.

La DIG ha desarrollado este documento, con el propósito de lograr establecer un marco de estándares de referencia, que garantice los niveles adecuados de integración, calidad y seguridad de los diferentes elementos tecnológicos. Es relevante indicar, que este debe tomarse en cuenta en los procesos de contratación de productos y/o servicios ejecutados por la organización o en la renovación de contratos de adquisiciones tecnológicas.

Las disposiciones técnicas contenidas en este documento, son un compendio de todas las necesidades tecnológicas que los departamentos de la DIG tienen a su cargo. Éstas deben mantenerse actualizadas de acuerdo con los avances tecnológicos y los requerimientos institucionales.

Para que los lineamientos y la estandarización sean efectivos, resulta necesario el cumplimiento obligatorio de los estándares, la metodología definida y el envío de la información específica que el órgano competente solicite.

3 DESCRIPCIÓN

La Dirección de Informática de Gestión se ha dado a la tarea de actualizar el Manual de Estándares Informáticos, en el cumplimiento de las recomendaciones efectuadas por la Contraloría General de la República.

Producto de esto, se obtiene un marco de referencia técnico que permite lograr homogeneidad y compatibilidad en la aplicación de los procesos informáticos orientados a las unidades de trabajo, mediante una planificación y desarrollo basada en la coordinación de procesos.

Los estándares informáticos indicados en este manual, pretenden generar un conjunto de especificaciones técnicas y procedimentales, que deben de ser usados consistentemente como guía para lograr así la unificación del desarrollo de software, diseño de bases de datos, la adquisición de tecnología y la administración de la plataforma tecnológica.

Por lo que, se entenderá por estándar informático todo aquel patrón o parámetro que permite establecer uniformidad en características de equipos, sistemas de cómputo, software de desarrollo y procedimientos de operación, con el cual se pretende

garantizar la integridad, compatibilidad, interoperabilidad y racionalidad en los procesos tecnológicos de la institución.

4 OBJETIVOS

4.1 Objetivo General

Establecer las directrices y los lineamientos relacionados al desarrollo, aplicación y control de los procesos informáticos, que deben ser acatados por las diferentes dependencias institucionales, a fin de mejorar los niveles de uniformidad, interoperabilidad, calidad, comunicación y coordinación de los principales procedimientos desarrollados por la DIG, para la administración de las tecnologías de información en el Ministerio de Educación Pública.

4.2 Objetivos Específicos

- Establecer estándares relacionados con software, equipo y comunicaciones involucrados en los procesos informáticos, a fin de lograr niveles de uniformidad, interoperabilidad, calidad, comunicación y coordinación en el desarrollo tecnológico Institucional.
- Asegurar que las directrices y los lineamientos existentes, vayan acorde a los estándares establecidos en este manual, para impulsar un crecimiento ordenado y estratégico.
- Evaluar los estándares informáticos periódicamente, en pro del mejoramiento de la calidad de los productos tecnológicos según las necesidades actuales y futuras del Ministerio.

5 ALCANCE

Los estándares que se establecen en este documento, están basados en el análisis de los procedimientos de operación de la Dirección de Informática de Gestión, para el aprovisionamiento de recursos tecnológicos, desarrollo de aplicaciones, administración de la infraestructura tecnológica y la prestación de servicios informáticos.

Se efectuará una regulación de los procedimientos, aplicando las mejores prácticas conocidas para la gestión de los recursos tecnológicos y su producto trascenderá en medida de conocimiento e información para su utilización por parte de las unidades organizacionales del Ministerio de Educación Pública.

6 DEFINICIONES Y ABREVIATURAS:

6.1 Abreviaturas:

BGP: *Border Gateway Protocol* o Protocolo de puerta de enlace de frontera.

BIOS: *Basic Input Output System* o sistema básico de entrada y salida.

CNTD: Código Nacional de Tecnologías Digitales.

CoS: Clase de Servicio.

CPU: *Central Processing Unit,* o Unidad Central de Procesamiento.

DIG: Dirección de Informática de Gestión.

DIMM: Módulo de memoria de dos líneas.

DPI: Puntos Por Pulgada.

DVI: *Digital visual interface* o interfaz Digital Visual.

ECC: Memoria con código de corrección de error.

FTP: *File Transfer Protocol* o Protocolo para la Transferencia de Archivos.

GB: *Gigabyte*.

GHz: *Gigahercios*.

HDD: *Hard Disk Drive* o discos duros mecánicos.

HDMI: *High-Definition Multimedia Interface* o Interface Multimedia de Alta Definición.

IEEE: *Institute of Electrical and Electronics Engineers* o Instituto de Ingenieros Eléctricos y Electrónicos.

IPDS: *Intelligent Printer Data Stream* o flujo de datos de la impresora inteligente.

IPSec: *Internet Protocol Security* o Seguridad del protocolo de Internet.

IPv4: *Internet Protocol Version 4.*

IPv6: *Internet Protocol Version 6.*

IPX/SPX: *Internetwork Packet eXchange/Sequenced Packet eXchange* o Intercambio de Paquetes entre Redes/Intercambio de Paquetes Secuenciales.

ISO: *International Organization for Standardization* u Organización Internacional para la Estandarización.

ITIL: *Information Technology Infrastructure Library* o Biblioteca de Infraestructura de Tecnologías de Información.

JPEG: *Joint Photographic Experts Group.*

LAN: *Local Area Network* o red de área local.

LCD: *Liquid Crystal Display* o Pantalla de cristal líquido.

LDP: *Digital Light Processing o* Procesamiento Digital de Luz.

Kbps: *Kilobits* por segundo.

MAI: Manual de Arquitectura de Información.

Mb: *Megabyte*.

MHz: *Megahercios*.

MEI: Manual de Estándares Informáticos.

MEP: Ministerio de Educación Pública.

OSI: *Open System Interconnection* o Modelo de interconexión de sistemas abiertos.

PCI Express: *Peripheral Component Interconnect Express* o Componente Periférico de Interconexión Express.

PCL5: *Printer Control Language* o Controlador PCL.

PDF: *Portable Document Format* o Formato de documento portable.

PMBOK: *Project Management Body of Knowledge* o Fundamentos para la Dirección de Proyectos.

PPI: Píxeles Por Pulgada.

Ppm: Páginas por minuto.

QoS: Calidad de servicios.

RAM: Memoria a corto plazo.

RTP: *Real-Time Transport Protocol* o Protocolo de Transporte en Tiempo Real.

SCI: Sistema de Control Interno.

Serial ATA o SATA: *Serial Advanced Technology Attachment* o una interfaz de transferencia de datos.

SFF: *Small Form Factor* ***o*** Factor de forma pequeña.

Sflow: *Sampled flow* o flujo de muestra.

SNMP: *Simple Network Management Protocol* o Protocolo simple de administración de red.

SRTP: *Secure Real–Time Transport Protocol* o Protocolo de Transporte Seguro en Tiempo Real.

TB: *Terabyte*.

TCP/IP: *Transmission Control Protocol/Internet Protocol* o Protocolo de Control de Transmisión/Protocolo de Internet.

TI: Tecnologías de la Información.

UDP: *User Datagram Protocol* o Protocolo para el intercambio de Datagramas.

USB: *Universal Serial Bus* o Bus Universal en Serie.

VGA: *Video Graphics Array* o pantalla estándar analógica de computadora.

VLANs: *Virtual LAN* o Red Virtual de Área Local.

VPN: *Virtual Private Network* o Red Privada Virtual.

WAN: *Wide Area Network* o Red de Área Extensa.

6.2 Definiciones:

Access Points: *Wireless Access point*, también conocidos como puntos de acceso. Son dispositivos para establecer una conexión inalámbrica entre equipos y pueden formar una red inalámbrica externa (local o internet) con la que interconectar dispositivos móviles o tarjetas de red inalámbricas.

Adobe PostScript 3: Permite que su impresora *EPSON®* imprima documentos con formato preparado para *PostScript®* del nivel ("level") 1 al 3.

Apple Talk: Conjunto de protocolos desarrollados por *Apple Inc*. para la interconexión de redes locales.

BGP: Sistema que utilizan los grandes nodos de Internet para comunicarse entre ellos y transferir una gran cantidad de información entre dos puntos de la Red.

Bluetooth: Especificación industrial para redes inalámbricas de área personal.

Boost: Potenciar algo en concreto.

Broadcast: Difusión masiva de información o paquetes de datos a través de redes informáticas. En el caso de la informática, *broadcast* o difusión es la transferencia de información desde un nodo emisor a una multitud de nodos receptores.

Buffer: Memoria de almacenamiento temporal de información, que permite transferir los datos entre unidades funcionales con características de transferencia diferentes.

Bypass: Circuito que actúa como válvula, modificando el flujo normal de datos hacia una ruta alternativa si se produce una caída de corriente o algún otro problema.

COBIT: Objetivos de Control para Tecnología de Información y Tecnologías relacionadas. Se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes.

Conector RJ45: Conector que se utiliza para conectar a redes dispositivos mediante un cable que puede ser de hasta 8 hilos en su interior.

CoS: Clase de Servicio, es la clasificación del tráfico específico manipulando los bits de la clase del servicio en el encabezado de trama.

Data Loss Prevention: Prevención de fuga de datos.

DDR5: Las nuevas memorias *RAM DDR5* empiezan a mostrar todo su potencial. Estos 12.600 millones de transferencias por segundo suponen el equivalente a una memoria *RAM* de 12.600 *MHz*. La mayor velocidad hasta la fecha en una memoria *RAM*.

Debug: Depurar.

Directory: El directorio activo o *Active Directory* (AD) es una manera de organizar y gestionar todos los elementos de una red informática.

Docking Station: Dispositivo o accesorio que sirve para convertir un ordenador portátil en un equipo de sobremesa.

DPI: Utilizado habitualmente para describir la resolución de una imagen.

Dúplex: Término utilizado en telecomunicación para definir un sistema que es capaz de mantener una comunicación bidireccional, enviando y recibiendo mensajes de forma simultánea.

Enclousure: Recinto.

Energy Star: Programa de la Agencia de Protección Ambiental de los Estados Unidos creado en 1992 para promover los productos eléctricos con consumo eficiente de electricidad, reduciendo de esta forma la emisión de gas de efecto invernadero por parte de las centrales eléctricas.

Fibra Monomodo: La fibra sólo puede propagarse un modo de la luz a la vez.

Fibra Multimodo: La fibra puede propagarse varios modos de la luz a la vez.

FTP: Protocolo usado para compartir archivos con otros usuarios.

Full-Duplex: Tipo de comunicación en el que los datos puede fluir de dos maneras al mismo tiempo.

Gateways: Conocido también como Puertas de enlace. Es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos. Posibilita compartir recursos entre dos o más ordenadores.

Half-Duplex: Transmisión de los datos que circulan en una sola dirección por vez. El canal de comunicaciones permite alternar la transmisión en dos direcciones, pero no en ambas direcciones simultáneamente.

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

HDMI: Conexión digital, de tamaño reducido que nos permite transmitir audio y vídeo en alta definición, sin comprimir, e incluso datos desde un equipo a otro con un único cable. Quizás sea la conexión más famosa y versátil actualmente.

Headphone: Audífono.

IEEE: Sociedad técnico-profesional más grande y prestigiosa del mundo, dedicada a promover y divulgar los avances científicos en las áreas de Ingeniería Eléctrica, Electrónica, Energética, Informática y afines.

IPDS: Protocolo de comunicación bidireccional o flujo de datos orientado a objetos entre sistemas informáticos e impresoras.

IPSec: Marco normalizado para asegurar las comunicaciones de *IP* mediante el cifrado y autenticación de cada paquete *IP* en un flujo de datos.

IPv4: Versión actual del Protocolo de Internet, el sistema de identificación que usa Internet para enviar información entre los dispositivos.

IPv6: Nueva versión del Protocolo de Internet.

IPX/SPX: Protocolos de transporte utilizados en las redes *Novell NetWare* que, juntos, corresponden a la combinación de *TCP* e *IP* en el conjunto de protocolos *TCP/IP*.

ITIL: Guía de buenas prácticas para la gestión de servicios de tecnologías de la información.

JPEG: Estándar de codificación y compresión de imágenes digitales.

JPG: Formato de compresión de imágenes, tanto en color como en escala de grises, con alta calidad.

LAN: Grupo de computadoras y dispositivos periféricos que comparten una línea de comunicación común o un enlace inalámbrico a un servidor dentro de un área geográfica específica.

LDP: Tecnología usada en proyectores y televisores de proyección.

Leasing: Permite utilizar activos productivos en la organización, sin necesidad de adquirirlos o ser propietario.

Linux: Sistema operativo semejante a *Unix*, de código abierto y desarrollado por una comunidad. Usado en computadoras, servidores, *mainframes*, dispositivos móviles, entre otros. Es multiusuario, multitarea y multiplataforma.

Multicast: Entrega de datos de forma simultánea a un grupo de nodos receptores como destino, desde un emisor como origen.

Netflow: Estándar más utilizado para estadísticas de datos de flujo. Monitorear y registrar todo el tráfico a medida que pasa hacia o desde una interfaz.

NVIDIA Corporation: Empresa multinacional especializada en el desarrollo de unidades de procesamiento gráfico y tecnologías de circuitos integrados para estaciones de trabajo, ordenadores personales y dispositivos móviles.

OSI: Propuesta que hizo la Organización Internacional para la Estandarización para estandarizar la interconexión de sistemas abiertos.

Overflow: Desbordamiento.

PC3-12800: La memoria *DDR3*-1600 tiene una clasificación de módulo de *PC*3-12800, que significa que la tasa de datos máxima del módulo es de 12,8 *GB/s*.

PCL5: Lenguaje de descripción de páginas muy sofisticado, desarrollado por *Hewlett Packard* para impresoras de chorro de tinta.

PCL6: Orientado a imprimir gráficos en color, así como texto.

PDF: Formato de archivo portátil y universal, que conserva las fuentes, imágenes y maquetación de los documentos originales creados en una amplia gama de aplicaciones y plataformas.

PMBOK: Manual que brinda a las organizaciones un conjunto de procesos, modelos de administración, criterios y más aspectos favorables para la dirección de proyectos. Para ello, otorga una serie de herramientas que permiten identificar procesos generales y dar resultados óptimos.

PostScript 3: El *kit* de *Adobe® PostScript® 3™* permite que su impresora *EPSON®* imprima documentos con formato preparado para *PostScript®* del nivel ("level") 1 al 3.

Rack: Estructura metálica o soporte cuya misión es alojar componentes informáticos y accesorios.

RADIUS: Radio.

RAM DDR3: Memoria estándar ya establecida.

Router: Dispositivo que ofrece una conexión *Wi-Fi*, que normalmente está conectado a un *módem* y que envía información de Internet a tus dispositivos personales, como ordenadores, teléfonos o *tablets.*

Salida *AV:* Conexión digital de tamaño reducido, que nos permite transmitir audio y vídeo en alta definición e incluso datos.

Scroll: Desplazar o deslizar.

Serial ATA o SATA: Interfaz de transferencia de datos en serie entre la placa base y algunos dispositivos de almacenamiento.

Servidor *blade:* Tipo de computadora para centros de procesamiento de datos, específicamente diseñado para aprovechar el espacio, reducir el consumo y simplificar su explotación.

Sflow: Utiliza muestras estadísticas del tráfico de datos para garantizar la escalabilidad de interfaces con grandes cantidades de datos.

SNMP: Protocolo para la gestión de la transferencia de información en redes, especialmente para uso en *LAN*, dependiendo de la versión elegida.

Snooping: Usurpar una identidad electrónica para ocultar la propia identidad y así cometer delitos en Internet.

Software: Equipamiento o soporte lógico de un sistema informático. Comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

SRTP: Perfil de extensión RTP que agrega funciones de seguridad, como autenticación de mensaje, confidencialidad y protección de respuesta, mayormente pensadas para las comunicaciones *VoIP*.

SSHv2: Protocolo que proporciona una conexión de acceso remoto segura a los dispositivos de red. La comunicación entre el cliente y el servidor se cifra tanto en la versión 1 de *SSH* como en la versión 2 de *SSH*.

SSM: Herramienta de propósito general utilizada para la resolución de problemas, por lo que es especialmente útil en la fase previa al desarrollo para identificar problemas organizativos y posibles soluciones a estos.

Switch: Dispositivo de interconexión utilizado para conectar equipos en red, formando lo que se conoce como una red de área local (LAN). También conocido como Conmutador.

Tarjeta Red Ethernet: Interfaz entre un nodo y el cable de red, respetando el protocolo *Ethernet*.

TCP/IP: Conjunto de reglas estandarizadas que permite a los equipos comunicarse en una red como Internet.

TIFF: Formato de archivo de imagen que se utiliza generalmente para trabajar con datos de imagen sin procesar.

Throughput: Tasa de producción o velocidad a la que algo se puede procesar. En las redes de comunicación, *throughput* es esencialmente sinónimo del consumo de ancho de banda digital.

Touchpad: Panel táctil que permite controlar un cursor o facilitar la navegación a través de un menú o de cualquier interfaz gráfica.

Trunking: Función para conectar dos *switches*, *routers* o servidores, del mismo modelo o no, mediante 2 cables en paralelo en modo *Full-Duplex*.

UDP: Protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 o de Transporte del Modelo OSI).

Unidad SATA: Interfaz de bus de computadoras para la transferencia de datos entre la placa base y algunos dispositivos de almacenamiento, como la unidad de disco duro, lectora y grabadora de discos ópticos.

VLANs: Acrónimo de virtual *LAN* o Red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

VPN: Virtual Private Network, es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

WAN: Red privada de telecomunicaciones geográficamente distribuida, que interconecta múltiples Redes de Área Local (*LAN*).

Web: Conjunto de información que se encuentra en una dirección determinada de Internet.

Windows: Sistema operativo para computadoras, cuyo propietario es de Microsoft.

Wireless: Red inalámbrica conocida como Wireless Network. Se utiliza para designar la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica.

XPS: Formato independiente de plataforma, que se podría leer en cualquier sistema operativo.

7 AUTORES:

Ing. Francini Padilla Campos, Departamento de Bases de Datos.

8 ACTUALIZADO POR:

Ana Chacón Guevara, Departamento Sistemas de Información, noviembre 2021.
Tahyli Mondragón Fonseca, Departamento Soporte Técnico, noviembre 2021.
Marlon Vásquez Vásquez, Departamento Soporte Técnico, noviembre 2021.
German Peraza Castro, Departamento Redes y Telecomunicaciones, noviembre 2021.
Ronny Rojas Vargas, Departamento Redes y Telecomunicaciones, noviembre 2021.
Jenny Navarro Blanco, Departamento Base de Datos, noviembre 2021.
Maximo Varela Castro, Departamento Adquisición Tecnológica, noviembre 2021.
Ana Marcela Barrantes Arias, Departamento Gestión y Control Informático, noviembre 2021.

9 DIRECTRICES

- Los funcionarios de los diversos departamentos que conforman la DIG; responsables de la adquisición de estos bienes y/o servicios, deben informar al equipo de actualización del documento denominado Modelo de Arquitectura de Información (MAI) de los cambios en los estándares definidos en este documento, según su obsolescencia o mejoramiento tecnológico.
- El Director y las Jefaturas de los diversos departamentos de la DIG deben velar por el cumplimiento de cada uno de los estándares definidos.

10 ESTÁNDARES INFORMÁTICOS

Los estándares que se detallan a continuación, cumplen con las mejores prácticas definidas en el Código Nacional de Tecnologías Digitales (CNTD) en relación con la adquisición, desarrollo y gestión de las tecnologías y los servicios digitales en el sector público costarricense; así como con los lineamientos estipulados por la Contraloría General de la República en las Normas de Control Interno para el Sector Público, en lo que respecta a la vinculación del Sistema de Control Interno (SCI) con la Calidad y el compromiso superior.

A continuación, se define una serie de estándares que deben considerarse como guía en el diseño de la base de datos (nomenclatura de los objetos), en etapas del desarrollo de sistema de información, estudios de factibilidad y determinación de la cantidad, así como las características de los equipos de cómputo.

11 ESTÁNDARES PARA LA ADQUISICIÓN DE EQUIPO DE CÓMPUTO

La existencia de los estándares para la adquisición de bienes y/o servicios, ya sea por modalidad de compra y/o alquiler, tiene como objetivo que las propuestas diseñadas para el mejoramiento de los bienes y/o servicios Informáticos se orienten en la satisfacción de las necesidades institucionales.

La adquisición de equipo de cómputo, quedará sujeta a los lineamientos establecidos en este documento.

11.1 Dimensionamiento de las características técnicas de los equipos de cómputo

Al comprar y/o arrendar equipo de cómputo, es necesario dimensionar el fin para el cual se desea adquirir dicho equipo. A continuación, se presenta la lista de consideraciones y/o especificaciones técnicas que se deben tomar en consideración según el tipo de equipo que se requiera:

11.1.1 Generalidades:

A continuación se definen aspectos básicos concernientes a cualquier tipo de equipo:

a) **Propósito del equipo:** Antes de iniciar con el dimensionamiento técnico de cualquier equipo, se deberá establecer claramente el

propósito de su adquisición, es decir, deberá definirse en detalle cual es la necesidad que se espera solventar con la adquisición del equipo.

b) **Entorno de operación:** Se deberá analizar el entorno de la ubicación en dónde se colocará el equipo por adquirir, y evaluarse aspectos como: temperatura, polvo, espacio físico, seguridad, tipo de soporte o accesorios para su instalación, estado de la red eléctrica y la de datos, entre otros. Todo lo anterior, con el propósito de realizar un análisis del entorno y determinar las mejoras y/o modificaciones que requiera el entorno de operación, antes de la colocación del equipo.

c) **Capacitación:** Siempre que se adquiera equipo con características tecnológicas de reciente desarrollo o implementación, deberá capacitarse al personal responsable de la gestión de estos equipos, con el objetivo de realizar una administración eficiente de la plataforma.

d) **Garantías:** Para cualquier compra de equipo, deberá considerarse solicitar una garantía completa para todos sus componentes. La duración de ésta se deberá determinar en función de los requerimientos y criticidad del proceso o servicio para el cual se desea adquirir el equipo.

e) **Alta disponibilidad:** Todo equipo de cómputo destinado a soportar procesos críticos y de alto riesgo, que administren y/o resguarden información de alta importancia e interés para la Administración, deberá contar con todas las condiciones que garanticen una alta disponibilidad y tolerancia a fallos; contemplando desde su entorno de operación (características de disponibilidad del centro de datos dónde se coloque el equipo), características de redundancia propia atinentes a la arquitectura del equipo (redundancia en fuentes de poder, discos, controladoras, red, entre otros) y finalmente deberán establecerse mecanismos ágiles para la resolución de incidencias, tales como, contratos de soporte, extensiones de garantía del fabricante, mantenimientos preventivos, entre otros.

f) **Experiencia de los proveedores:** La Administración debe asegurarse que los proveedores que deseen participar de procesos licitatorios, cuenten con un grado de experiencia atinente a la criticidad de los bienes y/o servicios que se deseen adquirir, por ende, se deberá establecer mecanismos que permitan la calificación de esa experiencia.

g) **Experiencia del personal técnico:** Cuando los requerimientos y el nivel de criticidad lo requieran, deberá evaluarse la experiencia profesional del personal técnico de los proveedores de bienes y/o servicios. Siempre y cuando el modelo de contratación lo requiera, deberán solicitarse la incorporación de personal certificado en el modelado de procesos (*ITIL, COBIT, PMBOK*, entre otros).

h) **Calidad del equipo:** El equipo que requiera la Administración para atender una necesidad o complemento de un proyecto, deberá contar con estándares de productividad y ser reconocido en el mercado por su calidad. Sus características de operación y producción deberán estar soportadas por estándares de sostenibilidad ambiental.

i) **Centros de servicio y distribución:** Se debe velar por que los bienes y/o servicios adquiridos cuenten con un soporte adecuado y respaldo de amplia gama. Que este pueda ser provisto por más de un proveedor, minimizando los riesgos relacionados a la dependencia de un único proveedor.

j) **Soporte:** Según la determinación de los requerimientos de criticidad de los bienes y/o servicios por adquirir, deberá considerarse siempre un plan de mantenimiento tanto preventivo como correctivo, estableciendo características tales como: alcances, tiempos de respuesta y sanciones por el incumplimiento de éstas cuando aplique.

k) **Esquemas de servicio:** Dependiendo de las características del bien y/o servicio a contratar, deberán detallarse las responsabilidades de las partes así como los alcances del servicio que la empresa proveedora deberá brindar durante la relación contractual.

l) **Canales de comunicación:** Deberán definirse los canales de comunicación entre las partes así como los responsables de la ejecución y control de las actividades que se planteen en un cronograma de proyecto.

11.1.2 Estándar de Microcomputadoras Portátiles-Línea 1

Memoria	8 *GB* de memoria *DIMM DDR3* o superior, para laptop *PC3-12800* de 1600 *MHz* este en un solo banco. Expandible a 16 *GB*.
Procesador	Procesador igual o superior en rendimiento al *Intel Core i7-4600M* de cuarta generación de 2.9 *GHz* a 3.6 *GHz* con turbo *boost* o su similar en *AMD*.
Bus y arquitectura	Bus del sistema de 1600 *MHz*. Debe tener un sistema de enfriamiento que evite el recalentamiento del procesador y las tarjetas internas adecuado y acorde.
Chasis	Anti-golpes.
Capacidades de vídeo y gráficos	Tarjeta de video de 512 *Mb* de memoria o Superior, integrada a la tarjeta madre.
Monitor	Pantalla mínimo de 13.1” pulgadas hasta un máximo de 14.1” pulgadas diagonal, tecnología *LCD*

	o superior con antirreflejo.
Conectividad	Tarjeta de Red *Ethernet* de 100/1000, Tarjeta inalámbrica interna o integrada compatible con 802.11 g/n. Además tecnología inalámbrica *Bluetooth*.
Unidades de almacenamiento	Disco duro de 500 *GB* o superior Tecnología *Sata* o superior, velocidad acorde con la tecnología. Contiene una herramienta o soporte que permite proteger el disco duro contra daños provocados por golpe y vibraciones.
DVD/RW	Posee una Unidad *SATA* de *DVD+/-RW* (8x).
Capacidades de administración y seguridad	Contraseña para acceso al *BIOS*.
Cámara y Sonido	Cámara *web* de alta definición mínimo 720pm, con micrófono incorporado Adaptador de sonido alta definición y con parlantes y micrófono incorporado, en ambos casos el micrófono debe existir.
Teclado	Teclado en español.
Interfaces	Con al menos 2 puertos *USB* 2.0 y (1) 3.0 de velocidad, puerto de entrada para micrófono, conector *RJ45* y (1) *VGA* y (1) *HDMI*, 1 conector para *Docking*.
Mouse	Sensitivo al tacto. Con al menos puntero: *Touchpad*.
Aditamentos	Maletín de mano acorde con el tamaño de la máquina, cables de poder, manuales de usuario en español, indicar *software* adicional de la portátil.
Almohadilla	Con apoyo para la muñeca de espuma suave, ergonómico, con reverso antideslizante.
Cada computadora portátil incluye una base de expansión (*Docking Station*): De la misma marca de la portátil, que proporciona al menos los siguientes puertos: 4 puertos *USB1*, *DVI*, 1 *VGA*, 1 puerto *RJ*-45, salida *AV*, *line-in*.	
Incluye los siguientes accesorios	
Teclado en español:	Teclado (físico y lógico) conexión *USB*. Ergonómico.
***Mouse* óptico de dos botones:**	Con la función *Scroll*, conexión *USB*, de la misma marca y compatibles con el modelo de la portátil.
Monitor tecnología (*LED*) o superior.	Con antirreflejo de 48.26 cm (19”), todos de la misma marca y compatibles con el modelo de la portátil.

11.1.3 Estándar Microcomputadoras Portátiles-Línea 2

Memoria	8 *GB* de memoria *DIMM DDR3* o superior, para *laptop PC3*-12800 de 1600 *MHz* este en un solo banco. Expandible a 16 *GB*.
Procesador	Al menos un procesador igual o superior en rendimiento al *Intel Core i7 – 4702QM* de cuarta generación de 2.2 *GHz* a 3.2 *GHz* con turbo *boost* o su similar en *AMD*.
Bus y arquitectura	Bus del sistema de 1600 *MHz*. Debe tener un sistema de enfriamiento que evite el recalentamiento del procesador y las tarjetas internas adecuado y acorde.
Capacidades de vídeo y gráficos	Tarjeta de video de 512 *Mb* de memoria o Superior. Esta debe ser integrada a la tarjeta madre.
Monitor	Con pantalla de al menos 15.1", hasta un máximo de 15.6 pulgadas diagonal, tecnología (*LED*) o superior. Con antirreflejo.
Conectividad	Tarjeta de Red *Ethernet* de al menos 100/1000, Tarjeta inalámbrica interna o integrada compatible con 802.11 *g/n*. Además tecnología inalámbrica *Bluetooth*.
Unidades de almacenamiento	Disco duro de 500 *GB* o superior Tecnología *Sata* o superior, velocidad acorde con la tecnología. Contiene una herramienta o soporte que permite proteger el disco duro contra daños provocados por golpe y vibraciones.
DVD/RW	Debe de poseer una Unidad *SATA* de *DVD+/-RW* (8x).
Capacidades de administración y seguridad	Contraseña para acceso al *BIOS*.
Cámara y Sonido	Cámara *web* de alta definición mínimo 720pm, con micrófono incorporado Adaptador de sonido alta definición y con parlantes y micrófono incorporado, en ambos casos el micrófono debe existir.
Teclado	Teclado en español.
Interfaces	Con al menos 2 puertos *USB* 2.0 y 1 puerto 3.0 de velocidad, puerto de entrada para micrófono, conector *RJ45* y (1) *VGA* y (1) *HDMI*.
Mouse	Sensitivo al tacto. Con al menos puntero: *Touchpad*. Mouse óptico de dos botones, con la función *Scroll*, conexión *USB*.
Aditamentos	Maletín de mano acorde con el tamaño de la máquina, cables de poder, manuales de usuario en

	español, indicar software adicional de la portátil.
Almohadilla	Con apoyo para la muñeca de espuma suave, ergonómico, con reverso antideslizante.

11.1.4 Estándar de Microcomputadoras de Escritorio- Línea 3

Memoria	Memoria *DDR3* de 8 *GB* 1600 *MHz* o superior, con capacidad de ampliarse a 16 *GB*.
Procesador	Similar o superior a *Intel Core i7*-4770 de cuarta generación de 3.*4GHz* a 3.9 *GHz* con turbo *boost*, de sócalo *LGA1150* o superior.
Chipset	*Chipset Intel* Q85 o superior.
Chasis	Tipo *Small Form Factor*, o Media Torre.
Capacidades de vídeo y gráficos	*PCI Express* independiente de *1GB DDR3* o superior.
Monitor	Tipo *LCD* de panel plano de 48,26cm (19") en diagonal, anti reflejo resolución 1280*1024 *píxeles* como mínimo. Con pedestal giratorio y altura ajustable.
Conectividad	Tarjeta de Red integrada *Ethernet* 100/1000. Tarjeta de red inalámbrica 802.11 g/n. integrada o de puerto *PCI*.
Fuente de poder	Soporta la configuración máxima del equipo, (110-200W), con eficiencia máxima del 90%, Certificada.
Unidades de almacenamiento	Disco duro de 500 *Gb* o superior, Tecnología *Sata* 6.0Gb/s, velocidad acorde con la tecnología.
DVD/RW	Poseer una Unidad *SATA* de *DVD+/-RW* (8x) + *DL* o superior.
Puertos	Conector para monitor externo (1) *VGA*, conector para micrófono y conector para audífono. Puerto paralelo bidireccional, (2) *PCI Express* x1 y (1) *PCI Express* x16.Conector *RJ45*.
Sonido	Tarjeta de sonido igual o superior Audio AC97 Integrada con salida sonido de 2.1.
Tarjeta madre	*Serial ATA*. *SATA* 3.*0 Gb/s And Sata* 6.*0Gb/s*. Con cuatro ranuras *SATA*.
Teclado	Teclado en español (físico y lógico).
Interfaces	Con siguientes puertos: Frontales al menos (2) *USB* 2.0. En la parte de atrás (4) *USB* 2.0. En la parte de atrás (2) *USB* 3.0.

	Los Puertos *USB* 3.0 compatibles con dispositivos *USB* 2.0, totalmente verificados.
Mouse	Mouse óptico de dos botones, con la función *Scroll*, conexión *USB*.
Almohadilla	Con apoyo para la muñeca de espuma suave, ergonómico, con reverso antideslizante.

11.1.5 Estándar de Microcomputadoras de Escritorio- Línea 4

Memoria	Memoria *DDR3* de 8 *GB* 1600 *MHz* o superior, con capacidad de ampliarse a 16 *GB*.
Procesador	Similar o superior en rendimiento a *Intel Core* i7-4770 de cuarta generación de 3.4 *GHz* a 3.9 *GHz* con turbo *boost* de formato *LGA1155* o superior.
Chipset	*Chipset Intel* Q85 o superior.
Chasis	Tipo *Small Form Factor*, o Media Torre.
Capacidades de vídeo y gráficos	*PCI Express* independiente de *1GB DDR3* o superior. Salida para 2 monitores.
Monitor	Tipo *LCD* de panel plano de 48,26cm (19") en diagonal, anti reflejo resolución 1280*1024 *píxeles* como mínimo. Con pedestal giratorio y altura ajustable.
Conectividad	Tarjeta de Red integrada *Ethernet* 100/1000. Tarjeta de red inalámbrica 802.11 g/n. integrada o de puerto *PCI*.
Fuente de poder	Soporta la configuración máxima del equipo, (110-200W), con eficiencia máxima del 90%, Certificada.
Unidades de almacenamiento	Disco duro de 500 *Gb* o superior, Tecnología *Sata* 6.*0Gb/s*, velocidad acorde con la tecnología.
DVD/RW	Poseer una Unidad *SATA* de *DVD+/-RW* (8x) + DL o superior.
Puertos	Conector para monitor externo (1) *VGA*, conector para micrófono y conector para audífono. Puerto paralelo bidireccional, (2) *PCI Express* x1 y (1) *PCI Express* x16.Conector *RJ45*.
Sonido	Tarjeta de sonido igual o superior Audio AC97 Integrada con salida sonido de 2.1.
Tarjeta madre	Controladora *SATA*. *Serial ATA*. *SATA* 3.0 *Gb/s And Sata 6.0Gb/s*. Mínimo Cuatro ranuras *SATA*.
Teclado	Teclado en español (físico y lógico).
Interfaces	Con los siguientes puertos:

	Frontales al menos (2) *USB* 2.0. En la parte de atrás (4) *USB* 2.0. En la parte de atrás (2) *USB* 3.0. Los Puertos *USB* 3.0 compatibles con dispositivos *USB* 2.0, totalmente verificados.
Mouse	*Mouse* óptico de dos botones, con la función *Scroll*, conexión *USB*.
Almohadilla	Con apoyo para la muñeca de espuma suave, ergonómico, con reverso antideslizante.

11.1.6 Estándar de Microcomputadoras Workstation - Línea 5

Memoria	Memoria *RAM* de 16 *GB* 1333/1600 *MHz*, *DDR3* Tipo *ECC* para *Workstation*. Con capacidad de expansión a 32 *GB*.
Procesador	Procesador igual o superior en características al *Intel Xeon Intel QPI E*5-1650 (*12M* Cache, 3.2 *GHz*).
Gabinete	Gabinete de 3 ranuras *PCI express* o una combinación de ambas, las 2 libres.
Chasis	Media Torre.
Capacidades de vídeo y gráficos	Tarjeta de video 2.0GB video *DDR5* dedicada (Externa) no compartida con el sistema. *NVIDIA* o *Ati* con conexiones *HDMI* y *DVI*. Con capacidad de expansión de otra tarjeta adicional según se requiera.
Monitor	Monitor *LCD* de 24 pulgadas, Tecnología *LED* o superior, Anti reflejo y anti brillo. Resolución 1920 x 1080p.
Capacidad de administración y seguridad	Contraseña para acceso al *BIOS*. Opcional: Un marchamo o precinta de alta seguridad u otro para asegurar contenido del *CPU*.
Conectividad	Conectividad tarjeta de red *Gigabit Ethernet* de 100/1000. Además, tarjeta inalámbrica interna o integrada compatible con 802.11 *g/n.*
Fuente de poder	Soporta la configuración máxima del equipo, (110-200W), con eficiencia máxima del 90%, Certificada.
Unidades de almacenamiento	Disco Duro unidad de *1TB* o superior *SATA* 3.*5Gb*/s, (*64MB* de cache o *buffer*.
DVD/RW	Poseer una Unidad *SATA* de *DVD+/-RW* (8x) + *DL* o superior.
Sonido	Tarjeta de sonido igual o superior Audio AC97 Integrada con salida sonido de 2.1 como mínimo.
Tarjeta madre	Controladora *SATA*.

	Serial *ATA*. *SATA* 3.0 *Gb/s And Sata 6.0Gb/s.* Mínimo Cuatro ranuras *SATA*.
Teclado	Teclado en español (físico y lógico).
Interfaces	Con los siguientes puertos: Frontales al menos (2) *USB* 2.0. En la parte de atrás (4) *USB* 2.0. En la parte de atrás (2) *USB* 3.0. Un (1) puerto de red *RJ45*. Micrófono y *Headphone*, frontales 3.5 mm. Los Puertos *USB* 3.0 compatibles con dispositivos *USB* 2.0, totalmente verificados.
Mouse	Mouse óptico de dos botones, con la función *Scroll*, conexión *USB*.
Almohadilla	Con apoyo para la muñeca de espuma suave, ergonómico, con reverso antideslizante.

11.1.7 Estándar de Microcomputadoras Workstation - Línea 6

Memoria	Memoria *RAM* instalada de 16 *GB* 1333/1600 *MHz*, *DDR3* Tipo *ECC* para *Workstation*. Con capacidad de expansión a 32 *GB*.
Procesador	Procesador igual o superior en características al *Intel Xeon Intel QPI* E5-1650 (12M Cache, 3.2 GHz).
Gabinete	Gabinete de 3 ranuras *PCI express* o una combinación de ambas, las 2 libres.
Chasis	Media Torre.
Capacidades de vídeo y gráficos	Tarjeta de video 2.*0GB* video *DDR5* dedicada (Externa) no compartida con el sistema. *NVIDIA* o *Ati* con conexiones *HDMI* y *DVI*. Con capacidad de expansión de otra tarjeta adicional según se requiera.
Monitor	Monitor *LCD* de 19 pulgadas, Tecnología *LED* o superior, Anti reflejo y anti brillo. Resolución 1920 x 1080p.
Conectividad	Conectividad tarjeta de red *Gigabit Ethernet* de 100/1000. Además, tarjeta inalámbrica interna o integrada compatible con 802.11 g/n.
Fuente de poder	Soporta la configuración máxima del equipo, (110-200W), con eficiencia máxima del 90%, Certificada.
Unidades de almacenamiento	Disco Duro unidad de *1TB* o superior *SATA* 3.*5Gb/s*, (*64MB* de cache o *buffer*.
DVD/RW	Unidad *SATA* de *DVD+/-RW* (8x). DL o superior.

Sonido	Tarjeta de sonido igual o superior Audio AC97 Integrada con salida sonido de 2.1 como mínimo.
Tarjeta madre	Controladora *SATA*. Serial *ATA*. *SATA* 3.0 *Gb/s And Sata 6.0Gb/s.* Mínimo Cuatro ranuras *SATA*.
Teclado	Teclado en español (físico y lógico).
Interfaces	Con al menos los siguientes puertos: Frontales al menos (2) *USB* 2.0. En la parte de atrás (4) *USB* 2.0. En la parte de atrás (2) *USB* 3.0. Un (1) puerto de red *RJ45*. Micrófono y *Headphone*, frontales 3.5 mm. Los Puertos *USB* 3.0 deben ser compatibles con dispositivos *USB* 2.0, totalmente verificados.
Mouse	*Mouse* óptico de dos botones, con la función *Scroll*, conexión *USB*.
Almohadilla	Con apoyo para la muñeca de espuma suave, ergonómico, con reverso antideslizante.

11.2 Dimensionamiento de las características técnicas de las impresoras

Los aspectos indicados en el punto 11.1.1 Generalidades, también aplican para las impresoras.

A continuación, se presenta la lista de especificaciones técnicas que se deben tomar en consideración según el tipo de impresora que se requiera:

11.2.1 Estándar de Impresoras Láser Blanco y Negro de Mediano Volumen

Función	Impresora.
Velocidad de Impresión	Mínima de 45 *ppm*, Se acepta variación sobre la base de +/- 10 *ppm*.
Salida de Primera Hoja	Máximo 8 segundos, Se acepta variación sobre la base de +/- 3 segundos.
Procesador	600 *MHz* mínimo.
Resolución	600 x 600 *dpi* mínimo.
Memoria	512 *MB RAM* como mínimo. Con Capacidad de Expandir, o en su defecto una memoria al menos del 150% mayor de la base solicitada.
Disco Duro	Mínimo 80 *GB HDD*.
Capacidad de impresión	De 3000 a 20,000 documentos mensuales y un ciclo

	de trabajo mensual máximo de 200.000 impresiones.
Rendimiento del tóner	Mínimo 15.000 al 5%.
Capacidad de Papel	Una Bandeja principal con capacidad de 500 hojas con posibilidad de adicionar una bandeja más de 500 hojas en un futuro, y una bandeja "*Bypass*" de al menos 100 hojas.
Alimentador de Papel	Mínimo 50 hojas.
Tamaño de Papel	A6, A5, A4, entre otros.
Interface	Una ranura de tarjeta interna *USB* de al menos 2.0 o superior (Tipo B) *Gigabit Ethernet* (10/100/1000) Puerto frontal *USB* 2.0 o superior (Tipo A).
Puerto adicional inalámbrico	Debe tener la capacidad de incorporación de tarjeta, Opcional.
Nivel de Ruido	55 *dB* Máximo. Se acepta variación sobre la base de + / -, 15 *dB*.
Ahorro de energía	Certificado por *Energy Star*.
Alimentación Eléctrica	120v, 60 *Hz*,12 A.
Dúplex	Automático.
Lenguaje	De descripción de páginas (*LDP*): al menos *PCL5*, *PCL6*. *Adobe PostScript* 3, *PDF*, *IPDS* (opcional).
Compatibilidad OS	Compatibilidad 100% con el último Sistema operativo en el Mercado. Sistemas operativos: *Windows* 10.0, *Windows* 8.1, *Windows* 8, *Windows* 7, *Windows XP/Server* 2003/*Vista*/*server Systems* 2008/7; *Mac OS* X 10.2; *Linux*.
Tiempo de Calentamiento	Máximo 45 segundos (se aceptan todos los tiempos inferiores a este).
Protocolo de Red	*TCP/IP* (*IPv4*, *IPv6*); opcionales *IPX/SPX*, *Apple Talk*, *UDP*.
***Software* de administración**	▪ Debe contar con *software* propio de administración, que permita asignar cuotas por usuario, tanto en las funciones de impresión. ▪ El *software* deberá permitir el acceso o no a las diferentes funciones del equipo, de acuerdo al perfil que el usuario tenga definido. ▪ El *software* deberá permitir identificar el detalle de copias e impresiones tales como: usuario, *dúplex*, cantidad de hojas, color o mono, nombre del documento impreso, así como un informe detallado de transacciones por equipo. Los reportes anteriores deben ser exportados a *Excel* y la información deberá ser almacenada en una base de datos para consultas posteriores. ▪ El *software* deberá permitir limitar el color por grupo, por usuario o por equipo.

	▪ El *Software* deberá permitir contabilizar el consumo y costos de impresión que cumpla con las especificaciones siguientes: ▪ Contabilización de consumos y costos desde aplicaciones bajo *Windows*. ▪ Definición de cuotas en color y/o monocromático que podrá ser consumido en impresiones o copias. ▪ Registrar los siguientes datos por cada impresión: ▪ Cuenta de acceso del usuario que realiza la impresión. ▪ Fecha y hora de la impresión. ▪ Nombre del archivo impreso. ▪ Cantidad de páginas impresas. ▪ Centro de costos al que pertenece el usuario. ▪ Especificar si se trata de una impresión doble cara o simple. ▪ Especificar si la impresión es monocromática o color. ▪ Tamaño del papel. ▪ Identificación de la *PC* de donde se envió la impresión. ▪ Funcionalidad de Retención de impresiones: ▪ Que permita habilitar la retención de los documentos impresos, permitiendo al usuario liberarlos posteriormente mediante autenticación. ▪ Permitir la eliminación del documento desde el equipo multifuncional, antes de que este sea impreso. ▪ Definir el tiempo de vencimiento de los documentos para la eliminación automática de los mismos si el usuario no los libera o elimina desde el equipo multifuncional. ▪ Posibilidad de delegar impresiones para que otro usuario pueda liberarlas. ▪ Permitir la liberación de las impresiones en cualquier equipo multifuncional de la institución sin importar la ubicación. ▪ Posibilidad de imprimir el documento y mantenerlo en la cola de impresión para una reimpresión posterior. ▪ Auditoría de las funciones de impresión y

	copiado en el caso de los multifuncionales. ▪ Deberá permitir generar los siguientes reportes: ▪ Los reportes de consumo y costos de impresión se presentan en forma electrónica en un formato adecuado. El objetivo de estos reportes es permitir el análisis y control del consumo de impresión de las diferentes gerencias hasta los usuarios finales. ▪ Generar Reporte que contenga el consumo mensual, cantidad de páginas impresas en blanco y negro, cantidad de páginas impresas a color por modelo de equipo, bajo la estructura Centro de Costo y usuario. ▪ Generar reporte consolidado y detallado mensual. ▪ Generar reporte de tendencia del consumo de impresión consolidado de forma mensual. ▪ Facilidades para análisis estadísticos del consumo para la emisión de recomendaciones para optimizar el consumo de impresión y su costo. ▪ Debe permitir la creación de cuotas de impresión por usuario para asignar máximos de impresión. ▪ La instalación de *hardware* y *software* e implementación antes mencionado, corre por cuenta del contratista sin ningún costo para la administración.

11.2.2 Estándar de Multifuncionales a Color Bajo Volumen

Función	Impresora, Fax, Escáner y Copiadora.
Velocidad de Impresión BN/COLOR	Mínima de 35 *ppm*, Se acepta variación sobre la base de +/- 5 *ppm*.
Procesador	600 *MHz* mínimo.
Resolución	600 x 600 *dpi* mínimo.
Memoria	512 *MB RAM* como mínimo. Expandible a 1,5 *GB* o en su defecto una memoria al menos del 200% mayor de la base solicitada.
Disco Duro	Mínimo 80 *GB HDD*.
Interface	Una ranura de tarjeta interna *USB* de al menos 2.0 o superior (Tipo B) *Gigabit Ethernet* (10/100/1000) Puerto frontal *USB* 2.0 o superior (Tipo A).
Escalas de grises	256 niveles.

Alimentador de Papel	Mínimo 50 hojas.
Compatibilidad OS	Compatibilidad 100% con el último Sistema operativo en el Mercado. Sistemas operativos: *Windows* 10.0, *Windows* 8.1, *Windows* 8, *Windows* 7, *Windows XP/Server* 2003/*Vista*/*server Systems* 2008/7; *Mac OS* X 10.2; *Linux*.
Alimentación Eléctrica	120v, 60 *Hz*,12 A.
Otras Funciones	Autenticación de código de usuario para impresión segura, mínimo 50 usuarios, *Scan To Email*, *FTP*, o carpetas varias.
Ahorro de energía	Certificado por *Energy Star*.
Accesorios	Panel de control digital a color configurable y pantalla táctil.
Rendimiento del tóner	Mínimo 10.000 al 5% tóner negro y mínimo 9.000 al 5% cada tóner de color.
Otros	Debe Contar con *Adobe PostScript* 3.

***Software* de administración**	▪ Debe contar con *software* propio de administración, que permita asignar cuotas por usuario, tanto en las funciones de impresión, copia, fax y escaneo a correo electrónico.
	▪ El *software* deberá permitir el acceso o no a las diferentes funciones del equipo de acuerdo al perfil que el usuario tenga definido.
	▪ El *software* deberá permitir identificar el detalle de copias e impresiones tales como: usuario, *dúplex*, cantidad de hojas, color o mono, nombre del documento impreso, así como un informe detallado de transacciones por equipo. Los reportes anteriores deben ser exportados a *Excel* y la información deberá ser almacenada en una base de datos para consultas posteriores.
	▪ El *software* deberá permitir limitar el color por grupo, por usuario o por equipo.
	▪ El *Software* deberá permitir contabilizar el consumo y costos de impresión que cumpla con las especificaciones siguientes:
	  ▪ Contabilización de consumos y costos desde aplicaciones bajo *Windows*.
	  ▪ Definición de cuotas en color y/o monocromático que podrá ser consumido en impresiones o copias.
	▪ Registrar los siguientes datos por cada impresión:
	  ▪ Cuenta de acceso del usuario que realiza la impresión.

	▪ Fecha y hora de la impresión. ▪ Nombre del archivo impreso. ▪ Cantidad de páginas impresas. ▪ Centro de costos al que pertenece el usuario. ▪ Especificar si se trata de una impresión doble cara o simple. ▪ Especificar si la impresión es monocromática o color. ▪ Tamaño del papel. ▪ Identificación de la *PC* de donde se envió la impresión. ▪ Funcionalidad de Retención de impresiones: ▪ Habilitar la retención de los documentos impresos, permitiendo al usuario liberarlos posteriormente mediante autenticación. ▪ Permitir la eliminación del documento desde el equipo multifuncional, antes de que este sea impreso. ▪ Definir el tiempo de vencimiento de los documentos para la eliminación automática de los mismos si el usuario no los libera o elimina desde el equipo multifuncional. ▪ Posibilidad de delegar impresiones para que otro usuario pueda liberarlas. ▪ Permite la liberación de las impresiones en cualquier equipo multifuncional de la institución sin importar la ubicación. ▪ Posibilidad de imprimir el documento y mantenerlo en la cola de impresión para una reimpresión posterior. ▪ Auditoría de las funciones de impresión y copiado en el caso de los multifuncionales. ▪ Deberá permitir generar los siguientes reportes: ▪ Los reportes de consumo y costos de impresión se presentan en forma electrónica en un formato adecuado. El objetivo de estos reportes es permitir el análisis y control del consumo de impresión de las diferentes gerencias hasta los usuarios finales. ▪ Generar Reporte que contenga el consumo mensual, cantidad de páginas impresas en blanco Y negro, cantidad de páginas

	impresas a color por modelo de equipo, bajo la estructura Centro de Costo y usuario. ▪ Generar reporte consolidado y detallado mensual. ▪ Generar reporte de tendencia del consumo de impresión consolidado de forma mensual. ▪ Facilidades para análisis estadísticos del consumo para la emisión de recomendaciones para optimizar el consumo de impresión y su costo. ▪ Debe permitir la creación de cuotas de impresión por usuario para asignar máximos de impresión. ▪ La instalación de *hardware* y *software* e implementación antes mencionado, corre por cuenta del contratista sin ningún costo para la administración.
Lenguaje	De descripción de páginas (*LDP*): al menos *PCL5*, *PCL6*. *PostScript* 3.
Protocolo de Red	*TCP/IP* (*IPv4*, *IPv6*); opcionales *IPX/SPX*, *Apple Talk*, *UDP*.
Capacidad de impresión	De 2000 a 6.000 documentos mensuales y un ciclo de trabajo mensual mínimo de 45.000 impresiones a 75.000 impresiones.
Capacidad de Papel	Una Bandeja principal con capacidad de 250 hojas con posibilidad de adicionar una bandeja más de 500 hojas en un futuro, y una bandeja "*Bypass*" de al menos 50 hojas.
Salida de Primera Hoja BN/Color	Máximo 11 segundos, Se acepta variación sobre la base de +/- 5 segundos.
Tiempo de Calentamiento	Máximo 40 segundos (se aceptan todos los tiempos inferiores a este).
Tamaño de Papel	A6, A5, A4.
Dúplex	Automático
Nivel de Ruido	55 dB Máximo. Se acepta variación sobre la base de + / -, 15 dB.
Características de Copia en el equipo	
Velocidad de Copia	Mínima de 35 *ppm*, Se acepta variación sobre la base de +/- 3 *ppm*.
Salida de Primera Copia	Máximo 11 segundos, Se acepta variación sobre la base de +/- 5 segundos.
Zoom	Rango de 25 a 400 %.
Resolución	Resolución de 600 x 600 *dpi* en la cama plana y 300 x 600 *dpi* en el alimentador automático de

	documentos (ADF).
Tiempo de calentamiento	Máximo 35 segundos, Se acepta variación sobre la base de +/- 5 segundos.
Características de Fax en el equipo	
Debe permitir al menos	*Internet FAX, Network Fax, PC Fax y estándar Fax*.
Fax Modem	33,6 *Kbps* mínimo.
Resolución mínima FAX	200 x 200 *dpi*.
Memoria de Fax mínima	3.*5MB RAM* o Memoria compartida.
Velocidad de Transmisión	Máximo 3 segundos.
Características de Escaneo en el equipo	
Tipo de escáner	Superficie Plana, alimentador automático de documentos (ADF).
Escaneo doble cara	Rotación automático de documentos (ADF).
Resolución de Digitalización BN/ Color	Resolución de 600 x 600 *dpi* en la cama plana y 300 x 600 *dpi* en el alimentador automático de documentos (ADF).
Tipos de Formatos	*JPG*, *JPEG*, *PDF*, *TIFF*, *XPS*, *FTP*.
Debe permitir Escáner a diferentes sitios	Carpeta, *email*, servidor, *USB*, internet FAX.
Escáner a Color/BN velocidad en 300 *dpi*	Se acepta un mínimo de 25 *ppm*.

11.2.3 Estándar de Multifuncionales a Color Mediano Volumen

Función	Impresora, Fax, Escáner y Copiadora.
Velocidad de Impresión BN/COLOR	Mínima de 35 *ppm*, Se acepta variación sobre la base de +/- 5 *ppm*.
Procesador	700 *MHz* mínimo.
Resolución	600 x 600 *dpi* mínimo.
Memoria	1 *GB RAM* como mínimo. Expandible a 2 *GB* o en su defecto una memoria al menos del 200% mayor de la base solicitada
Disco Duro	Mínimo 80 *GB HDD*.
Interface	Una ranura de tarjeta interna *USB* de al menos 2.0 o superior (Tipo B) *Gigabit Ethernet* (10/100/1000) Puerto frontal *USB* 2.0 o superior (Tipo A).
Escalas de grises	256 niveles.
Alimentador de Papel	Mínimo 50 hojas.
Compatibilidad OS	Compatibilidad 100% con el último Sistema operativo en el Mercado. Sistemas operativos: *Windows* 10.0,

	Windows 8.1, *Windows* 8, *Windows* 7, *Windows XP/Server* 2003/*Vista*/*server Systems* 2008/7; *Mac OS* X 10.2; *Linux*.
Alimentación Eléctrica	120v, 60 *Hz*,12 A.
Otras Funciones	Autenticación de código de usuario para impresión mínimo 50 usuarios, *Scan To Email*, *FTP*, o carpetas varias.
Ahorro de energía	Certificado por *Energy Star*.
Accesorios	Panel de control digital a color configurable y pantalla táctil.
Rendimiento del tóner	Mínimo 12.000 al 5% tóner negro y mínimo 9.500 al 5% cada tóner de color
Otros	Debe Contar con *Adobe PostScript* 3.

***Software* de administración**	▪ Debe contar con *software* propio de administración, que permita asignar cuotas por usuario, tanto en las funciones de impresión, copia, fax y escaneo a correo electrónico.
	▪ El *software* deberá permitir el acceso o no a las diferentes funciones del equipo de acuerdo al perfil que el usuario tenga definido.
	▪ El *software* deberá permitir identificar el detalle de copias e impresiones tales como: usuario, *dúplex*, cantidad de hojas, color o mono, nombre del documento impreso, así como un informe detallado de transacciones por equipo. Los reportes anteriores deben ser exportados a *Excel* y la información deberá ser almacenada en una base de datos para consultas posteriores.
	▪ El *software* deberá permitir limitar el color por grupo, por usuario o por equipo.
	▪ El *Software* deberá permitir contabilizar el consumo y costos de impresión que cumpla con las especificaciones siguientes:
	  ▪ Contabilización de consumos y costos desde aplicaciones bajo *Windows*.
	  ▪ Definición de cuotas en color y/o monocromático que podrá ser consumido en impresiones o copias.
	▪ Registrar los siguientes datos por cada impresión:
	  ▪ Cuenta de acceso del usuario que realiza la impresión.
	  ▪ Fecha y hora de la impresión.
	  ▪ Nombre del archivo impreso.
	  ▪ Cantidad de páginas impresas.
	  ▪ Centro de costos al que pertenece el

	usuario. ▪ Especificar si se trata de una impresión doble cara o simple. ▪ Especificar si la impresión es monocromática o color. ▪ Tamaño del papel. ▪ Identificación de la *PC* de donde se envió la impresión. ▪ Funcionalidad de Retención de impresiones: ▪ Habilitar la retención de los documentos impresos, permitiendo al usuario liberarlos posteriormente mediante autenticación. ▪ Permitir la eliminación del documento desde el equipo multifuncional, antes de que este sea impreso. ▪ Definir el tiempo de vencimiento de los documentos para la eliminación automática de los mismos si el usuario no los libera o elimina desde el equipo multifuncional. ▪ Posibilidad de delegar impresiones para que otro usuario pueda liberarlas. ▪ Permite la liberación de las impresiones en cualquier equipo multifuncional de la institución sin importar la ubicación. ▪ Posibilidad de imprimir el documento y mantenerlo en la cola de impresión para una reimpresión posterior. ▪ Auditoría de las funciones de impresión y copiado en el caso de los multifuncionales. ▪ Deberá permitir generar los siguientes reportes: ▪ Los reportes de consumo y costos de impresión se presentan en forma electrónica en un formato adecuado. El objetivo de estos reportes es permitir el análisis y control del consumo de impresión de las diferentes gerencias hasta los usuarios finales. ▪ Generar Reporte que contenga el consumo mensual, cantidad de páginas impresas en blanco y negro, cantidad de páginas impresas a color por modelo de equipo, bajo la estructura Centro de Costo y usuario. ▪ Generar reporte consolidado y detallado mensual. ▪ Generar reporte de tendencia del consumo

	de impresión consolidado de forma mensual. ▪ Facilidades para análisis estadísticos del consumo para la emisión de recomendaciones para Optimizar el consumo de impresión y su costo. ▪ Debe permitir la creación de cuotas de impresión por usuario para asignar máximos de impresión. ▪ La instalación de *hardware* y *software* e implementación antes mencionado, corre por cuenta del contratista sin ningún costo para la administración.
Lenguaje	De descripción de páginas (*LDP*): al menos *PCL5*, *PCL6*. *PostScript* 3.
Protocolo de Red	*TCP/IP* (*IPv4*, *IPv6*); opcionales *IPX/SPX*, *Apple Talk*, *UDP*.
Capacidad de impresión	De 4000 a 10,000 documentos mensuales y un ciclo de trabajo mensual máximo de 95.000 impresiones.
Capacidad de Papel	Una Bandeja principal con capacidad de 500 hojas con posibilidad de adicionar una bandeja más de 500 hojas en un futuro, y una bandeja "Bypass" de al menos 50 hojas.
Salida de Primera Hoja BN/Color	Máximo 8 segundos, Se acepta variación sobre la base de +/- 3 segundos.
Tiempo de Calentamiento	Máximo 45 segundos (se aceptan todos los tiempos inferiores a este).
Tamaño de Papel	A6, A5, A4.
Dúplex	Automático
Nivel de Ruido	55 *dB* Máximo. Se acepta variación sobre la base de + / -, 15 *dB*.
Características de Copia en el equipo	
Velocidad de Copia	Mínima de 33 *ppm*, Se acepta variación sobre la base de +/- 3 *ppm*.
Salida de Primera Copia	Máximo 11 segundos, Se acepta variación sobre la base de +/- 5 segundos.
Zoom	Rango de 25 a 400 %.
Resolución	Resolución de 600 x 600 *dpi* en la cama plana y 300 x 600 *dpi* en el alimentador automático de documentos (ADF)
Tiempo de calentamiento	Máximo 35 segundos, Se acepta variación sobre la base de +/- 5 segundos.
Características de Fax en el equipo	
Debe permitir al menos	Internet FAX, *Network F*ax, *PC Fax* y estándar Fax.
Fax Modem	33,6 *Kbps* mínimo.
Resolución mínima FAX	200 x 200 *dpi*.

Memoria de Fax mínima	4 *MB RAM* o Memoria compartida
Velocidad de Transmisión	Máximo 3 segundos.
Características de Escaneo en el equipo	
Tipo de escáner	Superficie Plana, alimentador automático de documentos (ADF).
Escaneo doble cara	Rotación automático de documentos (ADF)
Resolución de Digitalización BN/Color	Resolución de 600 x 600 dpi en la cama plana y 300 x 600 dpi en el alimentador automático de documentos (ADF)
Tipos de Formatos	*JPG, JPEG, PDF, TIFF, XPS, FTP.*
Debe permitir Escáner a diferentes sitios	Carpeta, *email*, servidor, *USB*, internet FAX.
Escáner a Color/BN velocidad en 300 *dpi*	Se acepta un mínimo de 25 ppm.

11.2.4 Estándar de Multifuncionales Monocromática a Bajo Volumen

Función	Impresora, Fax, Escáner y Copiadora.
Velocidad de Impresión	Mínimo de 35 *ppm*. Se acepta variación sobre la base de +/- 5 *ppm*.
Procesador	600 *MHz* mínimo.
Resolución	600 x 600 *dpi* mínimo.
Memoria	512 *MB RAM* como mínimo. Expandible a 1,5 *GB* o en su defecto una memoria al menos del 200% mayor de la base solicitada.
Disco Duro	Mínimo 80 *GB HDD*.
Interface	Una ranura de tarjeta interna *USB* de al menos 2.0 o superior (Tipo B) *Gigabit Ethernet* (10/100/1000) Puerto frontal *USB* 2.0 o superior (Tipo A).
Escalas de grises	256 niveles.
Alimentador de Papel	Mínimo 50 hojas.
Compatibilidad OS	Compatibilidad 100% con el último Sistema operativo en el Mercado. Sistemas operativos: *Windows* 10.0, *Windows* 8.1, *Windows* 8, *Windows* 7, *Windows* XP/Server 2003/Vista/*server Systems* 2008/7; *Mac* OS X 10.2; *Linux*.
Alimentación Eléctrica	120v, 60 *Hz*,12 A.
Otras Funciones	Autenticación de código de usuario para impresión segura, mínimo 50 usuarios *Scan To Email*, *FTP*, o carpetas varias.
Ahorro de energía	Certificado por *Energy Star*.

Accesorios	Panel de control digital a color configurable y pantalla táctil.
Rendimiento del tóner	Mínimo 10.000 AL 5%.
Otros	Debe contar con *Adobe PostScript* 3.

***Software* de administración**	▪ Debe contar con *software* propio de administración, que permita asignar cuotas por usuario, tanto en las funciones de impresión, copia, fax y escaneo a correo electrónico.
	▪ El *software* deberá permitir el acceso o no a las diferentes funciones del equipo de acuerdo al perfil que el usuario tenga definido.
	▪ El *software* deberá permitir identificar el detalle de copias e impresiones tales como: usuario, *dúplex*, cantidad de hojas, color o mono, nombre del documento impreso, así como un informe detallado de transacciones por equipo. Los reportes anteriores deben ser exportados a *Excel* y la información deberá ser almacenada en una base de datos para consultas posteriores.
	▪ El *software* deberá permitir limitar el color por grupo, por usuario o por equipo.
	▪ El *Software* deberá permitir contabilizar el consumo y costos de impresión que cumpla con las especificaciones siguientes:
	  ▪ Contabilización de consumos y costos desde aplicaciones bajo *Windows*.
	  ▪ Definición de cuotas en color y/o monocromático que podrá ser consumido en impresiones o copias.
	▪ Registrar los siguientes datos por cada impresión:
	  ▪ Cuenta de acceso del usuario que realiza la impresión
	  ▪ Fecha y hora de la impresión.
	  ▪ Nombre del archivo impreso.
	  ▪ Cantidad de páginas impresas.
	  ▪ Centro de costos al que pertenece el usuario.
	  ▪ Especificar si se trata de una impresión doble cara o simple.
	  ▪ Especificar si la impresión es monocromática o color.
	  ▪ Tamaño del papel.
	  ▪ Identificación de la *PC* de donde se envió la impresión.

	▪ Funcionalidad de Retención de impresiones:
	  ▪ Habilitar la retención de los documentos impresos, permitiendo al usuario liberarlos posteriormente mediante autenticación.
	  ▪ Permitir la eliminación del documento desde el equipo multifuncional, antes de que este sea impreso.
	  ▪ Definir el tiempo de vencimiento de los documentos para la eliminación automática de los mismos si el usuario no los libera o elimina desde el equipo multifuncional.
	  ▪ Posibilidad de delegar impresiones para que otro usuario pueda liberarlas.
	  ▪ Permite la liberación de las impresiones en cualquier equipo multifuncional de la institución sin importar la ubicación.
	  ▪ Posibilidad de imprimir el documento y mantenerlo en la cola de impresión para una reimpresión posterior.
	  ▪ Auditoría de las funciones de impresión y copiado en el caso de los multifuncionales.
	▪ Deberá permitir generar los siguientes reportes:
	  ▪ Los reportes de consumo y costos de impresión se presentan en forma electrónica en un formato adecuado. El objetivo de estos reportes es permitir el análisis y control del consumo de impresión de las diferentes gerencias hasta los usuarios finales.
	  ▪ Generar reporte que contenga el consumo mensual, cantidad de páginas impresas en blanco y negro, cantidad de páginas impresas a color por modelo de equipo, bajo la estructura Centro de Costo y usuario.
	  ▪ Generar reporte consolidado y detallado mensual.
	  ▪ Generar reporte de tendencia del consumo de impresión consolidado de forma mensual.
	▪ Facilidades para análisis estadísticos del consumo para la emisión de recomendaciones para optimizar el consumo de impresión y su costo.
	▪ Debe permitir la creación de cuotas de impresión por usuario para asignar máximos de impresión.
	▪ La instalación e implementación del *software* antes mencionado, corre por cuenta del contratista sin

	ningún costo para la administración.
Lenguaje	De descripción de páginas (*LDP*): al menos *PCL5*, *PCL6*. *PostScript* 3.
Protocolo de Red	*TCP/IP* (*IPv4*, *IPv6*); opcionales *IPX/SPX*, *Apple Talk*, *UDP*.
Capacidad de impresión	De 2000 a 6.000 documentos mensuales y un ciclo de trabajo mensual mínimo de 45.000 impresiones a 75.000 impresiones.
Capacidad de Papel	Una Bandeja principal con capacidad de 250 hojas con posibilidad de adicionar una bandeja más de 500 hojas en un futuro, y una bandeja "*Bypass*" de al menos 50 hojas.
Salida de Primera Hoja	Máximo 9 segundos, una variación de +/-, 3 segundos.
Tiempo de Calentamiento	Máximo 30 segundos (se aceptan todos los tiempos inferiores a este).
Tamaño de Papel	A6, A5, A4, papel normal, membrete, bond, reciclado, rugoso, satinado, transparencias, etiquetas, sobre, cartulina.
Dúplex	Automático.
Nivel de Ruido	55 *dB*. Se acepta un rango de +/-, 15 *dB*.
Características de Copia en el equipo	
Velocidad de Copia	Mínima de 35 *ppm*, Se acepta variación sobre la base de +/- 3 *ppm*.
Salida de Primera Copia	Máximo 11 segundos, Se acepta variación sobre la base de +/- 3 segundos.
Zoom	Rango de 25 a 400 %.
Resolución	Resolución de 600 x 600 dpi en la cama plana y 300 x 600 dpi en el alimentador automático de documentos (ADF).
Tiempo de calentamiento	Máximo 35 segundos, Se acepta variación sobre la base de +/- 5 segundos.
Características de Fax en el quipo	
Debe permitir al menos	Internet FAX, *Network Fax*, *PC Fax* y *estándar Fax.*
Fax Modem	33,6 *Kbps* mínimo.
Resolución mínima FAX	200 x 200 *dpi*.
Memoria de Fax mínima	3.*5MB RAM* o Memoria compartida.
Velocidad de Transmisión	Máximo 3 segundos.
Características de Escaneo en el equipo	
Tipo de escáner	Superficie Plana, alimentador automático de documentos (ADF).
Escaneo doble cara	Rotación automático de documentos (ADF).
Resolución de Digitalización	Resolución de 600 x 600 *dpi* en la cama plana y 300 x

	600 *dpi* en el alimentador automático de documentos (ADF).
Tipos de Formatos	*JPG, JPEG, PDF, TIFF, XPS, FTP*.
Debe permitir Escáner a diferentes sitios	Carpeta, *email*, servidor, *USB*, internet FAX.
Escáner a Color/BN velocidad en 300 *dpi*	Se acepta un mínimo de 25 *ppm*.

11.2.5 Estándar de Multifuncionales Monocromática a Mediano Volumen

Función	Impresora, Fax, Escáner y Copiadora.
Velocidad de Impresión	Mínimo de 45 *ppm*. Se acepta variación sobre la base de +/- 5 *ppm*.
Procesador	700 *MHz* mínimo.
Resolución	1200 x 1200 *dpi* mínimo.
Memoria	1 *GB RAM* mínimo. Expandible a 2 *GB* o en su defecto una memoria al menos del 200% mayor de la base solicitada.
Disco Duro	Mínimo 80 *GB HDD*.
Interface	Una ranura de tarjeta interna *USB* de al menos 2.0 o superior (Tipo B) *Gigabit Ethernet* (10/100/1000) Puerto frontal *USB* 2.0 o superior (Tipo A).
Escalas de grises	256 niveles.
Alimentador de Papel	Mínimo 50 hojas.
Compatibilidad OS	Compatibilidad 100% con el último Sistema operativo en el Mercado. Sistemas operativos: *Windows* 10.0, *Windows* 8.1, *Windows* 8, *Windows* 7, *Windows XP*/*Server* 2003/Vista/*server Systems* 2008/7; *Mac* OS X 10.2; *Linux*.
Alimentación Eléctrica	120v, 60 *Hz*,12 A.
Otras Funciones	Autenticación de código de usuario para impresión segura, mínimo 50 usuarios, *Scan To Email*, *FTP*, o carpetas varias.
Ahorro de energía	Certificado por *Energy Star*.
Accesorios	Panel de control digital a color configurable y pantalla táctil.
Rendimiento del tóner	Mínimo 12.500 al 5%.
Otros	Debe contar con *Adobe PostScript* 3.
***Software* de administración**	▪ Debe contar con *software* propio de administración, que permita asignar cuotas por usuario, tanto en las funciones de impresión, copia, fax y escaneo a correo electrónico.

	▪ El *software* deberá permitir el acceso o no a las diferentes funciones del equipo de acuerdo al perfil que el usuario tenga definido.
	▪ El *software* deberá permitir identificar el detalle de copias e impresiones tales como: usuario, *dúplex*, cantidad de hojas, color o mono, nombre del documento impreso, así como un informe detallado de transacciones por equipo. Los reportes anteriores deben ser exportados a *Excel* y la información deberá ser almacenada en una base de datos para consultas posteriores.
	▪ El *software* deberá permitir limitar el color por grupo, por usuario o por equipo.
	▪ El *Software* deberá permitir contabilizar el consumo y costos de impresión que cumpla con las especificaciones siguientes:
	  ▪ Contabilización de consumos y costos desde aplicaciones bajo *Windows*.
	  ▪ Definición de cuotas en color y/o monocromático que podrá ser consumido en impresiones o copias.
	▪ Registrar los siguientes datos por cada impresión:
	  ▪ Cuenta de acceso del usuario que realiza la impresión
	  ▪ Fecha y hora de la impresión.
	  ▪ Nombre del archivo impreso.
	  ▪ Cantidad de páginas impresas.
	  ▪ Centro de costos al que pertenece el usuario.
	  ▪ Especificar si se trata de una impresión doble cara o simple.
	  ▪ Especificar si la impresión es monocromática o color.
	  ▪ Tamaño del papel.
	  ▪ Identificación de la *PC* de donde se envió la impresión.
	▪ Funcionalidad de Retención de impresiones:
	  ▪ Habilitar la retención de los documentos impresos, permitiendo al usuario liberarlos posteriormente mediante autenticación.
	  ▪ Permitir la eliminación del documento desde el equipo multifuncional, antes de que este sea impreso.
	  ▪ Definir el tiempo de vencimiento de los

	documentos para la eliminación automática de los mismos si el usuario no los libera o elimina desde el equipo multifuncional. ▪ Posibilidad de delegar impresiones para que otro usuario pueda liberarlas. ▪ Permite la liberación de las impresiones en cualquier equipo multifuncional de la institución sin importar la ubicación. ▪ Posibilidad de imprimir el documento y mantenerlo en la cola de impresión para una reimpresión posterior. ▪ Auditoría de las funciones de impresión y copiado en el caso de los multifuncionales. ▪ Deberá permitir generar los siguientes reportes: ▪ Los reportes de consumo y costos de impresión se presentan en forma electrónica en un formato adecuado. El objetivo de estos reportes es permitir el análisis y control del consumo de impresión de las diferentes gerencias hasta los usuarios finales. ▪ Generar reporte que contenga el consumo mensual, cantidad de páginas impresas en blanco y negro, cantidad de páginas impresas a color por modelo de equipo, bajo la estructura Centro de Costo y usuario. ▪ Generar reporte consolidado y detallado mensual. ▪ Generar reporte de tendencia del consumo de impresión consolidado de forma mensual. ▪ Facilidades para análisis estadísticos del consumo para la emisión de recomendaciones para optimizar el consumo de impresión y su costo. ▪ Debe permitir la creación de cuotas de impresión por usuario para asignar máximos de impresión. ▪ La instalación de *hardware* y *software* e implementación antes mencionado, corre por cuenta del contratista sin ningún costo para la administración.
Lenguaje	De descripción de páginas (*LDP*): al menos *PCL5*, *PCL6*. *PostScript* 3.
Protocolo de Red	*TCP/IP* (*IPv4*, *IPv6*); opcionales *IPX/SPX, Apple Talk, UDP*.
Capacidad de impresión	De 4000 a 15000 documentos mensuales y un ciclo de trabajo mensual mínimo de 150.000 impresiones.
Capacidad de Papel	Una Bandeja principal con capacidad de 500 hojas

	con posibilidad de adicionar una bandeja más de 500 hojas en un futuro, y una bandeja "*Bypass*" de al menos 100 hojas.
Salida de Primera Hoja	Máximo 8 segundos, una variación de +/-, 3 segundos.
Tiempo de Calentamiento	Máximo 35 segundos (se aceptan todos los tiempos inferiores a este).
Tamaño de Papel	A6, A5, A4.
Dúplex	Automático.
Nivel de Ruido	55 *dB*. Se acepta un rango de +/-, 15 *dB*.
Características de Copia en el equipo	
Velocidad de Copia	Mínimo de 45 *ppm*. Se acepta variación sobre la base de +/- 5 *ppm*.
Salida de Primera Copia	Máximo 10 segundos, Se acepta variación sobre la base de +/- 3 segundos.
Zoom	Rango de 25 a 400 %.
Resolución	Resolución de 600 x 600 *dpi* en la cama plana y 300 x 600 *dpi* en el alimentador automático de documentos (ADF)
Tiempo de calentamiento	Aproximado a 30 segundos. +/- 5 segundos.
Características de Fax en el equipo	
Debe permitir al menos	Internet FAX, *Network Fax, PC Fax y estándar Fax*.
Fax Modem	33,6 *Kbps* mínimo.
Resolución mínima FAX	200 x 200 *dpi*.
Memoria de Fax mínima	3.*5MB RAM* o Memoria compartida.
Velocidad de Transmisión	Máximo 3 segundos.
Características de Escaneo en el quipo	
Tipo de escáner	Superficie Plana, alimentador automático de documentos (ADF).
Escaneo doble cara	Rotación automático de documentos (ADF).
Resolución de Digitalización	Resolución de 600 x 600 *dpi* en la cama plana y 300 x 600 *dpi* en el alimentador automático de documentos (ADF).
Tipos de Formatos	*JPG, JPEG, PDF, TIFF, XPS, FTP*.
Debe permitir Escáner a diferentes sitios	Carpeta, *email*, servidor, *USB*, internet FAX.
Escáner a Color/BN velocidad en 300 *dpi*	Se acepta un mínimo de 25 *ppm*.

11.2.6 Estándar de Multifuncionales Monocromática a Alto Volumen

Función	Impresora, Fax, Escáner y Copiadora.
Velocidad de Impresión	Mínimo de 55 *ppm*. Se acepta variación sobre la base de +/- 5 *ppm*.
Procesador	800 *MHz* mínimo.
Resolución	1200 x 1200 *dpi* mínimo.
Memoria	1 *GB RAM* mínimo. Expandible a 2 *GB* o en su defecto una memoria al menos del 200% mayor de la base solicitada.
Disco Duro	Mínimo 80 *GB HDD*.
Interface	Una ranura de tarjeta interna *USB* de al menos 2.0 o superior (Tipo B) *Gigabit Ethernet* (10/100/1000) Puerto frontal *USB* 2.0 o superior (Tipo A).
Escalas de grises	256 niveles.
Alimentador de Papel	Mínimo 50 hojas.
Compatibilidad OS	Compatibilidad 100% con el último Sistema operativo en el Mercado. Sistemas operativos: *Windows* 10.0, *Windows* 8.1, *Windows* 8, *Windows* 7, *Windows* XP/*Server* 2003/Vista/*server Systems* 2008/7; *Mac* OS X 10.2; *Linux*.
Alimentación Eléctrica	120v, 60 *Hz*,12 A.
Ahorro de energía	Certificado por *Energy Star*.
Accesorios	Panel de control digital a color configurable y pantalla táctil.
Rendimiento del tóner	Mínimo 20.000 al 5%.
Otros	Debe Contar con *Adobe PostScript* 3.
***Software* de administración**	▪ Debe contar con *software* propio de administración, que permita asignar cuotas por usuario, tanto en las funciones de impresión, copia, fax y escaneo a correo electrónico. ▪ El *software* deberá permitir el acceso o no a las diferentes funciones del equipo de acuerdo al perfil que el usuario tenga definido. ▪ El *software* deberá permitir identificar el detalle de copias e impresiones tales como: usuario, *dúplex*, cantidad de hojas, color o mono, nombre del documento impreso, así como un informe detallado de transacciones por equipo. Los reportes anteriores deben ser exportados a *Excel* y la información deberá ser almacenada en una base de datos para consultas posteriores. ▪ El *software* deberá permitir limitar el color por grupo, por usuario o por equipo.

	▪ El *Software* deberá permitir contabilizar el consumo y costos de impresión que cumpla con las especificaciones siguientes:
	  ▪ Contabilización de consumos y costos desde aplicaciones bajo Windows.
	  ▪ Definición de cuotas en color y/o monocromático que podrá ser consumido en impresiones o copias.
	▪ Registrar los siguientes datos por cada impresión:
	  ▪ Cuenta de acceso del usuario que realiza la impresión
	  ▪ Fecha y hora de la impresión.
	  ▪ Nombre del archivo impreso.
	  ▪ Cantidad de páginas impresas.
	  ▪ Centro de costos al que pertenece el usuario.
	  ▪ Especificar si se trata de una impresión doble cara o simple.
	  ▪ Especificar si la impresión es monocromática o color.
	  ▪ Tamaño del papel.
	  ▪ Identificación de la *PC* de donde se envió la impresión.
	▪ Funcionalidad de Retención de impresiones:
	  ▪ Habilitar la retención de los documentos impresos, permitiendo al usuario liberarlos posteriormente mediante autenticación.
	  ▪ Permitir la eliminación del documento desde el equipo multifuncional, antes de que este sea impreso.
	  ▪ Definir el tiempo de vencimiento de los documentos para la eliminación automática de los mismos si el usuario no los libera o elimina desde el equipo multifuncional.
	  ▪ Posibilidad de delegar impresiones para que otro usuario pueda liberarlas.
	  ▪ Permite la liberación de las impresiones en cualquier equipo multifuncional de la institución sin importar la ubicación.
	  ▪ Posibilidad de imprimir el documento y mantenerlo en la cola de impresión para una reimpresión posterior.
	  ▪ Auditoría de las funciones de impresión y copiado en el caso de los multifuncionales.

	▪ Deberá permitir generar los siguientes reportes: ▪ Los reportes de consumo y costos de impresión se presentan en forma electrónica en un formato adecuado. El objetivo de estos reportes es permitir el análisis y control del consumo de impresión de las diferentes gerencias hasta los usuarios finales. ▪ Generar reporte que contenga el consumo mensual, cantidad de páginas impresas en blanco y negro, cantidad de páginas impresas a color por modelo de equipo, bajo la estructura Centro de Costo y usuario. ▪ Generar reporte consolidado y detallado mensual. ▪ Generar reporte de tendencia del consumo de impresión consolidado de forma mensual. ▪ Facilidades para análisis estadísticos del consumo para la emisión de recomendaciones para optimizar el consumo de impresión y su costo. ▪ Debe permitir la creación de cuotas de impresión por usuario para asignar máximos de impresión. ▪ La instalación de *hardware* y *software* e implementación antes mencionado, corre por cuenta del contratista sin ningún costo para la administración.
Lenguaje	De descripción de páginas (*LDP*): al menos *PCL5*, *PCL6*. *PostScript* 3.
Protocolo de Red	*TCP/IP* (*IPv4*, *IPv6*); opcionales *IPX/SPX*, *Apple Talk*, UDP.
Capacidad de impresión	De 15.000 a 30.000 documentos mensuales y un ciclo de trabajo mensual máximo de 200.000 impresiones.
Capacidad de Papel	Una Bandeja principal con capacidad de 500 hojas con posibilidad de adicionar una bandeja más de 500 hojas en un futuro, y una bandeja "*Bypass*" de al menos 100 hojas.
Salida de Primera Hoja	Máximo 5.5 segundos, una variación de +/-, 4 segundos.
Tiempo de Calentamiento	Máximo 30 segundos (se aceptan todos los tiempos inferiores a este).
Tamaño de Papel	A6, A5, A4.
Dúplex	Automático.
Nivel de Ruido	55 *dB*. Se acepta un rango de +/-, 15 *dB*.
Características de Copia en el equipo	
Velocidad de Copia	Mínima de 55 *ppm*, Se acepta variación sobre la base de +/- 5 *ppm*.

Salida de Primera Copia	Máximo 6 segundos, Se acepta variación sobre la base de +/- 4 segundos.
Zoom	Rango de 25 a 400 %.
Resolución	Resolución de 600 x 600 *dpi* en la cama plana y 300 x 600 *dpi* en el alimentador automático de documentos (ADF).
El tiempo de calentamiento	Aproximado a 25 segundos. +/- 5 segundos.
Características de Fax en el equipo	
Debe permitir al menos	Internet FAX, *Network Fax, PC Fax y estándar Fax*.
Fax Modem	33,6 *Kbps* mínimo.
Resolución mínima FAX	200 x 200 *dpi*.
Memoria de Fax mínima	4MB *RAM* o Memoria compartida.
Velocidad de Transmisión	Máximo 3 segundos.
Características de Escaneo en el equipo	
Tipo de escáner	Superficie Plana, alimentador automático de documentos (ADF).
Escaneo doble cara	Rotación automático de documentos (ADF).
Resolución de Digitalización	Resolución de 600 x 600 *dpi* en la cama plana y 300 x 600 *dpi* en el alimentador automático de documentos (ADF).
Tipos de Formatos	*JPG, JPEG, PDF, TIFF, XPS, FTP.*
Debe permitir Escáner a diferentes sitios	Carpeta, *email*, servidor, *USB*, internet FAX.
Escáner a Color/BN velocidad en 300 *dpi*	Se acepta un mínimo de 33 *ppm*.

11.3 Dimensionamiento de las características técnicas de la *UPS*

11.3.1 Estándar de UPS

TIPO DE EQUIPO	Producto reconocido en el mercado internacional por alto rendimiento, normas de calidad y servicio. No se aceptará equipo usado o reconstruido, deberá entregarse documentación probatoria con números de serie del fabricante del equipo para constatar dicha información.
CAPACIDAD DE POTENCIA	1000 *VA* 900 *W* mínimo, deberá ser de operación plena en línea (doble conversión *true on-line*) totalmente automática con el inversor alimentando la carga.
TOMAS DE SALIDA	Debe de contar con 8 tomas de salida 5-*15R* protegidos por el *UPS*.

VOLTAJE NOMINAL DE E/S	120 *V* / 50 *Hz*-60 *Hz*.
RANGO DE VOLTAJE	60 *V* a 140 *V*, sin que la *UPS* pase a modo de *bypass* o a funcionamiento en baterías.
INTERFACE	Capacidad para incorporar tarjeta de red *SNMP*.
PANEL DE INDICACIÓN	Debe de contar con pantalla digital *LCD* que indique las funciones de operación al usuario de interpretación fácil. Nivel de carga, nivel de carga de la batería, modo de operación (*on-line, bypass*, batería) e indicador de falla.
ALARMA PROTECCIÓN	Audibles en caso de falla.
TIEMPO DE RESPALDO	5 minutos a capacidad máxima de la *UPS*, esto cuando opere con baterías, entrando éstas a funcionar en el momento de una interrupción de la alimentación eléctrica, supliendo un voltaje constante, libre de transientes, inestabilidades en frecuencia y otros disturbios eléctricos. No deberá existir tiempo de transferencia cuando entre en modo batería (doble conversión *true on-line*). No se admiten bancos de baterías externos para garantizar la carga solicitada en este punto.
TIPO DE BATERÍA	Selladas y de libre mantenimiento, con tiempo de recarga de 4 horas al 90%.
SOBRECARGA	Protección 400 *joules* mínimo.
MEDIDAS	380 mm de altura x 438 mm de profundidad y 88 mm de ancho. Se aceptan una variación de +/- 50 mm en las dimensiones y medidas.
CAPACIDAD	La *UPS* debe de venir con capacidad de ser instalada en el piso; proporcionando para ello las respectivas bases que brindaran una estabilidad apropiada.
CARACTERÍSTICAS IMPORTANTES	El equipo deberá contar con su rectificador, inversor, cargador de baterías, baterías, interruptor de transferencia automático para la línea de desvío (*bypass*) en caso de sobrecarga o falla del equipo, alarmas y demás implementos para su correcto funcionamiento.
FACTOR DE POTENCIA	El factor de potencia a la entrada deberá ser mayor a 0.99.
RANGO DE FRECUENCIA	El rango de frecuencia de entrada deberá estar dentro del rango de 40 a 70 *Hz* y la frecuencia de salida de 60 *Hz*.
CHASIS	El chasis y cobertor de la *UPS* ofrecida debe ser metálico.
DISPOSITIVOS DE	Deberá contar con dispositivos de protección para la

PROTECCIÓN	entrada, la salida y las baterías, los cuales deberán describirse.
TOLERANCIA DE TEMPERATURA	La temperatura de operación de la unidad de potencia interrumpida deberá estar al menos entre 10 y 40 grados centígrados, y la humedad relativa de operación entre 20% y 90% sin condensación.
CERTIFICACIONES SOLICITADAS	▪ ***RoHS*** - Es una sigla que proviene del inglés y significa: "*Restriction of Hazardous Substances*". El *RoHS* es una directiva que adopto la Comunidad Europea en febrero de 2003 (2002/95/CE) y está orientada a reducir el uso de algunas sustancias peligrosas en aparatos eléctricos y electrónicos. ▪ ***Energy star*** - Es un programa de la Agencia de Protección Ambiental de los Estados Unidos creado en 1992 para promover los productos eléctricos con consumo eficiente de electricidad, reduciendo de esta forma la emisión de gas de efecto invernadero por parte de las centrales eléctricas. ▪ ***Epeat*** - Significa "Herramienta de Evaluación Ambiental de Productos Electrónicos" y es un sistema de clasificación ambiental importante para los productos electrónicos, diseñada para ayudar a los consumidores a evaluar, seleccionar y comparar productos ambientalmente preferibles.

11.4 Dimensionamiento de las características técnicas de Servidores

Las siguientes definiciones deberán ser contempladas al dimensionar las características necesarias para la adquisición de un servidor:

a) **Procesos por soportar:** Deben definirse claramente los requerimientos del servicio o servicios a soportar, la estimación de transacciones en un intervalo de tiempo determinado así como la de conexiones concurrentes, el entorno de operación y la criticidad de los procesos que se ejecutarán en el equipo. Para lograr lo indicado anteriormente, debe analizarse integralmente por los sectores profesionales involucrados, haciendo uso de los artefactos de investigación que permitan recopilar la información básica.

b) **Licenciamiento:** Tipo de *software* base (sistema operativo) y *software* de producción (aplicaciones específicas), analizando los requerimientos de *hardware* recomendados por estas aplicaciones para su correcto desempeño.

c) **Redundancia:** Determinar las características de alta disponibilidad del equipo y analizar que componentes de *hardware* podrían requerir duplicidad para configuraciones que permitan una mejor tolerancia a fallos; en dónde en caso de que un componente falle, otro igual asumirá su función hasta que el original sea reparado o reemplazado.

d) **Escalabilidad:** Contemplar la capacidad de escalabilidad del equipo, para poder realizar actualizaciones de su *hardware*, agregar nuevo *hardware* o establecer configuraciones con otros equipos.

e) **Especificaciones técnicas mínimas que considerar:** Una vez determinada la orientación técnica del equipo, deberán dimensionarse las características de sus componentes primarios, esto en función de las necesidades de los servicios y/o procesos a soportar, considerando al menos los siguientes aspectos:

- **Procesador:** Tipo y velocidad de procesamiento en función del licenciamiento y sus características, además de la estimación de la carga de transacciones promedio.
- **Memoria:** Tipo, velocidad y cantidad de memoria *RAM* en función del licenciamiento a soportar y las características del uso promedio estimadas para el equipo.
- **Almacenamiento:** Velocidad y capacidad de los dispositivos de almacenamiento en función del licenciamiento y/o procesos a soportar por el equipo una vez en operación, considerando estándares para alta disponibilidad y tolerancia a errores/fallas.
- **Unidades de respaldo:** Tamaño, velocidad y capacidad de la unidad en relación al nivel de criticidad de la información y/o procesos soportados por el servidor.
- **Red:** Determinar la velocidad de conexión a la red en *MB* (10/100/1000 ó superiores) en función del entorno de operación, selección de los tipos de tarjetas, *Ethernet* o *Wireless* (determinación del estándar a utilizar, G, N u otro), conexiones de alta capacidad con unidades externas de almacenamiento en función del entorno, disponibilidad y requerimientos.
- **Estructura del equipo:** Selección de las características específicas del diseño como, equipo de Torre, Gabinete, o *Blade*, de acuerdo al análisis de los requerimientos de operación de los servicios a soportar por el equipo, así como el entorno de operación y la disponibilidad técnica.
- **Periféricos:** Características y dimensiones de dispositivos como *Mouse*, Teclado, Monitor, lectores de *DVD*, puertos *USB*, entre otros.

- **Características especiales:** Se deberá contemplar cualquier otro requerimiento especial que apoye el soporte de los procesos y/o servicios para los cuales se requiere adquirir el equipo.
- **Características ecológicas:** Deberá considerarse siempre la eficiencia técnica en pro del medio ambiente, para que los equipos adquiridos siempre cuenten con estándares de sostenibilidad ambiental.

11.4.1 Estándar de servidor tipo Blade

Procesador	El servidor *blade* debe tener al menos 2 procesadores *Intel Xeon* E5-2650v3 (2.*3GHz*/10-core/*25MB*/105W) *Processor Kit.*
Memoria *RAM*	El servidor *Blade* debe contar con al menos *256GB DDR4 SmartMemory 2133MHz*.
Software	Una licencia de *Microsoft Windows Server* 2019 *Datacenter Edition - License* - 2 *processors* - *OEM* - *ROK* - *DVD* - *BIOS-locked* (*Hewlett-Packard*). Dos licencias de *VMw vSph Ent* 1P 4yr *Channel E-LTU.*
Almacenamiento	El servidor *blade* debe tener 2 (dos) discos duros *300GB* 6G *SAS* 10K 2.5in *SC ENT HDD* removibles en caliente configurados en *RAID*-1 por *hardware*.
Adaptadores de red *Gigabit Ethernet*	El servidor *Blade* deberá contar en su configuración base al menos con dos (2) tarjetas de red de dos (2) adaptadores de 10Gb.
Conectividad *SAN*	Un adaptador *HP QMH*2672 *16Gb FC HBA* para conexión a *3PAR* por fibra.
Otras características	El equipo deberá ser compatible y funcional al 100% con el *enclousure* C7000 de *HPe* y con el *Enclousure Sinergy*.

11.5 Dimensionamiento de las características técnicas de infraestructura y equipamiento de telecomunicaciones

11.5.1 Equipamiento

Los siguientes aspectos deberán ser contemplados al dimensionar las características necesarias para la adquisición de equipos para la red de datos institucional.

a) **Servicios de red a soportar:** Deben definirse claramente los requerimientos de los servicios a soportar, en función de los anchos de banda requeridos, características de control y administración del tráfico,

seguridad, eficiencia en administración y confiabilidad, integridad de la plataforma, entre otros.

b) **Determinación del tipo de equipo:** De acuerdo con los requerimientos y considerando el entorno de operación y sus características de compatibilidad, para la selección de dispositivos de red como: enrutadores, *switches*, *firewalls*, *access points*, y otros tipos de *appliances* para la red de datos.

c) **Integridad de la plataforma:** Deberá velarse por mantener la integridad en los componentes y/o equipos por adquirir, en relación con la plataforma existente, que facilite la interacción con un mismo sistema operativo, esquemas de licenciamiento, comandos de administración, compatibilidad técnica, escalabilidad, y respaldo técnico.

d) **Redundancia:** Determinar las características de alta disponibilidad del equipo, analizar que componentes de *hardware* podrían requerir duplicidad para configuraciones que permitan una mejor tolerancia a fallos, en donde en caso de que un componente falle, otro asumirá su función hasta que el original sea reparado o reemplazado.

e) **Escalabilidad:** Contemplar la capacidad de escalabilidad del equipo, para poder realizar actualizaciones de su *hardware*, agregar nuevo *hardware*, actualizaciones de su *software* base o establecer configuraciones con otros equipos.

f) **Especificaciones técnicas mínimas para considerar**: Una vez determinada la orientación técnica del equipo, deberá dimensionarse las características de sus componentes primarios, esto en función de las necesidades de los servicios de red a soportar y considerando al menos los siguientes aspectos:

- **Capacidad de Procesamiento de paquetes:** Tipo y velocidad de procesamiento en función de los servicios de red y sus características, además de la estimación de la carga de transacciones promedio.
- **Memoria:** Tipo, velocidad y cantidad de memoria *RAM* en función del licenciamiento a soportar y las características del uso promedio estimadas para el equipo.
- **Componentes para el soporte de la red:** Determinar la cantidad, tipo y velocidad de los puertos de red requeridos en función del propósito del equipo, servicios a soportar y su orientación técnica.
- **Estructura del equipo:** Selección de las características específicas del diseño como la cantidad de unidades de *rack*, tipo de enfriamiento y conexión eléctrica, así como características modulares, entre otras.

- **Características especiales:** Se deberá contemplar cualquier otro requerimiento especial que apoye el soporte de los procesos y/o servicios para los cuales se requiere adquirir el equipo.
- **Software de operación:** Características del *software* de operación que permitan hacer un uso eficiente del equipo para la satisfacción de los requerimientos.
- **Características ecológicas:** Deberá considerarse siempre la eficiencia técnica en pro del medio ambiente, para que los equipos adquiridos siempre cuenten con estándares de sostenibilidad ambiental.

11.5.2 Estándar para enrutadores (Router) Perfil 1:

Especificaciones técnicas	1. Debe incluir fuente de poder interna capaz de operar en un rango de voltaje de 100 a 240 *VAC*. 2. Debe ser de una unidad de *rack* e incluir los aditamentos necesarios para ser montados en los *racks* o gabinetes actuales. 3. Debe contar con capacidad instalada, de actualizar el sistema operativo por vía de cable consola y a través de cualquiera de los interfaces de red *LAN* o *WAN*. 4. Debe contar con memoria *flash* mínima de 256 *MB* instalada. 5. Debe contar con al menos memoria *RAM* instalada de 1 *GB*, con capacidad de crecimiento hasta 2048 *MB* para soportar futuras funcionalidades. 6. Debe tener capacidad de desempeño de al menos 160 *Megabits* por segundo y 320,000 paquetes por segundo, para paquetes *IPv4* de 64 *bytes*. 7. Debe contener integrados al chasis o de forma modular, al menos cuatro (4) interfaces *Giga-Ethernet* 10/100/*1000Mbps* cada uno. Todas deben tener capacidad de enrutamiento instalada. 8. Debe poseer capacidad instalada de encriptación por *hardware* basada en los estándares *IPSEC 3DES* y *AES* 256. 9. Debe tener capacidad instalada para generar

	múltiples *VPN*. 10. El dispositivo debe soportar mecanismos de autenticación de usuarios para control de acceso basado en puerto, según el estándar *IEEE* 802.1X y a través de un servidor de *RADIUS*. 11. Debe tener capacidad de manejar los siguientes protocolos de enrutamiento para *IPv4*: *RIPv2*, *OSPF*, *IS-IS* y *BGP*, así como los siguientes protocolos de enrutamiento para *IPv6*: *OSPFv3*, *RIPng* y *multiprotocol BGP*. 12. El equipo debe ser capaz de soportar *IPv4* y *IPv6*. 13. Debe tener capacidad de manejar los siguientes protocolos de enrutamiento *multicast* para *IPv4*: *PIM-SM*, *PIM Bidirectional*, *PIM SSM*, así como los siguientes protocolos de enrutamiento *multicast* para *IPv6*: *PIM SM* y *PIM SSM*. 14. Debe tener capacidad de reportar estadísticas de flujos de tráfico a través de *Netflow*, *sflow* o su equivalente en todas sus interfaces. 15. Debe contar con capacidad instalada de realizar *Secure RTP* (*SRTP*). 16. Debe contar con capacidad instalada de realizar compresión de encabezados *RTP* y *TCP*. 17. Los equipos deberán contar con capacidad instalada para soportar los siguientes protocolos de redundancia y alta disponibilidad: *RRPP*, *REP*, *VRRP*, *HSRP* o su equivalente según la marca de equipo. 18. El equipo debe permitir la definición e implementación de Clases de Servicio (*CoS*) y Calidad de Servicio (*QoS*) para el manejo eficiente del tráfico. 19. El equipo deberá ser integrable con el *software* de monitoreo *OPManager* propiedad del Ministerio por lo que debe manejar *SNMP* Versiones 2, 2c y 3. (en caso de requerir las *MIBS* del equipo la empresa deberá brindarlas). 20. Debe contar con capacidad instalada de emplear *SNMP* (versión 3) y *SSHv2* para la gestión.

	21. Debe contar con capacidad instalada de administración vía múltiples usuarios y múltiples niveles de privilegios (incluyendo modo de sólo lectura). 22. Debe ser de una unidad de *rack* e incluir los aditamentos necesarios para ser montados en los gabinetes existentes en cada sitio. 23. Debe soportar al menos 5 sesiones simultáneas para gestión por línea de comando. Estas sesiones pueden ser local mediante un puerto de consola o remotas mediante sesiones *Telnet* seguras (*SSH* v2). 24. El proveedor deberá entregar los equipos con todo el licenciamiento requerido para satisfacer los requerimientos planteados por el MEP, este licenciamiento deberá ser en modalidad *Enterprise* o su equivalente, y deberá detallarlo en su oferta. 25. Debe operar en un rango de temperatura ambiente de 0C a 40C un rango de humedad relativa entre 10% y 85%. 26. El equipo debe contar con al menos los siguientes estándares de la *IEEE*. ▪ *IEEE* 802.1Q ▪ *IEEE* 802.1p.

11.5.3 Estándar para enrutadores (Router) Perfil 2

Especificaciones técnicas	1. El equipo debe permitir la definición e implementación de Clases de Servicio (*CoS*) y Calidad de Servicio (*QoS*) para el manejo eficiente del tráfico. 2. Debe poseer sistema de alimentación en *AC* (rango de 110 *VAC* a 220 *VAC* auto ajustable). 3. Debe contar con capacidad instalada, de actualizar el sistema operativo por vía de cable consola y a través de cualquiera de los interfaces de red *LAN* o *WAN*. 4. El tamaño del equipo debe ser de máximo de dos unidades de *rack* e incluir los aditamentos necesarios para ser montados en los *racks* o gabinetes actuales. 5. Debe contar con memoria *flash* mínima de 256

	MB instalada. 6. Contar con al menos memoria *RAM* instalada de 1 *GB*, con capacidad de crecimiento hasta 2048 *MB* para soportar futuras funcionalidades. 7. Con capacidad de desempeño de al menos 280 *Megabits* por segundo y 580,000 paquetes por segundo, para paquetes *IPv4* de 64 bytes. 8. El equipo debe soportar mecanismos de autenticación de usuarios para control de acceso basado en puerto, según el estándar *IEEE* 802.1X y a través de un servidor de *RADIUS*. 9. Debe contener integrados al chasis o de forma modular, al menos seis (6) interfaces *Giga-Ethernet* 10/100/*1000Mbps* cada uno, todas con capacidad de enrutamiento instalada. 10. Debe poseer capacidad instalada de encriptación por *hardware* basada en los estándares *IPSEC 3DES* y *AES* 256. 11. Debe tener capacidad instalada para generar múltiples *VPN*. 12. Debe tener capacidad de manejar los siguientes protocolos de enrutamiento para *IPv4*: *OSPF*, *RIPv2*, *IS-IS*, y *BGP*, así como los siguientes protocolos de enrutamiento para *IPv6*: *OSPFv3*, *RIPng* y *multiprotocol BGP*. 13. El equipo debe ser capaz de soportar *IPv4* y *IPv6*. 14. Los equipos deberán contar con capacidad instalada para soportar los siguientes protocolos de redundancia y alta disponibilidad: *RRPP*, *REP*, *VRRP*, *HSRP* o su equivalente según la marca de equipo. 15. Capacidad de manejar los siguientes protocolos de enrutamiento *multicast* para *IPv4*: PIM-*SM*, *PIM Bidirectional*, *PIM SSM*, así como los siguientes protocolos de enrutamiento *multicast* para *IPv6*: *PIM SM* y *PIM SSM*. 16. El proveedor deberá entregar los equipos con todo el licenciamiento requerido para satisfacer los requerimientos planteados por el MEP, este licenciamiento deberá ser en modalidad *Enterprise* o su equivalente, (deberá detallar el licenciamiento incluido en su oferta).

	17. El equipo debe contar con capacidad de reportar estadísticas de flujos de tráfico a través de *Netflow*, *sflow* o su equivalente en todos sus puertos. 18. Contar con capacidad instalada de realizar *Secure RTP* (*SRTP*). 19. Debe contar con capacidad instalada de realizar compresión de encabezados *RTP* y *TCP*. 20. Debe contar con capacidad instalada de emplear *SNMP* (versión 3) y *SSHv2* para la gestión. 21. Debe contar con capacidad instalada de administración vía múltiples usuarios y múltiples niveles de privilegios (incluyendo modo de sólo lectura). 22. El equipo debe incluir los aditamentos necesarios para ser montados en *Rack* de diecinueve (19) pulgadas. 23. Soportar al menos 5 sesiones simultáneas para gestión por línea de comando. Estas sesiones pueden ser local mediante un puerto de consola o remotas mediante sesiones *Telnet* seguras (*SSH* v2). 24. Incluir fuente de poder interna capaz de operar en un rango de voltaje de 100 a 240 *VAC*. 25. Debe operar en un rango de temperatura ambiente de 0C a 40C. 26. El equipo debe contar con al menos los siguientes estándares de la *IEEE*: ▪ *IEEE* 802.1Q. ▪ *IEEE* 802.1p.

11.5.4 Estándar para enrutadores (Router) Perfil 3

Especificaciones técnicas	1. El equipo debe permitir la definición e implementación de Clases de Servicio (*CoS*) y Calidad de Servicio (*QoS*) para el manejo eficiente del tráfico. 2. Debe poseer sistema de alimentación en *AC* (rango de 110 *VAC* a 220 *VAC* auto ajustable). 3. Debe contar con capacidad instalada, de actualizar el sistema operativo por vía de cable

	consola y a través de cualquiera de los interfaces de red *LAN* o *WAN*. 4. El tamaño del equipo debe ser de máximo de dos unidades de *rack* e incluir los aditamentos necesarios para ser montados en los *racks* o gabinetes actuales. 5. Debe contar con memoria flash mínima de 256 *MB* instalada. 6. Contar con al menos memoria *RAM* instalada de 1 *GB*, con capacidad de crecimiento hasta 2048 *MB* para soportar futuras funcionalidades. 7. Con capacidad de desempeño de al menos 3.*5Mpps*, para paquetes *IPv4* de 64 *bytes*. 8. El equipo debe soportar mecanismos de autenticación de usuarios para control de acceso basado en puerto, según el estándar *IEEE* 802.1X y a través de un servidor de *RADIUS*. 9. Debe contener integrados al chasis o de forma modular, al menos seis (6) interfaces *Giga-Ethernet* 10/100/*1000Mbps* cada uno, todas con capacidad de enrutamiento instalada. 10. Debe poseer capacidad instalada de encriptación por *hardware* basada en los estándares *IPSEC 3DES* y *AES* 256. 11. Debe tener capacidad instalada para generar múltiples *VPN*. 12. Debe tener capacidad de manejar los siguientes protocolos de enrutamiento para *IPv4*: *OSPF, RIPv2, IS-IS* y *BGP*, así como los siguientes protocolos de enrutamiento para *IPv6*: *OSPFv3*, *RIPng* y *multiprotocol BGP*. 13. El equipo debe ser capaz de soportar *IPv4* y *IPv6*. 14. Los equipos deberán contar con capacidad instalada para soportar los siguientes protocolos de redundancia y alta disponibilidad: *RRPP*, *REP*, *VRRP*, *HSRP* o su equivalente según la marca de equipo. 15. Capacidad de manejar los siguientes protocolos de enrutamiento *multicast* para *IPv4*: *PIM-SM*, *PIM Bidirectional*, *PIM SSM*, así como los siguientes protocolos de enrutamiento *multicast* para *IPv6*: *PIM SM* y *PIM SSM*.

	16. El proveedor deberá entregar los equipos con todo el licenciamiento requerido para satisfacer los requerimientos planteados por el MEP, este licenciamiento deberá ser en modalidad Enterprise o su equivalente, (deberá detallar el licenciamiento incluido en su oferta). 17. El equipo debe contar con capacidad de reportar estadísticas de flujos de tráfico a través de *Netflow*, *sflow* o su equivalente en todos sus puertos. 18. Contar con capacidad instalada de realizar *Secure RTP* (*SRTP*). 19. Debe contar con capacidad instalada de realizar compresión de encabezados *RTP* y *TCP*. 20. Debe contar con capacidad instalada de emplear *SNMP* (versión 3) y *SSHv2* para la gestión. 21. Debe contar con capacidad instalada de administración vía múltiples usuarios y múltiples niveles de privilegios (incluyendo modo de sólo lectura). 22. El equipo debe incluir los aditamentos necesarios para ser montados en *Rack* de diecinueve (19) pulgadas. 23. Soportar al menos 5 sesiones simultáneas para gestión por línea de comando. Estas sesiones pueden ser local mediante un puerto de consola o remotas mediante sesiones *Telnet* seguras (*SSH* v2). 24. Incluir fuente de poder interna capaz de operar en un rango de voltaje de 100 a 240 *VAC*. 25. Debe operar en un rango de temperatura ambiente de 0C a 40C. 26. El equipo debe contar con al menos los siguientes estándares de la *IEEE*: ▪ *IEEE* 802.1Q. ▪ *IEEE* 802.1p.

11.5.5 Estándar para enrutadores (Router) Perfil 4

Especificaciones técnicas	1. El equipo debe permitir la definición e implementación de Clases de Servicio (*CoS*) y Calidad de Servicio (*QoS*) para el manejo eficiente del tráfico. 2. Debe poseer sistema de alimentación en *AC* (rango de 110 *VAC* a 220 *VAC* auto ajustable). 3. Debe contar con capacidad instalada, de actualizar el sistema operativo por vía de cable consola y a través de cualquiera de los interfaces de red *LAN* o *WAN*. 4. El tamaño del equipo debe ser de máximo de dos unidades de *rack* e incluir los aditamentos necesarios para ser montados en los *racks* o gabinetes actuales. 5. Debe contar con memoria *flash* mínima de 256 *MB* instalada. 6. Contar con al menos memoria *RAM* instalada de 1 *GB*, con capacidad de crecimiento hasta 2048 *MB* para soportar futuras funcionalidades. 7. Con capacidad de desempeño de al menos 5 *Mpps*, para paquetes *IPv4* de 64 *bytes*. 8. El equipo debe soportar mecanismos de autenticación de usuarios para control de acceso basado en puerto, según el estándar *IEEE* 802.1X y a través de un servidor de *RADIUS*. 9. Debe contener integrados al chasis o de forma modular, al menos seis (6) interfaces *Giga-Ethernet* 10/100/*1000Mbps* cada uno, todas con capacidad de enrutamiento instalada. 10. Debe poseer capacidad instalada de encriptación por *hardware* basada en los estándares *IPSEC 3DES* y *AES* 256. 11. Debe tener capacidad instalada para generar múltiples *VPN*. 12. Debe tener capacidad de manejar los siguientes protocolos de enrutamiento para *IPv4*: *OSPF*, *RIPv2*, *IS*-IS, y *BGP*, así como los siguientes protocolos de enrutamiento para *IPv6*: *OSPFv3*, *RIPng* y *multiprotocol BGP*. 13. El equipo debe ser capaz de soportar *IPv4* y *IPv6*.

	14. Los equipos deberán contar con capacidad instalada para soportar los siguientes protocolos de redundancia y alta disponibilidad: *RRPP*, *REP*, *VRRP*, *HSRP* o su equivalente según la marca de equipo. 15. Capacidad de manejar los siguientes protocolos de enrutamiento *multicast* para *IPv4*: *PIM-SM*, *PIM Bidirectional*, *PIM SSM*, así como los siguientes protocolos de enrutamiento *multicast* para *IPv6*: *PIM SM* y *PIM SSM*. 16. El proveedor deberá entregar los equipos con todo el licenciamiento requerido para satisfacer los requerimientos planteados por el MEP, este licenciamiento deberá ser en modalidad Enterprise o su equivalente, (deberá detallar el licenciamiento incluido en su oferta). 17. El equipo debe contar con capacidad de reportar estadísticas de flujos de tráfico a través de *Netflow*, *sflow* o su equivalente en todos sus puertos. 18. Contar con capacidad instalada de realizar *Secure RTP* (*SRTP*). 19. Debe contar con capacidad instalada de realizar compresión de encabezados *RTP* y *TCP*. 20. Debe contar con capacidad instalada de emplear *SNMP* (versión 3) y *SSHv2* para la gestión. 21. Debe contar con capacidad instalada de administración vía múltiples usuarios y múltiples niveles de privilegios (incluyendo modo de sólo lectura). 22. El equipo debe incluir los aditamentos necesarios para ser montados en *Rack* de diecinueve (19) pulgadas. 23. Soportar al menos 5 sesiones simultáneas para gestión por línea de comando. Estas sesiones pueden ser local mediante un puerto de consola o remotas mediante sesiones *Telnet* seguras (*SSH* v2). 24. Incluir fuente de poder interna capaz de operar en un rango de voltaje de 100 a 240 *VAC*. 25. Debe operar en un rango de temperatura ambiente de 0C a 40C.

	26. El equipo debe contar con al menos los siguientes estándares de la *IEEE*: ▪ *IEEE* 802.1Q ▪ *IEEE* 802.1p.

11.5.6 Estándar de conmutadores de red (Switch) Perfil 1

Especificaciones técnicas	1. El equipo debe tener 24 puertos *Ethernet* 10/100/1000, de los cuales, al menos 8 puertos deben contar con la capacidad de *PoE*+ (*PoE Plus*) con *30Watts* por puerto de forma simultánea en base a los estándares *IEEE* 802.3af y *IEEE* 802.3at, para soportar varios puntos de acceso inalámbrico tecnología *AC*. 2. Debe tener adicionalmente 2 puertos *Gigabit Ethernet* multipropósito configurado en *1000BaseT* (10/100/1000) los cuales se utilizarán para las cascadas y conexión con el *router*, estos puertos deberán tener la posibilidad de convertirse en fibra (*1000BaseSX*, *1000BaseLX*) con transductores ópticos tipo *SFP*, en caso de que en el futuro se requieran cambiar. 3. El equipo debe ser capaz de soportar *IPv4* y *IPv6*. 4. Debe tener soporte para conmutación de paquetes en las capas 2. 5. Los puertos 10/100/1000 deben ser del tipo *Auto MDI/MDIX* de forma que reconozcan automáticamente el tipo de cable que se conecta en ellos (*straigththrough* o *crossover*). 6. Los puertos 10/100/1000 deben soportar la negociación automática de la velocidad y modo *Duplex* (*Half-Duplex* o *Full-Duplex*). 7. Debe tener una capacidad de conmutación (*switching*) mínima de al menos *16Gbps* y una capacidad de entrega de paquetes (*forwarding*) mínima de al menos 6.*5mpps*. 8. Debe poseer como mínimo a nivel de memoria 128 *Mb* en *RAM* y *32Mb* en *Flash*. 9. Debe ser compatible con los principales protocolos de *Spanning Tree* (*STP*): 802.1d, 802.1s y 802.1w. 10. Debe permitir configurar al menos 50 *VLANs* de

	forma simultánea. 11. Debe soportar al menos 8000 direcciones *MAC*. 12. Debe tener la posibilidad de autenticación de usuarios para control de acceso basado en puerto, según el estándar *IEEE* 802.1x y a través de un servidor de *RADIUS*. 13. Debe manejar al menos 4 colas de prioridad por *hardware*, administradas por el método *Weighted Round Robin (WRR) o Weghted Deficit Round Robin (WDRR)* y reconocer marcado de paquetes a través del estándar 802.1p. 14. Debe tener la capacidad de manejar listas de acceso (*ACL*). 15. Debe soportar enlaces agregados, es decir, la capacidad de configurar y agrupar lógicamente varios puertos físicos para formar uno virtual de mayor ancho de banda, de forma que se permita una mejor velocidad de conexión entre dispositivos, así como el respaldo en caso de fallo de algún enlace. Estos enlaces deben realizar el balanceo de tráfico entre los puertos que lo forman. 16. Debe soportar el protocolo *IGMP Snooping* versiones 1, 2 y 3 para la administración de los grupos y usuarios de *Multicast*. Debe ser posible definir al menos 250 grupos de *multicast*. 17. Debe incluir soporte para *SNMP* Versiones 2, 2c y 3, así como los grupos de *RMON* definidos en RFC 1757. 18. Deberá garantizarse la compatibilidad con el *software* de monitoreo de redes *OPmanager* propiedad del Ministerio. 19. Debe incluir soporte para el protocolo *NTP* (*Network Time Protocol*) para sincronización de los eventos. 20. Debe ser de una unidad de *rack* e incluir los aditamentos necesarios para ser montados en los *racks* o gabinetes actuales. 21. Debe soportar al menos 5 sesiones simultáneas para gestión por línea de comando. Estas sesiones pueden ser local mediante un puerto de consola o remotas mediante sesiones *Telnet* seguras (*SSH* v2). 22. Debe contar con capacidad instalada de

	administración vía múltiples usuarios y múltiples niveles de privilegios (incluyendo modo de sólo lectura). 23. El equipo debe contar con capacidad instalada, de actualizar el sistema operativo por vía de cable consola y a través de cualquiera de sus puertos. 24. Debe poseer al menos los siguientes tipos de mecanismos que permitan la mitigación de ataques y accesos no deseados a nivel de comunicaciones: *Dynamic ARP Inspecction*, *MAC address notification*. 25. El equipo deberá poder realizar Clase de Servicio y Calidad de Servicio (*CoS* y *QoS*). 26. Debe incluir fuente de poder interna capaz de operar en un rango de voltaje de 100 a 240 *VAC*. 27. Debe operar en un rango de temperatura ambiente de 0C a 40C. 28. Debe disponer de mecanismos para replicar y monitorear el tráfico tanto de puertos de origen como *VLAN* de origen en alguno de sus otros puertos. Debe manejar filtros que permitan monitorear solo el tráfico de interés. Deberá permitir hasta dos sesiones de replicación de tráfico de forma simultánea. 29. El equipo ofertado debe cumplir con los siguientes estándares de la industria: ▪ *IEEE 802.1D Spanning Tree Protocol.* ▪ *IEEE 802.1p CoS Prioritization.* ▪ *IEEE 802.1Q VLAN.* ▪ *IEEE 802.1s.* ▪ *IEEE 802.1w.* ▪ *IEEE 802.1X.* ▪ *IEEE 802.1ab (LLDP without MED*).* ▪ *IEEE 802.3ad.* ▪ *IEEE 802.3ah (100BASE-X single- and multimode fiber only).* ▪ *IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports.* ▪ *IEEE 802.3 10BASE-T specification.* ▪ *IEEE 802.3u 100BASE-TX specification.* ▪ *IEEE 802.3ab 1000BASE-T specification.* ▪ *IEEE 802.3z 1000BASE-X specification.* ▪ *Remote Monitoring (RMON) I and II standards.* ▪ *SNMPv1, v2c, and v3.* ▪ *RFC 768 – UDP.*

	▪ *RFC 783 – TFTP.* ▪ *RFC 791 – IP.* ▪ *RFC 792 – ICMP.* ▪ *RFC 793 – TCP.* ▪ *RFC 826 - Address Resolution Protocol (ARP).* ▪ *RFC 854 – Telnet.* ▪ *RFC 951 - Bootstrap Protocol (BOOTP).* ▪ *RFC 959 – FTP.* ▪ *RFC 1112 - IP Multicast and IGMP.* ▪ *RFC 1157 - SNMP v1.* ▪ *RFC 1166 - IP addresses.* ▪ *RFC 1305 – NTP.* ▪ *RFC 1492 - TACACS+.* ▪ *RFC 1493 - Bridge MIB.* ▪ *RFC 1542 - BOOTP extensions.* ▪ *RFC 1643 - Ethernet Interface MIB.* ▪ *RFC 1757 – RMON.* ▪ *RFC 1901 - SNMP v2C.* ▪ *RFC 1902-1907 - SNMP v2.* ▪ *FRC 2068 – HTTP.* ▪ *RFC 2131 – DHCP.* ▪ *RFC 2138 – RADIUS.* ▪ *RFC 2233 - IF MIB.* ▪ *RFC 2273-2275 - SNMP v3.* ▪ *RFC 2474 - Differentiated Services (DiffServ) Precedence.* ▪ *RFC 2597 - Assured Forwarding.* ▪ *RFC 2598 - Expedited Forwarding.* ▪ *RFC 2571 - SNMP Management.* ▪ *RFC 3046 - DHCP Relay Agent Information Option.* ▪ *RFC 3376 - IGMP v3.* ▪ *RFC 3580 - 802.1X RADIUS.*

11.5.7 Estándar para conmutador de CORE capa 3 (Switch) Perfil 2

Especificaciones técnicas	1. Se requiere contratar el aprovisionamiento por modalidad de arrendamiento mensual de 1 *Switch* (conmutador) de *Core* capa 3, que opere en alta disponibilidad y redundancia, para sustituir el equipo actual *Cisco* modelo *Catalyst* 4507R+E, con el propósito de mantener la comunicación entre los servidores principales del MEP, con oficinas centrales y direcciones regionales. 2. El equipo debe ser modular e incluir fuentes de poder redundantes capaces de operar en un rango de voltaje de 100 a 240 *VAC* autoajustable. Estas fuentes se deben poder reemplazar sin necesidad de apagar el equipo.

	3. El oferente deberá realizar los trabajos eléctricos necesarios para que el equipo quede operando correctamente. 4. El equipo debe contar con una matriz de conmutación (*switching*) de al menos 900 *Gbps* con un *throughput* en *IPv6* de 125 *Mpps*. 5. El dispositivo debe entregarse instalado con al menos *2GB* de *RAM* y 1 *GB flash*. 6. El equipo debe tener como mínimo noventa y seis (96) puertos 10/100/1000 *Base-T* (configurados como *auto MDI*/*MDIX*), con capacidad de negociación automática de velocidad y *dúplex*. 7. Los puertos 10/100/1000 *Base-T* deben ser del tipo *Auto MDI/MDIX* de forma que reconozcan automáticamente el tipo de cable que se conecta en ellos (*straigth-through* o *crossover*). 8. El equipo debe contar adicionalmente con un mínimo de quince (15) puertos de agregación en el chasis para interfaces de fibra, de los cuales 4 puertos deben ser de 10 *Gigabit* (*IEEE* 802.3ae) en *SPF*+ y los restantes a *1000Base*-X, tipo *SFP*. El uso de estos puertos no debe deshabilitar otros puertos del equipo. 9. El equipo debe incluir todos los componentes y/o accesorios necesarios para que los puertos de fibra queden habilitados (conectores, cable fibra, entre otros) los cuales serán para la interconexión de la solución. 10. La unidad deberá tener indicadores de energía como también de actividad y alarmas (Visualizar el estado de cada puerto y a su vez si el equipo presenta alguna falla por medio de indicadores de luz). 11. El *switch* que se adjudiquen deberá ser capa3. 12. Capacidad de poder realizar enrutamiento *IPv4* y *IPv6*. *IPv4*: Estático, *RIPv1*, *RIPv2*, *OSPF*, *IS-IS*, *BGPv4*. *IPv6*: Estático, *Dual IP Stack*, *RIPng*, *OSPFv3*, *IS-IS*, *BGP*+, *IPv6 tunneling*. 13. El equipo debe ser capaz de soportar *IPv4* y 14. *IPv6*. 15. El equipo debe permitir el soporte de configuración de al menos 11000 rutas *unicast* y al menos 1000 *multicast*.

	16. El equipo debe manejar los siguientes protocolos de *Multicast* en *IPv4*: *PIM* versión 2, *IGMPv2*, *IGMPv3* y *MSDP* (*Multicast Source Discovery Protocol*). 17. El equipo debe soportar el protocolo *IGMP Snooping* para la administración de los grupos y usuarios de *Multicast*. 18. El equipo debe soportar el control de tormentas de *broadcast*, *multicast* y *unicast* en cada uno de los puertos. 19. El equipo debe manejar al menos 8 colas de prioridad por *hardware*, administradas por el método *Weighted Round Robin* (*WRR*). 20. Calidad de Servicio (*Qos*) con soporte de acciones de congestión *Strict Priority* (*SP*), *Weighted Round Robin* (*WRR*), *Weighted Fair Queuing* (*WFQ*) y *WRED* (*Weigthed Random Early Detection*). 21. El equipo debe permitir la definición e implementación de Clases de Servicio (*CoS*) y Calidad de Servicio (*QoS*) para el manejo eficiente del tráfico. 22. El equipo debe tener la capacidad de bloquear tráfico no permitido dentro de la red local según el tipo de aplicación o tráfico. 23. Debe tener la capacidad de configurarse redes privadas virtuales (*VPN- Virtual Private Network*), con manejo de los siguientes protocolos *Tuneles IPSec*, *Tuneles Gre*, *Internet Key Exchange* (*IKE*). 24. Capacidad de administración empleando las siguientes formas: a. Puerto de consola. b. *SNMP* V2, V3. c. *sFlow* (*RFC* 3176). d. *FTP*, *TFTP* y *SFTP*. e. *NTP (Network Time Protocol).* *f. NQA (Network Quality Analyzer).* g. El equipo debe contar con al menos los siguientes grupos de *RMON* I y II (Monitoreo Remoto): estadísticas, historial, alarma y eventos. 25. El equipo debe contar con capacidad instalada de administración vía múltiples usuarios y múltiples niveles de privilegios (incluyendo modo de sólo lectura).

	26. Deberá garantizarse la compatibilidad con el *software* de monitoreo de redes *opmanager* propiedad del Ministerio para el monitoreo de equipos por *SNMP* v3 y *Netflow*. 27. El equipo debe incluir soporte para el protocolo *NTP* (*Network Time Protocol0*) para sincronización de los eventos. 28. El equipo debe soportar al menos 5 sesiones simultáneas para gestión por línea de comando. 29. Estas sesiones pueden ser local mediante un puerto de consola o remotas mediante sesiones *Telnet* seguras (*SSH* v2). 30. El equipo debe contar con una *CLI* (Interfaz de Línea de Comando) a través del puerto de la consola (consola de control), además de ser accedida por *Telnet* o *SSH*. 31. El equipo debe poderse denegar el acceso a usuarios no autorizados basado en el *MAC Address*. 32. Debe poseer al menos los siguientes tipos de mecanismos que permitan la mitigación de ataques y accesos no deseados a nivel de comunicaciones: "*Dynamic ARP Inspecction*", "*MAC address notification*". 33. El equipo deberá ser capaz de reportar su flujo de tráfico para el análisis de protocolos a través de mecanismos como *Net-Flow*, *S-Flow* o su equivalente, en todos sus puertos. 34. El equipo debe manejar listas de control de acceso en capa dos, capa tres y cuatro, estas listas de acceso se deben poder aplicar a cualquier puerto físico, así como a cualquier *VLAN*. 35. Soporte de listas de control de acceso (*ACL*) en capa 2 y 3. 36. El equipo debe tener soporte para manejar direccionamiento *IPv4* y *IPv6*. 37. El equipo debe soportar *DHCP Relay*. 38. El equipo debe contar con capacidad instalada, de actualizar el sistema operativo por vía de cable consola (en *RS*-232) y a través de cualquiera de sus puertos vía *tftp* y *ftp*. 39. El equipo debe operar en un rango de

	temperaturas de 0C a 40C. 40. El equipo debe contar con información detallada de alarmas y *debug*. 41. Los equipos deberán contar con capacidad instalada para soportar los siguientes protocolos de redundancia y alta disponibilidad, *VRRP, RRPP, REP, HSRP, GLBP, y CARP*, o su equivalente según la marca. 42. El equipo debe soportar ping y rastreo de rutas *IPv4* y *IPv6*. 43. El equipo debe ser compatible con los principales protocolos de *Spanning Tree* (*STP*): *IEEE* 802.1d, *IEEE* 802.1s *Multiple Spanning Tree Protocol* y *IEEE* 802.1w *Rapid Spanning Tree Protocol* (*RSTP*). 44. El equipo debe soportar mecanismos de autenticación de usuarios para control de acceso basado en puerto, según el estándar *IEEE* 802.1X y a través de un servidor de *RADIUS*. 45. El equipo debe soportar la autenticación vía *TACACS*+ o *RADIUS* que permita un control centralizado de la administración e impida que usuarios no autorizados puedan alterar la configuración. 46. El equipo debe tener la capacidad de ofrecer seguridad a nivel de direccionamiento *MAC* en los puertos, para así prevenir que usuarios no autorizados se conecten a un puerto en específico. 47. El equipo debe permitir configurar al menos 1000 *VLANs* de forma simultánea y permitir configurar "*trunking*" de *VLANs* mediante 802.1q en cualquiera de sus puertos. 48. El equipo debe disponer de mecanismos para replicar y monitorear el tráfico tanto de puertos de origen como *VLAN* de origen en alguno de sus otros puertos. 49. Debe manejar filtros que permitan monitorear solo el tráfico de interés. Deberá permitir hasta dos sesiones de replicación de tráfico de forma simultánea. 50. El proveedor debe aportar todos los implementos y accesorios necesarios para que

	el equipo quede totalmente operativo con la plataforma actual. 51. El proveedor deberá entregar los equipos con todo el licenciamiento requerido para satisfacer los requerimientos planteados por el MEP, este licenciamiento deberá ser en modalidad Enterprise o su equivalente, (deberá detallar el licenciamiento incluido en su oferta). 52. El equipo ofertado debe soportar al menos 6000 direcciones *MAC*, 1000 grupos *IGMP* de multicast, y 8000 rutas *IPv4* e *IPv6* de forma simultánea. 53. Debe soportar enlaces agregados, es decir, la capacidad de configurar y agrupar lógicamente varios puertos físicos para formar uno virtual de mayor ancho de banda, de forma que se permita una mejor velocidad de conexión entre dispositivos así como el respaldo en caso de fallo de algún enlace. Estos enlaces deben realizar el balanceo de tráfico entre los puertos que lo forman. 54. El equipo ofertado debe cumplir con los siguientes estándares de la industria: ▪ *IEEE 802.1D Spanning Tree Protocol.* ▪ *IEEE 802.1p CoS Prioritization.* ▪ *IEEE 802.1Q VLAN.* ▪ *IEEE 802.1s.* ▪ *IEEE 802.1w.* ▪ *IEEE 802.1X.* ▪ *IEEE 802.3ad (Link aggregation).* ▪ *IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports.* ▪ *IEEE 802.3 10BASE-T specification.* ▪ *IEEE 802.3u 100BASE-TX specification.* ▪ *IEEE 802.3ab 1000BASE-T specification.* ▪ *IEEE 802.3z 1000BASE-X specification.* ▪ *Remote Monitoring (RMON) I and II standards.* ▪ *SNMPv1, v2c, and v3.* ▪ *RFC 768 – UDP.* ▪ *RFC 783 – TFTP.* ▪ *RFC 791 – IP.* ▪ *RFC 792 – ICMP.* ▪ *RFC 793 - TCP* ▪ *RFC 826 - Address Resolution Protocol (ARP).* ▪ *RFC 854 – Telnet.* ▪ *RFC 951 - Bootstrap Protocol (BOOTP).* ▪ *RFC 959 – FTP.* ▪ *RFC 1112 - IP Multicast and IGMP.*

	▪ *RFC 1166 - IP addresses.* ▪ *RFC 1305 – NTP.* ▪ *RFC 1492 - TACACS+.* ▪ *RFC 1493 - Bridge MIB.* ▪ *RFC 1542 - BOOTP extensions.* ▪ *RFC 1643 - Ethernet Interface MIB.* ▪ *RFC 1757 – RMON.* ▪ *RFC 1901 - SNMP v2C.* ▪ *RFC 1902-1907 - SNMP v2.* ▪ *RFC 2068 – HTTP.* ▪ *RFC 2131 – DHCP.* ▪ *RFC 2138 – RADIUS.* ▪ *RFC 2273-2275 - SNMP v3.* ▪ *RFC 2474 - Differentiated Services (DiffServ) Precedence.* ▪ *RFC 2597 - Assured Forwarding.* ▪ *RFC 2598 - Expedited Forwarding.* ▪ *RFC 2571 - SNMP Management.* ▪ *RFC 3046 - DHCP Relay Agent Information Option.* ▪ *RFC 3376 - IGMP v3.* ▪ *RFC 3580 - 802.1X RADIUS.*

11.5.8 Estándar para conmutadores de red (Switch) Perfil 3

Especificaciones técnicas	1. Debe tener soporte para conmutación de paquetes en las capas 2, según el modelo de referencia *OSI*. 2. Debe contar con 24 puertos 10/100/*1000BASE*-T con auto-negociación configurados como auto *MDI/MDIX*, utilizando conectores *RJ-45*. 3. El equipo debe contar con capacidad de conmutación de paquetes de al menos 88 *Gbps*. 4. El equipo debe contar con al menos dos ranuras de expansión, en la parte trasera o delantera, donde permita colocar un módulo con al menos 2 puertos para conexiones de fibra óptica en 10 *Gigabyte Ethernet* o conexiones CX 1 ó CX4. Asimismo, debe contar con la posibilidad de apilarse al menos 4 equipos. El apilamiento debe hacerse por medio de un puerto especial para dicho efecto, es decir, debe ser distinto a los puertos frontales. 5. El equipo debe contar con un ancho de banda de apilamiento *full-duplex* de 10 *Gbps*. 6. El equipo debe contar con auto-negociación de la velocidad del puerto y del modo de operación *dúplex* (*Half* o *Full*).

	7. El equipo debe contar con una única dirección *IP* e interfaces de administración para control en toda la pila. 8. El equipo debe contar con cuatro colas de *hardware* por puerto. 9. El equipo debe contar con una tabla de direcciones *MAC* capaz de almacenar como mínimo 16000 direcciones dinámicas. 10. El equipo debe contar con una tabla de direcciones *MAC* estáticas de al menos 1024 direcciones. 11. Debe de contar con un *backplane* al menos 40 *Gigas*. 12. El equipo debe poder configurar al menos 250 *VLANs* y 2000 etiquetas de *Vlans* definidas mediante el protocolo *IEEE* 802.1Q. 13. El equipo debe soportar el protocolo *Spanning Tree* (*STP*) *IEEE* 802.1D. 14. El equipo debe soportar el protocolo *Rapid Spanning Tree* (*RSTP*) *IEEE* 802.1w. 15. El equipo debe soportar el protocolo de Control de Agregación de Enlaces (*LACP*) *IEEE* 802.3ad. 16. El equipo debe contar con soporte para Agregación Manual, Agregación entre las unidades. 17. El equipo debe contar con la posibilidad de realizar al menos 6 grupos de entronque con otros conmutadores de red, donde cada uno de estos grupos debe ser de 8 puertos 10/100/1000. 18. El equipo debe contar con la posibilidad de definirle al menos 5 interfaces *IP*. 19. El equipo debe soportar el protocolo *IGMP* v1 y v2. 20. El equipo debe contar con la posibilidad de realizar *DHCP Relay*. 21. El equipo deberá poder realizar Clase de Servicio y Calidad de Servicio (*CoS* y *QoS*) *IEEE* 802.1p en el egreso de los paquetes de datos por sus diferentes puertos. 22. El equipo debe poder aplicar listas de control de acceso (*ACLs*). 23. El equipo debe poder realizar bloqueo de aplicaciones y protocolo en todos sus puertos.

	24. El equipo debe poder hacer autentificación de usuarios por medio del protocolo *IEEE* 802.1X y de esta manera utilizar autentificación *RADIUS*, múltiples usuarios por puerto al asegurarse a la dirección *MAC*, asignación automática de puertos de *VLANs* y acceso de dispositivos autenticados con *RADIUS*. 25. El equipo debe poder realizar autenticación *PAP*, *CHAP*, *EAPoL* (*EAP* sobre *LAN*), para múltiples usuarios por puerto. 26. El equipo debe poder realizar la desconexión de dispositivos desconocidos (*DUD*) en caso de que el dispositivo conectado a un puerto no sea válido a ese puerto. 27. El equipo debe poder aplicar filtros por listas de control de acceso (*ACL*) para las capas 2, 3 y 4, validando direcciones *MAC* de fuente/destino, direcciones *MAC* de fuente y/o destino, dirección *IP* de fuente, dirección *IP* de destino, puerto *TCP* de fuente, puerto *TCP* de destino, puerto *UDP* de fuente, puerto *UDP* de destino. 28. El equipo debe poder realizar múltiples sesiones concurrentes de administración. 29. El equipo debe poder soportar tráfico de administración encriptado, accesible a través de *Secure Shell* (*SSH* v2) o interfaz *SNMP* v3. 30. El equipo debe soportar que los registros administración de actividad sean grabados y reenviados a un servidor *syslog*. 31. El equipo debe contar con una *CLI* (Interfaz de Línea de Comando) a través del puerto de la consola (consola de control) o por medio de *Telnet*. 32. El equipo debe contar con soporte para el protocolo *SNMP* v1, 2 y 3. 33. El equipo debe contar con al menos los siguientes grupos de *RMON* (Monitoreo Remoto): estadísticas, historial, alarma y eventos. 34. El equipo debe contar con estadísticas para *ACL* y *QoS*. 35. El equipo debe contar con estadísticas detalladas del comportamiento de la interfaz *IP*. 36. El equipo debe soportar múltiples imágenes de

	software instaladas en el equipo así como múltiples archivos de configuración. 37. El equipo debe poder realizar duplicación de puertos en todas las siguientes formas: ▪ Duplicación de puerto 1 a 1. ▪ Duplicación de puerto Varios-a-1. 38. El equipo debe contar con información detallada de alarmas y *debug*. 39. El equipo debe soportar *ping* y rastreo de rutas. 40. El equipo debe contar con la posibilidad de realizar respaldo y restauración de imagen de *software*, así como de su configuración. 41. El equipo debe contar con al menos las siguientes herramientas de *debugging* de red: *DHCP tracker* y *UDP Helper*. 42. El equipo debe soportar la carga y descarga de archivos por medio de: ▪ *Xmodem*. ▪ *FTP* (Protocolo de Transferencia de Archivos). ▪ *TFTP* (Protocolo de Transferencia de Archivos Triviales). 43. El equipo debe operar bajo las siguientes condiciones: ▪ Temperatura operativa: 0° a 40°C. ▪ Temperatura de almacenamiento: -10° a 70°C. ▪ Humedad (operación y almacenamiento): 10% a 95% sin condensación. 44. El equipo debe soportar al menos los siguientes estándares: ▪ *EN 60068 (IEC 68).* ▪ *IEEE 802.1D (STP).* ▪ *IEEE 802.1p (CoS).* ▪ *IEEE 802.1Q (VLANs).* ▪ *IEEE 802.1S (MSTP).* ▪ *IEEE 802.1w (RSTP).* ▪ *IEEE 802.1X (Seguridad).* ▪ *IEEE 802.3 (Ethernet).* ▪ *IEEE 802.3ad (Agregación de Enlaces).* ▪ *IEEE 802.3ab (1000BASE-T).* ▪ *IEEE 802.3ae (10G-Ethernet).* ▪ *IEEE 802.3i (10BASE-T).* ▪ *IEEE 802.3u (Fast Ethernet).* ▪ *IEEE 802.3x (Flow Control).* ▪ *IEEE 802.3z (Gigabit Ethernet).* 45. El equipo debe soportar al menos los

	siguientes *RFC*: ▪ *RFC 1213/2233 (MIB II).* ▪ *RFC 2233 (Interfaces MIB).* ▪ *RFC 2571 (FrameWork).* ▪ *RFC 2571-2575 (SNMP).* ▪ *RFC 2668 (IEEE 802.3 MAU MIB).* ▪ *RFC 2674 (Extensión VLAN MIB).* ▪ *RFC 2819 (RMON MIB).* 46. El equipo debe contar con al menos las siguientes certificaciones de emisiones y aprobaciones: ▪ *CISPR 22 Clase A.* ▪ *FCC Parte 15 Clase A.* ▪ *EN 55022 1998 Clase A.* ▪ *VCCI Clase A.* ▪ *EN 55024.* ▪ *UL 60950.* ▪ *IEC 60950-1.* ▪ *EN 60950-1.* ▪ *CAN/CSA-C22.2 No. 60950-1-03.*

11.5.9 Estándar para conmutadores de red (Switch) Perfil 4

Especificaciones técnicas	1. Deberá tener soporte para conmutación de paquetes en Capa 2 y capacidad de ruteo Capa 3 según el modelo de referencia *OSI*. 2. Debe tener instalados 24 puertos 10/100/1000 *Base-T*, conector *RJ45*. De los cuales 4 deben ser de doble propósito y puedan ser utilizados como puertos 10/100/1000 *Base-T* o bien en Fibra Óptica con módulos *SFP*. 3. Los puertos 10/100/1000 *Base-T* deben ser del tipo *Auto MDI/MDIX* de forma que reconozcan automáticamente el tipo de cable que se conecta en ellos (*straigth-thru* o *crossover*). 4. Debe contar con al menos una ranura para colocar módulos de expansión o apilamiento en la parte trasera. 5. Los módulos de expansión deben permitir ampliar la capacidad del equipo en al menos dos puertos *10Gigabit Ethernet*. Los puertos en los módulos pueden ser para fibra óptica multimodo con conector *SFP*, fibra óptica monomodo con conector *SFP* o puertos *10Gigabit Ethernet* en cobre, con conector *RJ45*. 6. El equipo debe ser apilable hasta sumar, al

	menos, 192 puertos o sea 8 dispositivos puertos por pila. El apilamiento debe hacerse por medio de un puerto especial para dicho efecto, es decir, debe ser distinto a los puertos frontales. El puerto de apilamiento debe operar a una velocidad de operación de al menos 48 *Gbps*. 7. Los equipos apilados deben tener la capacidad de ser administrados como una sola unidad utilizando una única dirección *IP*. 8. Los equipos deben tener la capacidad de ser retirados de la pila en caso de fallo, sin que se afecte la operación normal del resto de equipos apilados, es decir, la pila debe seguir operando normalmente. 9. Deberá tener indicadores de actividad, enlace y colisión por puerto *Ethernet*. La unidad deberá tener indicadores de energía como también de actividad y alarmas. 10. Debe soportar la negociación automática de la velocidad de operación de los puertos 10/100/*1000Base-T*. 11. Debe poder configurarse el modo de operación de cada puerto en *Half-Duplex* o *Full-Duplex*. 12. El equipo debe ser "*non-blocking*", esto es, que la matriz de conmutación sin el uso de búferes permita simultáneamente el manejo de todos los puertos sin bloquearse. El *backplane* debe ser de al menos 120 *Gbps*. 13. El equipo debe contar con al menos *16MB* de memoria *FLASH* y 64 *MB* de memoria *DRAM*. 14. Debe tener una estructura tal que permita ser colocado en un bastidor (*rack*) estándar de 19 pulgadas. 15. Deberá operar de manera continua con fuente de poder de 120 VAC, *60Hz*. 16. Deberá tener la capacidad de utilizar al menos una fuente de poder redundante. 17. El equipo debe cumplir con el estándar *IEEE* P802.3af, de modo que pueda suministrar alimentación eléctrica a los dispositivos que así lo requieran, a través de los puertos frontales. 18. Debe tener un mecanismo de monitoreo de los valores mínimos, máximos y promedio en el

	consumo de energía eléctrica. Además debe estar en capacidad de enviar notificaciones en caso de alarmas o fallos. 19. Debe tener un mecanismo de control centralizado que permita habilitar, deshabilitar o limitar el suministro de electricidad por puerto. 20. Debe tener la capacidad de garantizar el suministro de electricidad a dispositivos de misión crítica, para lo cual debe ser posible identificar o configurar los puertos en los cuales están conectados esos dispositivos para tal efecto. 21. En caso de que un equipo de misión crítica aumente sus requerimientos de potencia o el consumo total de los puertos exceda la capacidad máxima de suministro del conmutador, este debe estar capacitado para deshabilitar automáticamente el suministro de potencia a uno o varios puertos que no estén identificados como críticos. 22. La configuración, el monitoreo y el control de estos parámetros de suministro de potencia deben hacerse vía línea de comandos (*CLI*), y vía interface *WEB*. **Nota:** Para los puntos 19, 20 y 21 anteriores, debe entenderse que los equipos deben manejar la propiedad *power over ethernet*, según estándar *IEEE* 802.3 AF. 23. Debe tener capacidad instalada de procesamiento de al menos 92 *Mbps* (Millones de paquetes por segundo). 24. El método de conmutación utilizado debe ser del tipo *Store and Forward*. 25. Soporte de por lo menos 16.000 direcciones *MAC*. Debe soportar al menos 1000 direcciones *MAC* estáticas. 26. Debe contar con control de flujo en todos los puertos que operan en modo *Full-Duplex*, según el estándar *IEEE* 802.3x. 27. Soporte instalado de *Spanning Tree Protocol* (*STP*) según el estándar *IEEE* 802.1D y soporte de *Rapid Spanning Tree Protocol* (*RSTP*) según el estándar *IEEE* 802.1w.

	28. Soporte para enlaces agregados, es decir, la capacidad de configurar y agrupar lógicamente varios puertos físicos para formar uno virtual de mayor ancho de banda, de forma que se permita una mejor velocidad de conexión entre dispositivos así como el respaldo en caso de fallo de algún enlace. Estos enlaces deben realizar el balanceo de tráfico entre los puertos que lo forman. 29. Se deben poder configurar al menos 12 grupos de enlaces agregados por equipo. 30. Los enlaces agregados deben poder configurarse de manera manual o automática según el estándar 802.3ad. (*LACP*). 31. Los enlaces agregados pueden estar formados por puertos ubicados en equipos distintos, en caso de que se implemente el apilamiento de varios equipos. 32. Soporte del protocolo *IGMP* para la administración de los grupos y usuarios de *Multicast*. Debe ser posible definir al menos 128 grupos de *multicast*. 33. Debe soportar *IGMP Snooping*, como mecanismo de control de tráfico de *multicast*. 34. Debe permitir configurar redes *Ethernet* conmutadas convencionales y virtuales. Deberá soportar al menos 4000 *VLANs* según el estándar *IEEE* 802.1Q. 35. Debe contar con un mecanismo de control de tormentas de *broadcast*. 36. El equipo deberá tener la capacidad de alto grado de disponibilidad con enlaces de puertos redundantes para tener conexiones dobles y en caso de falla de la conexión primaria la conexión secundaria entre en funcionamiento instantáneamente. 37. Debe permitir la configuración automática de su dirección *IP* vía *DHCP* y tener soporte de *BOOTP*. 38. Debe permitir la definición e implementación de Clases de Servicio y Calidad de Servicio para la clasificación de tráfico, y asignarle prioridad a dichas clasificaciones. 39. Debe cumplir con el estándar 802.1p.

	40. La clasificación de tráfico debe implementarse usando al menos alguno de estos métodos: estándar *IEEE* 802.1p, puertos de *TCP/UDP*, dirección *IP*, número de puerto físico. 41. Debe manejar al menos 8 colas de prioridad por puerto, administradas por el método *Weighted Round Robin* (*WRR*). 42. El equipo deberá tener la capacidad de bloquear tráfico no permitido dentro de la red local según el tipo de aplicación. 43. Debe contar con varios niveles de usuarios y claves de acceso. 44. Debe estar en capacidad de interactuar con un servidor *RADIUS* para la autenticación de usuarios. 45. Debe tener instalado algún mecanismo de autenticación de usuarios para control de acceso basado en puerto, según el estándar *IEEE* 802.1X. 46. Capacidad instalada de replicar y monitorear el tráfico de un puerto en alguno de sus otros puertos. 47. Debe tener capacidad instalada para denegar el acceso a usuarios no autorizados basado en el *MAC Address*. 48. Debe permitir la configuración vía línea de comandos. 49. La unidad deberá tener un puerto de consola con *i*nterface *RS*-232 (*DB*-9) que permita la configuración, mantenimiento y administración local del *Switch*. 50. Debe controlar y permitir el acceso y configuración vía *TELNET* de manera local o remota. 51. La unidad podrá configurarse por medio de una sesión de navegador de Internet (*Web Browser*). 52. Debe permitir la configuración y administración remota vía protocolo *SNMP MIB* I y *MIB* II. 53. Debe contar con soporte de al menos los siguientes cuatro grupos de monitoreo *RMON*: Estadísticas, Históricos, Alarmas y Eventos. 54. Capacidad de actualizar el sistema operativo del equipo vía *TFTP*. 55. Deberá ofrecerse con la capacidad de ser

	gestionado desde un sistema de administración. La administración de los dispositivos deberá ser basada en el protocolo estándar de redes *SNMP* y los agentes de administración, monitoreo y alarmas deberán ser compatibles, administrables y programables desde el sistema de gestión de redes. 56. Deberá incluir el *software* necesario para su configuración y administración. El *software* deberá ser capaz de reconocer dispositivos con soporte de *SNMP* de red tanto cableada como inalámbrica para facilitar la administración de la red. El *software*, como mínimo, deberá realizar estas funciones: a. Descubrir Topología de red. b. Mostrar estrés de la red. c. Segmentar *VLAN´*s de manera gráfica. d. Bloquear puertos. e. Bloquear Aplicaciones *UDP*/*TCP*. f. Priorizar aplicaciones. g. Alarmas hacia correo electrónico, *pager* o pantalla de Administración. h. Inventario de Equipo. i. Alertas. j. Salvar Mapas. k. Importar Mapas. l. Búsqueda de Equipos. m. Tareas Agendadas. n. Realizar *Backups* de la Topología. 57. El equipo debe tener la capacidad de realizar el respaldo y recuperación de los archivos de configuración. 58. Debe cumplir al menos con los siguientes estándares y protocolos de la industria: *a.* Protocolos de capa 1 y capa 2: *IEEE 802.1D, IEEE 802.1w, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802ad, IEEE P802.3af draft.* *b.* Gestion, incluyendo *MIBs* soportados: *SNMP Protocol (RFC 1157), MIB-II (RFC 1213), Bridge MIB (RFC 1493), RMON MIB II (RFC 2021), Remote Monitoring MIB (RFC 1757), Interface MIB (2233), MAU MIB (RFC 2668), PoE MIB (3FC 484).* *c. Emissions / Agency Approvals*: *CISPR 22 CLASS A, EN55022 CLASS A, FCC PART 15 SUBPART B*

	CLASS A, ICES-003 CLASS A, AS/NZS 3548 CLASS A, VCCI CLASS A, CNS 13438 CLASS A, EN61000-3-2, EN61000-3-3 EN55024. d. Certificaciones de Seguridad: *UL60950*, *EN60950*, *CSA22.2 No. 60950, IEC 60950*.

11.5.10 Estándar para Firewall perfil 1

Especificaciones técnicas	1. El equipo ofertado deberá incluir fuente de poder interna capaz de operar en un rango de voltaje entre 100 a 240 *VAC*. 2. Deberá contener integrados al chasis o de forma modular, al menos doce (12) puertos de interfaces 10/100/1000 *Base-T RJ45* cada uno. 3. Deberán contener puerto independiente de consola. 4. Deberán contener mínimo *4GB* de disco duro que garantice la utilización del equipo, actualizaciones y demás funciones dentro del periodo de contrato. 5. Deberán manejar un *Throughput* de *Firewall* de al menos 11 *Gbps*. 6. Deberán manejar un *Throughput* de *IPS* de al menos 6 *Gbps*. 7. Deberán de manejar al menos 70.000 (setenta mil) nuevas conexiones por segundo. 8. Deberán tener capacidad de manejar los siguientes protocolos de enrutamiento para *IPv4*: *OSPF* y *BGP*, así como protocolos de enrutamiento para *IPv6*. 9. Deberán contar con capacidad instalada de administración vía múltiples usuarios y múltiples niveles de privilegios. 10. Deberán soportar y gestionar el protocolo *IPv4* y *IPv6*. 11. Deberán soportar y gestionar capa 2 y capa 3 del modelo *OSI*. 12. Deberán soportar y manejar zonas de seguridad para la aplicación de políticas de seguridad. 13. El *Firewall* deberá incluir lo siguiente: a. Las reglas de *firewall* deberán analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o

	Zonas) y *VLANs*. b. Será posible definir políticas de *firewall* que sean independientes del puerto de origen y puerto de destino. c. Las reglas del *firewall* deberán tomar en cuenta dirección *IP* origen (que puede ser un grupo de direcciones *IP*), dirección *IP* destino (que puede ser un grupo de direcciones *IP*) y servicio (o grupo de servicios) de la comunicación que se está analizando. d. Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación. e. Deberá soportar la capacidad de definir nuevos servicios *TCP* y *UDP* que no estén contemplados en los predefinidos. f. Capacidad de hacer traslación de direcciones estático, uno a uno, *NAT*. g. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, *PAT*. h. Deberá soportar reglas de firewall en IPv6 configurables tanto por *CLI* (*Command Line Interface*, Interface de línea de comando) como por *GUI* (*GraphicalUser Interface*, Interface Gráfica de Usuario). 14. Deberá tener *IPS* que incluya lo siguiente: a. Deberá apoyar las políticas de la granularidad de *IPS*, que permite la creación de diferentes políticas de seguridad de la zona, la dirección de origen, dirección de destino, y la combinación de servicios de todos estos elementos. b. Deberá ser posible crear diferentes perfiles de *IPS* para su aplicación por la zona de seguridad, dirección de origen, dirección de destino, y la combinación de servicios de todos estos elementos. c. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico *IPv6*. d. Capacidad de actualización automática de firmas *IPS* mediante tecnología de tipo "*Push*" (permitir recibir las actualizaciones cuando los centros de actualización envíen

	notificaciones sin programación previa), adicional a tecnologías tipo "*pull*" (Consultar los centros de actualización por versiones nuevas). e. El detector y preventor de intrusos deberá de estar orientado para la protección de redes. f. El detector y preventor de intrusos deberá estar integrado en el equipo ofertado. Sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o *software* adicional para realizar la prevención de intrusos. g. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del equipo ofertado, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. h. El equipo deberá permitir el bloqueo de vulnerabilidades y deberá incluir la protección contra ataques de denegación de servicio. i. Basado en análisis de firmas en el flujo de datos en la red, deberá permitir configurar firmas nuevas para cualquier protocolo. j. Deberá contar con las firmas necesarias para bloquear los ataques "*buffer overflow*". k. Deberá contar con las firmas necesarias para ayudar en el bloqueo de ataques *DoS*/*DDoS*. l. Deberá permitir la creación de excepciones / *hosts* exclusiones para ciertas firmas. m. Actualización automática de firmas para el detector de intrusos a través de una conexión segura. n. El equipo deberá contar con granularidad de configuración que le permita anular firmas individualmente. o. Todos los modelos de equipos deberán usar las mismas firmas. p. Deberá bloquear el tráfico malicioso de países con reputación de generar ataques.

	15. Deberá tener *VPN* que incluya lo siguiente: a. Soporte *VPN* de sitio a sitio y cliente a sitio. b. Licenciamiento mínimo de 100 *VPN* para sitio a sitio. c. Licenciamiento mínimo de 5 usuarios para cliente a sitio. d. Capacidad de realizar *IPSecVPNs*. e. Soporte para Algoritmo de Internet *Key Exchange* (*IKE*). f. Deberá soportar la configuración mínima de túneles *L2TP*. g. Deberá soportar la configuración mínima de túneles *PPTP*. h. Soporte de *VPNs* con algoritmos de cifrado: *AES*, *DES*, *3DES*. i. Se deberá soportar longitudes de llave para *AES* de 128, 192 y 256 *bits*. j. Se deberá soportar los siguientes algoritmos de integridad: *MD5*, *SHA*-1. k. Posibilidad de crear *VPN's* entre *gateways* y clientes con *IPSec*. Esto es, *VPNs IPSeC site-to-site* y *VPNs IPSec client-to-site*. l. La *VPN IPSec* deberá poder ser configurada en modo interface (*interface-mode VPN*). m. En modo interface, la *VPN IPSec* deberá poder tener asignada una dirección *IP*, tener rutas asignadas para ser ruteadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de *firewall*. n. Tanto para *IPSec* como para *L2TP* deberá soportarse los clientes terminadores de túneles nativos de *Windows*. o. Los Túneles *L2TP* y *PPTP* deberán poder manejar varios perfiles para distintos grupos de usuarios. 16. Deberá tener *URL Filtering* que incluya lo siguiente: a. El equipo deberá permitir la creación de políticas para usuarios, grupos de usuarios, *IPS*, Redes y zonas de seguridad. b. El equipo ofertado deberá ser capaz de ajustar los horarios para el funcionamiento de la política.

	c. El equipo ofertado deberá incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando qué *URL* a través de la integración con los servicios de directorio, autenticación vía *LDAP*, *Active Directory* y base de datos local. d. El equipo ofertado deberá soportar la capacidad de crear políticas basadas en el control por categoría de *URL*. e. El equipo ofertado deberá permitir el control de tráfico *URL* sin necesidad de instalar *software* cliente en los equipos para salir a Internet. f. El equipo ofertado deberá soportar la autenticación de usuarios de *Microsoft Terminal Server*, para permitir la visibilidad y el control sobre el uso de direcciones *URL* que se accede a través de estos servicios. g. Deberá permitir el crear categorías personalizadas de *URL*. h. Los registros de productos deberán incluir información detallada de las actividades de los usuarios. i. La actualización de la base de datos deberá ser automática con la opción de hacerse de forma manual. 17. Deberá tener control de aplicaciones a nivel granular que incluya lo siguiente: a. El control de aplicaciones deberá de ser una parte integral primaria del cortafuego, no como un mecanismo secundario de análisis que se base primero en puertos y luego en aplicaciones. b. Capacidad para identificar aplicaciones activas actuales (aplicaciones sociales como *Facebook, Spotify, Tuenti, Webex, Bit Torrent, Logmein, Xunlei, Circumventor, phproxy, proxono, psiphon, suresome, zelune, Freenet, Hamachi, Foldera, Ultrasurf, VNN, Pingfu, Jap, Bypass, Bypassthat, Hopster, Remobo, GMail, Megaupload, Last.Fm, Skype, Meeb*o, entre otros). c. Clasificación de tráfico a nivel de capa 7 (independientemente del puerto y del protocolo). d. Identificar, clasificar y gestionar

	sistemáticamente el tráfico desconocido. e. La solución deberá clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con dichas categorías/subcategorías (control granular dentro de la aplicación como sólo permitir *webmail* pero filtrar chat, video, mensajería instantánea). f. Aplicar técnicas de identificación de aplicaciones en todo el puerto *TCP*/*UDP* y no solo en los más comunes. g. Facilitar la visibilidad de detalles particulares de cada aplicación, como su nivel de riesgo, quién la está usando, cuánto tráfico está generando, cuáles son el origen y el destino, entre otros. h. Utilizar la identificación de la aplicación como base para las decisiones a la hora de establecer políticas de uso, permitiendo un control granular sobre el tráfico de la red. i. Habilitar controles positivos de todas las aplicaciones basándose en un amplio conjunto de criterios desde una única y centralizada tabla de políticas. j. Capacidad para identificar aplicaciones *HTTP* propietarias desarrolladas. k. Capacidad para identificar las aplicaciones bajo túneles *HTTPS* y *SSH.* l. Capacidad de crear reglas de *QoS* por aplicaciones y/o usuarios. m. *Heuristics*. En ciertos casos, las tácticas evasivas que se emplean no pueden ser identificadas, a pesar del análisis avanzado de firmas y protocolos descrito anteriormente. En estas situaciones, se necesita utilizar técnicas heurísticas adicionales, o análisis del comportamiento, para identificar ciertas aplicaciones que utilizan mecanismos de cifrado propietarios (por ejemplo aplicaciones *peer-to-peer*, de *VoIP* –como *Skype*- o de *proxies* personales –como *Ultrasurf*). Las técnicas heurísticas se emplean para ofrecer visibilidad y control sobre aplicaciones que podrían de otro

	modo eludir la identificación positiva. n. La solución deberá ser capaz no solamente de identificar las aplicaciones base, sino diferentes sub aplicaciones dentro de la misma aplicación padre, que pueden ofrecer capacidades y comportamientos diversos (por ejemplo *WebEx base* para realizar conferencias, frente a *WebEx Desktop Sharing* para compartir escritorios). o. Permite aplicarse a grupos y usuarios. 18. Deberá poder integrarse a *Microsoft Active Directory*. 19. Deberá generar reportes y poder personalizarlos, además de tener la capacidad para obtener informes de actividad por usuario: aplicaciones utilizadas, *web sites* visitados. Informes de anchos de banda utilizado por aplicación. Envío automático del informe. 20. Deberá manejar al menos *2Gbps* de *Throughput* de *VPN IPSec* (AES-128). 21. Deberá poder identificar, controlar e inspeccionar el tráfico encriptado de entrada y salida de la red (*SSL*). 22. Deberá poder filtrar archivos y datos. 23. Deberá poder habilitar aplicaciones por usuarios y grupos. 24. Deberá Implementar políticas de *QoS* (*Quality* of *Service* o calidad de servicio). 25. Deberá denegar todo el tráfico procedente de determinados países o bloquear aplicaciones no deseadas. 26. Deberá de incluir características de *Next Generation Firewall*. 27. Deberá manejar al menos 3.000.000 (tres millones) de conexiones concurrentes. 28. Deberá poder gestionar horarios de tiempo a las políticas que se les configuren. 29. Deberá poder detectar y detener *botnets* en la red. 30. Deberá tener un antivirus perimetral que proteja la red de ataques de *malware* entrantes y sitios web con *malware*.

11.5.11 Estándar para Firewall perfil 2

Especificaciones técnicas	1. El equipo ofertado deberá incluir fuente de poder interna capaz de operar en un rango de voltaje entre 100 a 240 *VAC*. 2. Deberá contener integrados al chasis o de forma modular, al menos ocho (8) puertos de interfaces 10/100/1000 *Base-T RJ45* cada uno. 3. Deberán contener puerto independiente de consola. 4. Deberán contener mínimo *4GB* de disco duro que garantice la utilización del equipo, actualizaciones y demás funciones dentro del periodo de contrato. 5. Deberán manejar un *Throughput* de *Firewall* de al menos 9 *Gbps*. 6. Deberán manejar un *Throughput* de *IPS* de al menos 3 *Gbps*. 7. Deberán de manejar al menos 50.000 (cincuenta mil) nuevas conexiones por segundo. 8. Deberán tener capacidad de manejar los siguientes protocolos de enrutamiento para *IPv4*: *OSPF* y *BGP*, así como protocolos de enrutamiento para *IPv6*. 9. Deberán contar con capacidad instalada de administración vía múltiples usuarios y múltiples niveles de privilegios. 10. Deberán soportar y gestionar el protocolo *IPv4* y *IPv6*. 11. Deberán soportar y gestionar capa 2 y capa 3 del modelo *OSI*. 12. Deberán soportar y manejar zonas de seguridad para la aplicación de políticas de seguridad. 13. El *Firewall* deberá incluir lo siguiente: a. Las reglas de *firewall* deberán analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y *VLANs*. b. Será posible definir políticas de *firewall* que sean independientes del puerto de origen y puerto de destino. c. Las reglas del *firewall* deberán tomar en

	cuenta dirección *IP* origen (que puede ser un grupo de direcciones *IP*), dirección *IP* destino (que puede ser un grupo de direcciones *IP*) y servicio (o grupo de servicios) de la comunicación que se está analizando. d. Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación. e. Deberá soportar la capacidad de definir nuevos servicios *TCP* y *UDP* que no estén contemplados en los predefinidos. f. Capacidad de hacer traslación de direcciones estático, uno a uno, *NAT*. g. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, *PAT*. h. Deberá soportar reglas de *firewall* en *IPv6* configurables tanto por *CLI* (*Command Line Interface*, Interface de línea de comando) como por *GUI* (*GraphicalUser Interface*, Interface Gráfica de Usuario). 14. Deberá tener *IPS* que incluya lo siguiente: a. Deberá apoyar las políticas de la granularidad de *IPS*, que permite la creación de diferentes políticas de seguridad de la zona, la dirección de origen, dirección de destino, y la combinación de servicios de todos estos elementos. b. Deberá ser posible crear diferentes perfiles de *IPS* para su aplicación por la zona de seguridad, dirección de origen, dirección de destino, y la combinación de servicios de todos estos elementos. c. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico *IPv6*. d. Capacidad de actualización automática de firmas *IPS* mediante tecnología de tipo "*Push*" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "*pull*" (Consultar los centros de actualización por versiones nuevas). e. El detector y preventor de intrusos deberá de

	estar orientado para la protección de redes. f. El detector y preventor de intrusos deberá estar integrado en el equipo ofertado. Sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o *software* adicional para realizar la prevención de intrusos. g. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del equipo ofertado, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. h. El equipo deberá permitir el bloqueo de vulnerabilidades y deberá incluir la protección contra ataques de denegación de servicio. i. Basado en análisis de firmas en el flujo de datos en la red, deberá permitir configurar firmas nuevas para cualquier protocolo. j. Deberá contar con las firmas necesarias para bloquear los ataques "*buffer overflow*". k. Deberá contar con las firmas necesarias para ayudar en el bloqueo de ataques *DoS* / *DDoS*. l. Deberá permitir la creación de excepciones / *hosts* exclusiones para ciertas firmas. m. Actualización automática de firmas para el detector de intrusos a través de una conexión segura. n. El equipo deberá contar con granularidad de configuración que le permita anular firmas individualmente. o. Todos los modelos de equipos deberán usar las mismas firmas. p. Deberá bloquear el tráfico malicioso de países con reputación de generar ataques. 15. Deberá tener *VPN* que incluya lo siguiente: a. Soporte *VPN* de sitio a sitio y cliente a sitio. b. Licenciamiento mínimo de 100 *VPN* para sitio a sitio. c. Licenciamiento mínimo de 5 usuarios para

	cliente a sitio. d. Capacidad de realizar *IPSecVPNs*. e. Soporte para Algoritmo de Internet *Key Exchange* (*IKE*). f. Deberá soportar la configuración mínima de túneles *L2TP*. g. Deberá soportar la configuración mínima de túneles *PPTP*. h. Soporte de *VPNs* con algoritmos de cifrado: *AES, DES, 3DES*. i. Se deberá soportar longitudes de llave para *AES* de 128, 192 y 256 bits. j. Se deberá soportar los siguientes algoritmos de integridad: *MD5*, *SHA*-1. k. Posibilidad de crear *VPN's* entre *gateways* y clientes con *IPSec*. Esto es, *VPNs IPSeC site-to-site* y *VPNs IPSec client-to-site*. l. La VPN *IPSec* deberá poder ser configurada en modo interface (*interface-mode VPN*). m. En modo interface, la *VPN IPSec* deberá poder tener asignada una dirección *IP*, tener rutas asignadas para ser ruteadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de *firewall*. n. Tanto para *IPSec* como para *L2TP* deberá soportarse los clientes terminadores de túneles nativos de *Windows*. o. Los Túneles *L2TP* y *PPTP* deberán poder manejar varios perfiles para distintos grupos de usuarios. 16. Deberá tener *URL Filtering* que incluya lo siguiente: a. El equipo deberá permitir la creación de políticas para usuarios, grupos de usuarios, *IPS*, Redes y zonas de seguridad. b. El equipo ofertado deberá ser capaz de ajustar los horarios para el funcionamiento de la política. c. El equipo ofertado deberá incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando qué *URL* a través de la integración con los servicios de directorio, autenticación vía

	LDAP, *Active Directory* y base de datos local. d. El equipo ofertado deberá soportar la capacidad de crear políticas basadas en el control por categoría de *URL*. e. El equipo ofertado deberá permitir el control de tráfico *URL* sin necesidad de instalar *software* cliente en los equipos para salir a Internet. f. El equipo ofertado deberá soportar la autenticación de usuarios de *Microsoft Terminal Server*, para permitir la visibilidad y el control sobre el uso de direcciones *URL* que se accede a través de estos servicios. g. Deberá permitir el crear categorías personalizadas de *URL*. h. Los registros de productos deberán incluir información detallada de las actividades de los usuarios. i. La actualización de la base de datos deberá ser automática con la opción de hacerse de forma manual. 17. Deberá tener control de aplicaciones a nivel granular que incluya lo siguiente: a. El control de aplicaciones deberá de ser una parte integral primaria del cortafuego, no como un mecanismo secundario de análisis que se base primero en puertos y luego en aplicaciones. b. Capacidad para identificar aplicaciones activas actuales (aplicaciones sociales como *Facebook, Spotify, Tuenti, Webex, Bit Torrent, Logmein, Xunlei, Circumventor, phproxy, proxono, psiphon, suresome, zelune, Freenet, Hamachi, Foldera, Ultrasurf, VNN, Pingfu, Jap, Bypass, Bypassthat, Hopster, Remobo, GMail, Megaupload, Last.Fm, Skype, Meebo*, entre otros). c. Clasificación de tráfico a nivel de capa 7 (independientemente del puerto y del protocolo). d. Identificar, clasificar y gestionar sistemáticamente el tráfico desconocido. e. La solución deberá clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con dichas categorías/subcategorías (control

	granular dentro de la aplicación como sólo permitir *webmail* pero filtrar chat, video, mensajería instantánea). f. Aplicar técnicas de identificación de aplicaciones en todos los puertos *TCP*/*UDP* y no solamente en los más comunes. g. Facilitar la visibilidad de detalles particulares de cada aplicación, como su nivel de riesgo, quién la está usando, cuánto tráfico está generando, cuáles son el origen y el destino, entre otros. h. Utilizar la identificación de la aplicación como base para las decisiones a la hora de establecer políticas de uso, permitiendo un control granular sobre el tráfico de la red. i. Habilitar controles positivos de todas las aplicaciones basándose en un amplio conjunto de criterios desde una única y centralizada tabla de políticas. j. Capacidad para identificar aplicaciones *HTTP* propietarias desarrolladas. k. Capacidad para identificar las aplicaciones bajo túneles *HTTPS* y *SSH* l. Capacidad de crear reglas de QoS por aplicaciones y/o usuarios. m. *Heuristics*. En ciertos casos, las tácticas evasivas que se emplean no pueden ser identificadas, a pesar del análisis avanzado de firmas y protocolos descrito anteriormente. En estas situaciones, se necesita utilizar técnicas heurísticas adicionales, o análisis del comportamiento, para identificar ciertas aplicaciones que utilizan mecanismos de cifrado propietarios (por ejemplo aplicaciones peer-to-peer, de *VoIP* –como *Skype*- o de *proxies* personales –como *Ultrasurf*). Las técnicas heurísticas se emplean para ofrecer visibilidad y control sobre aplicaciones que podrían de otro modo eludir la identificación positiva. n. La solución deberá ser capaz no solamente de identificar las aplicaciones base, sino diferentes sub aplicaciones dentro de la misma aplicación padre, que pueden ofrecer

	capacidades y comportamientos diversos (por ejemplo *WebEx base* para realizar conferencias, frente a *WebEx Desktop* Sharing para compartir escritorios). o. Permite aplicarse a grupos y usuarios. 18. Deberá poder integrarse a *Microsoft Active Directory*. 19. Deberá generar reportes y poder personalizarlos, además de tener la capacidad para obtener informes de actividad por usuario: aplicaciones utilizadas, *web sites* visitados. Informes de anchos de banda utilizado por aplicación. Envío automático del informe. 20. Deberá manejar al menos 1.5 *Gbps* de *Throughput* de *VPN IPSec* (*AES*-128). 21. Deberá poder identificar, controlar e inspeccionar el tráfico encriptado de entrada y salida de la red (*SSL*). 22. Deberá poder filtrar archivos y datos. 23. Deberá poder habilitar aplicaciones por usuarios y grupos. 24. Deberá Implementar políticas de *QoS* (*Quality of Service* o calidad de servicio). 25. Deberá denegar todo el tráfico procedente de determinados países o bloquear aplicaciones no deseadas. 26. Deberá de incluir características de *Next Generation Firewall*. 27. Deberá manejar al menos 1.200.000 (un millón doscientos mil) de conexiones concurrentes. 28. Deberá poder gestionar horarios de tiempo a las políticas que se les configuren. 29. Deberá poder detectar y detener *botnets* en la red. 30. Deberá tener un antivirus perimetral que proteja la red de ataques de *malware* entrantes y sitios web con *malware*.

11.5.12 Estándar para Firewall perfil 3

Especificaciones técnicas	1. El equipo ofertado deberá incluir fuente de poder interna capaz de operar en un rango de voltaje entre 100 a 240 *VAC*.

	2. Deberá contener integrados al chasis o de forma modular, al menos ocho (8) puertos de interfaces 10/100/1000 *Base-T RJ45* cada uno. 3. Deberán contener puerto independiente de consola. 4. Deberán contener mínimo *4GB* de disco duro que garantice la utilización del equipo, actualizaciones y demás funciones dentro del periodo de contrato. 5. Deberán manejar un *Throughput* de *Firewall* de al menos 5 *Gbps*. 6. Deberán manejar un *Throughput* de *IPS* de al menos 3 *Gbps*. 7. Deberán de manejar al menos 40.000 (cuarenta mil) nuevas conexiones por segundo. 8. Deberán tener capacidad de manejar los siguientes protocolos de enrutamiento para *IPv4: OSPF y BGP*, así como protocolos de enrutamiento para *IPv6*. 9. Deberán contar con capacidad instalada de administración vía múltiples usuarios y múltiples niveles de privilegios. 10. Deberán soportar y gestionar el protocolo *IPv4* y *IPv6*. 11. Deberán soportar y gestionar capa 2 y capa 3 del modelo *OSI*. 12. Deberán soportar y manejar zonas de seguridad para la aplicación de políticas de seguridad. 13. El *Firewall* deberá incluir lo siguiente: a. Las reglas de *firewall* deberán analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y *VLANs*. b. Será posible definir políticas de *firewall* que sean independientes del puerto de origen y puerto de destino. c. Las reglas del *firewall* deberán tomar en cuenta dirección *IP* origen (que puede ser un grupo de direcciones *IP*), dirección *IP* destino (que puede ser un grupo de direcciones *IP*) y servicio (o grupo de servicios) de la comunicación que se está analizando.

	d. Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación. e. Deberá soportar la capacidad de definir nuevos servicios *TCP* y *UDP* que no estén contemplados en los predefinidos. f. Capacidad de hacer traslación de direcciones estático, uno a uno, *NAT*. g. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, *PAT*. h. Deberá soportar reglas de *firewall* en *IPv6* configurables tanto por *CLI* (*Command Line Interface*, Interface de línea de comando) como por *GUI* (*GraphicalUser* Interface, Interface Gráfica de Usuario). 14. Deberá tener *IPS* que incluya lo siguiente: i. Deberá apoyar las políticas de la granularidad de *IPS*, que permite la creación de diferentes políticas de seguridad de la zona, la dirección de origen, dirección de destino, y la combinación de servicios de todos estos elementos. j. Deberá ser posible crear diferentes perfiles de *IPS* para su aplicación por la zona de seguridad, dirección de origen, dirección de destino, y la combinación de servicios de todos estos elementos. k. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico *IPv6*. l. Capacidad de actualización automática de firmas *IPS* mediante tecnología de tipo "*Push*" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "*pull*" (Consultar los centros de actualización por versiones nuevas). m. El detector y preventor de intrusos deberá de estar orientado para la protección de redes. n. El detector y preventor de intrusos deberá estar integrado en el equipo ofertado. Sin

	necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o *software* adicional para realizar la prevención de intrusos. o. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del equipo ofertado, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. p. El equipo deberá permitir el bloqueo de vulnerabilidades y deberá incluir la protección contra ataques de denegación de servicio. q. Basado en análisis de firmas en el flujo de datos en la red, deberá permitir configurar firmas nuevas para cualquier protocolo. r. Deberá contar con las firmas necesarias para bloquear los ataques "*buffer overflow*". s. Deberá contar con las firmas necesarias para ayudar en el bloqueo de ataques *DoS*/*DDoS*. t. Deberá permitir la creación de excepciones/*hosts* exclusiones para ciertas firmas. u. Actualización automática de firmas para el detector de intrusos a través de una conexión segura. v. El equipo deberá contar con granularidad de configuración que le permita anular firmas individualmente. w. Todos los modelos de equipos deberán usar las mismas firmas. x. Deberá bloquear el tráfico malicioso de países con reputación de generar ataques. 15. Deberá tener *VPN* que incluya lo siguiente: a. Soporte *VPN* de sitio a sitio y cliente a sitio. b. Licenciamiento mínimo de 100 *VPN* para sitio a sitio. c. Licenciamiento mínimo de 5 usuarios

	para cliente a sitio. d. Capacidad de realizar *IPSecVPNs*. e. Soporte para Algoritmo de Internet *Key Exchange* (*IKE*). f. Deberá soportar la configuración mínima de túneles *L2TP*. g. Deberá soportar la configuración mínima de túneles *PPTP*. h. Soporte de *VPNs* con algoritmos de cifrado: *AES, DES, 3DES*. i. Se deberá soportar longitudes de llave para *AES* de 128, 192 y 256 bits. j. Se deberá soportar los siguientes algoritmos de integridad: *MD5*, *SHA*-1. k. Posibilidad de crear *VPN's* entre *gateways* y clientes con *IPSec*. Esto es, *VPNs IPSeC site-to-site* y *VPNs IPSec client-to-site*. l. La *VPN IPSec* deberá poder ser configurada en modo interface (*interface-mode VPN*). m. En modo interface, la *VPN IPSec* deberá poder tener asignada una dirección *IP*, tener rutas asignadas para ser ruteadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de *firewall*. n. Tanto para *IPSec* como para *L2TP* deberá soportarse los clientes terminadores de túneles nativos de *Windows*. o. Los Túneles *L2TP* y *PPTP* deberán poder manejar varios perfiles para distintos grupos de usuarios. 16. Deberá tener *URL Filtering* que incluya lo siguiente: a. El equipo deberá permitir la creación de políticas para usuarios, grupos de usuarios, *IPS*, Redes y zonas de seguridad. b. El equipo ofertado deberá ser capaz de ajustar los horarios para el funcionamiento de la política. c. El equipo ofertado deberá incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está

	usando qué *URL* a través de la integración con los servicios de directorio, autenticación vía *LDAP*, *Active Directory* y base de datos local. d. El equipo ofertado deberá soportar la capacidad de crear políticas basadas en el control por categoría de *URL*. e. El equipo ofertado deberá permitir el control de tráfico *URL* sin necesidad de instalar *software* cliente en los equipos para salir a Internet. f. El equipo ofertado deberá soportar la autenticación de usuarios de *Microsoft Terminal Server*, para permitir la visibilidad y el control sobre el uso de direcciones *URL* que se accede a través de estos servicios. g. Deberá permitir el crear categorías personalizadas de *URL*. h. Los registros de productos deberán incluir información detallada de las actividades de los usuarios. i. La actualización de la base de datos deberá ser automática con la opción de hacerse de forma manual. 17. Deberá tener control de aplicaciones a nivel granular que incluya lo siguiente: a. El control de aplicaciones deberá de ser una parte integral primaria del cortafuego, no como un mecanismo secundario de análisis que se base primero en puertos y luego en aplicaciones. b. Capacidad para identificar aplicaciones activas actuales (aplicaciones sociales como *Facebook, Spotify, Tuenti, Webex, Bit Torrent, Logmein, Xunlei, Circumventor, phproxy, proxono, psiphon, suresome, zelune, Freenet, Hamachi, Foldera, Ultrasurf, VNN, Pingfu, Jap, Bypass, Bypassthat, Hopster, Remobo, GMail, Megaupload, Last.Fm, Skype, Meebo*, entre otros). c. Clasificación de tráfico a nivel de capa 7 (independientemente del puerto y del protocolo). d. Identificar, clasificar y gestionar

	sistemáticamente el tráfico desconocido. e. La solución deberá clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con dichas categorías/subcategorías (control granular dentro de la aplicación como sólo permitir *webmail* pero filtrar chat, video, mensajería instantánea). f. Aplicar técnicas de identificación de aplicaciones en todo el puerto *TCP*/*UDP* y no solo en los más comunes. g. Facilitar la visibilidad de detalles particulares de cada aplicación, como su nivel de riesgo, quién la está usando, cuánto tráfico está generando, cuáles son el origen y el destino, entre otros. h. Utilizar la identificación de la aplicación como base para las decisiones a la hora de establecer políticas de uso, permitiendo un control granular sobre el tráfico de la red. i. Habilitar controles positivos de todas las aplicaciones basándose en un amplio conjunto de criterios desde una única y centralizada tabla de políticas. j. Capacidad para identificar aplicaciones *HTTP* propietarias desarrolladas. k. Capacidad para identificar las aplicaciones bajo túneles *HTTPS* y *SSH*. l. Capacidad de crear reglas de *QoS* por aplicaciones y/o usuarios. m. *Heuristics*. En ciertos casos, las tácticas evasivas que se emplean no pueden ser identificadas, a pesar del análisis avanzado de firmas y protocolos descrito anteriormente. En estas situaciones, se necesita utilizar técnicas heurísticas adicionales, o análisis del comportamiento, para identificar ciertas aplicaciones que utilizan mecanismos de cifrado propietarios (por ejemplo aplicaciones *peer-to-peer*, de *VoIP* –como *Skype*- o de *proxies* personales –como

	Ultrasurf). Las técnicas heurísticas se emplean para ofrecer visibilidad y control sobre aplicaciones que podrían de otro modo eludir la identificación positiva. n. La solución deberá ser capaz no solamente de identificar las aplicaciones base, sino diferentes sub aplicaciones dentro de la misma aplicación padre, que pueden ofrecer capacidades y comportamientos diversos (por ejemplo *WebEx base* para realizar conferencias, frente a *WebEx Desktop Sharing* para compartir escritorios). o. Permite aplicarse a grupos y usuarios. 18. Deberá poder integrarse a *Microsoft Active Directory*. 19. Deberá generar reportes y poder personalizarlos, además de tener la capacidad para obtener informes de actividad por usuario: aplicaciones utilizadas, *web sites* visitados. Informes de anchos de banda utilizado por aplicación. Envío automático del informe. 20. Deberá manejar al menos 1.2Gbps de Throug*h*put de *VPN IPSec* (AES-128). 21. Deberá poder identificar, controlar e inspeccionar el tráfico encriptado de entrada y salida de la red (*SSL*). 22. Deberá poder filtrar archivos y datos. 23. Deberá poder habilitar aplicaciones por usuarios y grupos. 24. Deberá Implementar políticas de *QoS* (*Quality of Service* o calidad de servicio). 25. Deberá denegar todo el tráfico procedente de determinados países o bloquear aplicaciones no deseadas. 26. Deberá de incluir características de *Next Generation Firewall*. 27. Deberá manejar al menos 1.200.000 (un millón doscientos mil) de conexiones concurrentes. 28. Deberá poder gestionar horarios de tiempo a las políticas que se les configuren. 29. Deberá poder detectar y detener *botnets* en la red. 30. Deberá tener un antivirus perimetral que

	proteja la red de ataques de *malware* entrantes y sitios web con *malware*.

11.5.13 Estándar para Firewall perfil 4

Especificaciones técnicas	1. El equipo ofertado deberá incluir fuente de poder interna capaz de operar en un rango de voltaje entre 100 a 240 *VAC*. 2. Deberá contener integrados al chasis o de forma modular, al menos seis (6) puertos de interfaces 10/100/1000 *Base-T RJ45* cada uno. 3. Deberán contener puerto independiente de consola. 4. Deberán contener mínimo *4GB* de disco duro que garantice la utilización del equipo, actualizaciones y demás funciones dentro del periodo de contrato. 5. Deberán manejar un *Throughput* de *Firewall* de al menos 3 *Gbps*. 6. Deberán manejar un *Throughput* de *IPS* de al menos 700 *Mbps*. 7. Deberán de manejar al menos 15.000 (quince mil) nuevas conexiones por segundo. 8. Deberán tener capacidad de manejar los siguientes protocolos de enrutamiento para *IPv4*: *OSPF* y *BGP*, así como protocolos de enrutamiento para *IPv6*. 9. Deberán contar con capacidad instalada de administración vía múltiples usuarios y múltiples niveles de privilegios. 10. Deberán soportar y gestionar el protocolo *IPv4* y *IPv6*. 11. Deberán soportar y gestionar capa 2 y capa 3 del modelo *OSI*. 12. Deberán soportar y manejar zonas de seguridad para la aplicación de políticas de seguridad. 13. El *Firewall* deberá incluir lo siguiente: a. Las reglas de *firewall* deberán analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y *VLANs*. b. Será posible definir políticas de *firewall* que

	sean independientes del puerto de origen y puerto de destino. c. Las reglas del *firewall* deberán tomar en cuenta dirección *IP* origen (que puede ser un grupo de direcciones *IP*), dirección *IP* destino (que puede ser un grupo de direcciones *IP*) y servicio (o grupo de servicios) de la comunicación que se está analizando. d. Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación. e. Deberá soportar la capacidad de definir nuevos servicios *TCP* y *UDP* que no estén contemplados en los predefinidos. f. Capacidad de hacer traslación de direcciones estático, uno a uno, *NAT*. g. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, *PAT*. h. Deberá soportar reglas de *firewall* en *IPv6* configurables tanto por *CLI* (*Command Line Interface*, Interface de línea de comando) como por *GUI* (*GraphicalUser* Interface, Interface Gráfica de Usuario). 14. Deberá tener *IPS* que incluya lo siguiente: a. Deberá apoyar las políticas de la granularidad de *IPS*, que permite la creación de diferentes políticas de seguridad de la zona, la dirección de origen, dirección de destino, y la combinación de servicios de todos estos elementos. b. Deberá ser posible crear diferentes perfiles de *IPS* para su aplicación por la zona de seguridad, dirección de origen, dirección de destino, y la combinación de servicios de todos estos elementos. c. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico *IPv6*. d. Capacidad de actualización automática de firmas *IPS* mediante tecnología de tipo "*Push*" (permitir recibir las actualizaciones cuando los centros de actualización

	envíen notificaciones sin programación previa), adicional a tecnologías tipo "*pull*" (Consultar los centros de actualización por versiones nuevas). e. El detector y preventor de intrusos deberá de estar orientado para la protección de redes. f. El detector y preventor de intrusos deberá estar integrado en el equipo ofertado. Sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o *software* adicional para realizar la prevención de intrusos. g. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del equipo ofertado, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. h. El equipo deberá permitir el bloqueo de vulnerabilidades y deberá incluir la protección contra ataques de denegación de servicio. i. Basado en análisis de firmas en el flujo de datos en la red, deberá permitir configurar firmas nuevas para cualquier protocolo. j. Deberá contar con las firmas necesarias para bloquear los ataques "*buffer overflow*". k. Deberá contar con las firmas necesarias para ayudar en el bloqueo de ataques *DoS*/*DDoS*. l. Deberá permitir la creación de excepciones/*hosts* exclusiones para ciertas firmas. m. Actualización automática de firmas para el detector de intrusos a través de una conexión segura. n. El equipo deberá contar con granularidad de configuración que le permita anular

	firmas individualmente. o. Todos los modelos de equipos deberán usar las mismas firmas. p. Deberá bloquear el tráfico malicioso de países con reputación de generar ataques. 15. Deberá tener *VPN* que incluya lo siguiente: a. Soporte *VPN* de sitio a sitio y cliente a sitio. b. Licenciamiento mínimo de 5 *VPN* para sitio a sitio. c. Licenciamiento mínimo de 5 usuarios para cliente a sitio. d. Capacidad de realizar *IPSecVPNs*. e. Soporte para Algoritmo de Internet *Key Exchange* (*IKE*). f. Deberá soportar la configuración mínima de túneles *L2TP*. g. Deberá soportar la configuración mínima de túneles *PPTP*. h. Soporte de *VPNs* con algoritmos de cifrado: *AES, DES, 3DES*. i. Se deberá soportar longitudes de llave para *AES* de 128, 192 y 256 *bits*. j. Se deberá soportar los siguientes algoritmos de integridad: *MD5*, *SHA*-1. k. Posibilidad de crear *VPN's* entre *gateways* y clientes con *IPSec*. Esto es, *VPNs IPSeC site-to-site* y *VPNs IPSec client-to-site*. l. La VPN *IPSec* deberá poder ser configurada en modo interface (*interface-mode VPN*). m. En modo interface, la *VPN IPSec* deberá poder tener asignada una dirección *IP*, tener rutas asignadas para ser ruteadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de *firewall*. n. Tanto para *IPSec* como para *L2TP* deberá soportarse los clientes terminadores de túneles nativos de *Windows*. o. Los Túneles *L2TP* y *PPTP* deberán poder manejar varios perfiles para distintos grupos de usuarios.

	16. Deberá tener *URL Filtering* que incluya lo siguiente: a. El equipo deberá permitir la creación de políticas para usuarios, grupos de usuarios, *IPS*, Redes y zonas de seguridad. b. El equipo ofertado deberá ser capaz de ajustar los horarios para el funcionamiento de la política. c. El equipo ofertado deberá incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando qué *URL* a través de la integración con los servicios de directorio, autenticación vía *LDAP*, *Active Directory* y base de datos local. d. El equipo ofertado deberá soportar la capacidad de crear políticas basadas en el control por categoría de *URL*. e. El equipo ofertado deberá permitir el control de tráfico *URL* sin necesidad de instalar *software* cliente en los equipos para salir a Internet. f. El equipo ofertado deberá soportar la autenticación de usuarios de *Microsoft Terminal Server*, para permitir la visibilidad y el control sobre el uso de direcciones *URL* que se accede a través de estos servicios. g. Deberá permitir el crear categorías personalizadas de *URL*. h. Los registros de productos deberán incluir información detallada de las actividades de los usuarios. i. La actualización de la base de datos deberá ser automática con la opción de hacerse de forma manual. 17. Deberá tener control de aplicaciones a nivel granular que incluya lo siguiente: a. El control de aplicaciones deberá de ser una parte integral primaria del cortafuego, no como un mecanismo secundario de análisis que se base primero en puertos y luego en aplicaciones.

	b. Capacidad para identificar aplicaciones activas actuales (aplicaciones sociales como *Facebook, Spotify, Tuenti, Webex, Bit Torrent, Logmein, Xunlei, Circumventor, phproxy, proxono, psiphon, suresome, zelune, Freenet, Hamachi, Foldera, Ultrasurf, VNN, Pingfu, Jap, Bypass, Bypassthat, Hopster, Remobo, GMail, Megaupload, Last.Fm, Skype, Meebo*, entre otros). c. Clasificación de tráfico a nivel de capa 7 (independientemente del puerto y del protocolo). d. Identificar, clasificar y gestionar sistemáticamente el tráfico desconocido. e. La solución deberá clasificar las aplicaciones en diferentes categorías y subcategorías, para poder aplicar reglas de acuerdo con dichas categorías/subcategorías (control granular dentro de la aplicación como sólo permitir *webmail* pero filtrar chat, video, mensajería instantánea). f. Aplicar técnicas de identificación de aplicaciones en todo el puerto *TCP*/*UDP* y no solo en los más comunes. g. Facilitar la visibilidad de detalles particulares de cada aplicación, como su nivel de riesgo, quién la está usando, cuánto tráfico está generando, cuáles son el origen y el destino, entre otros. h. Utilizar la identificación de la aplicación como base para las decisiones a la hora de establecer políticas de uso, permitiendo un control granular sobre el tráfico de la red. i. Habilitar controles positivos de todas las aplicaciones basándose en un amplio conjunto de criterios desde una única y centralizada tabla de políticas. j. Capacidad para identificar aplicaciones *HTTP* propietarias desarrolladas. k. Capacidad para identificar las aplicaciones bajo túneles *HTTPS* y *SSH*. l. Capacidad de crear reglas de *QoS* por aplicaciones y/o usuarios.

	m. *Heuristics*. En ciertos casos, las tácticas evasivas que se emplean no pueden ser identificadas, a pesar del análisis avanzado de firmas y protocolos descrito anteriormente. En estas situaciones, se necesita utilizar técnicas heurísticas adicionales, o análisis del comportamiento, para identificar ciertas aplicaciones que utilizan mecanismos de cifrado propietarios (por ejemplo aplicaciones *peer-to-peer*, de *VoIP* –como *Skype*- o de *proxies* personales –como *Ultrasurf*). Las técnicas heurísticas se emplean para ofrecer visibilidad y control sobre aplicaciones que podrían de otro modo eludir la identificación positiva. n. La solución deberá ser capaz no solamente de identificar las aplicaciones base, sino diferentes sub aplicaciones dentro de la misma aplicación padre, que pueden ofrecer capacidades y comportamientos diversos (por ejemplo *WebEx base* para realizar conferencias, frente a W*e*bEx De*s*ktop *Sharing* para compartir escritorios). o. Permite aplicarse a grupos y usuarios. 18. Deberá poder integrarse a *Microsoft Active Directory*. 19. Deberá generar reportes y poder personalizarlos, además de tener la capacidad para obtener informes de actividad por usuario: aplicaciones utilizadas, *web sites* visitados. Informes de anchos de banda utilizado por aplicación. Envío automático del informe. 20. Deberá manejar al menos 400 *Mbps* de *Throughput* de *VPN IPSec* (AES-128). 21. Deberá poder identificar, controlar e inspeccionar el tráfico encriptado de entrada y salida de la red (*SSL*). 22. Deberá poder filtrar archivos y datos. 23. Deberá poder habilitar aplicaciones por usuarios y grupos. 24. Deberá Implementar políticas de *QoS* (*Quality* of *Service* o calidad de servicio).

	25. Deberá denegar todo el tráfico procedente de determinados países o bloquear aplicaciones no deseadas. 26. Deberá de incluir características de *Next Generation Firewall*. 27. Deberá manejar al menos 1.200.000 (un millón doscientos mil) de conexiones concurrentes. 28. Deberá soportar *Point-to-Point Protocol over Ethernet* (*PPPoE*). 29. Deberá soportar al menos 120 usuarios. 30. Deberá poder gestionar horarios de tiempo a las políticas que se les configuren. 31. Deberá poder detectar y detener *botnets* en la red. 32. Deberá tener un antivirus perimetral que proteja la red de ataques de *malware* entrantes y sitios web con *malware*.

11.5.14 Estándar para consola de administración para los Firewall

Especificaciones técnicas	1. Deberá poder agrupar los dispositivos de la plataforma de seguridad. 2. Deberá poder gestionar plantillas de configuración para todos los dispositivos de la plataforma de seguridad. 3. Deberá poder gestionar usuarios por privilegios, ej: Administrador, Visor, entre otros. 4. Deberá poder generar informes de distintos tipos para cualquier dispositivo de la plataforma de seguridad. 5. Deberá poder administrar todos los dispositivos que conforman la plataforma de seguridad para poder enviar políticas, configuraciones, entre otras. 6. Deberá identificar los eventos de seguridad críticos en líneas de tiempo, gráficos y mapas. 7. Deberá ver los estados de rendimiento como *CPU*, Memoria *RAM*, espacio en disco de los equipos así como los fallos presentados en el *hardware* de toda la plataforma de seguridad. 8. Deberá poder generar informes automáticamente en días programados y enviarlos a cuentas de correo.

	9. Deberá poder ver en tiempo real el tráfico de red detallado para análisis y seguimiento. 10. La consola deberá ser *appliance* o un *software* que se instale en un servidor con las características optimas de *hardware* recomendadas por el fabricante y que soporte toda la plataforma de seguridad, además deberá proveer todo el *hardware*, *software* y licenciamiento necesario para la consola. En caso que la consola sea *software* deberá estar soportado en un servidor de montaje en *rack*. 11. La consola deberá tener un almacenamiento mínimo de 4.*2TB* (*terabyte*).

11.5.15 Infraestructura

Se refiere a todo el equipo pasivo que conforma la base principal y medios físicos de trasmisión de datos, así como otros componentes y accesorios de red requeridos para la correcta operación de la red de datos, los cuales deberán analizarse con el propósito de ajustarlos a los requerimientos de red. Entre estos están:

a) **Topología de la red:** Determinación y diseño de la topología de red que presente la mejor solución a los requerimientos y servicios de red planteados.

b) **Cables UTP y Fibra Óptica:** Selección del tipo de cable y su categoría, siguiendo las normas de cableado estructurado establecidas por la *IEEE*, en su estándar *ANSI*/*TIA*/*EIA-568-B*.

c) **Gabinetes de pared o Racks de piso:** Tamaño y tipo de gabinete con sus accesorios de red: organizadores, regletas, *UPS*, entre otros. De acuerdo a los lineamientos del estándar *ANSI*/*TIA*/*EIA-568-B* para cableado estructurado.

d) **Instalaciones eléctricas:** Determinación del estado de la instalación eléctrica, para asegurarse que este cumpla con las normas del código eléctrico nacional y cuenta con las características de calidad y seguridad, que garanticen el buen desempeño de los equipos.

e) **Conectores de red:** Selección del tipo de conectores y elementos de red para la determinación de la mejor configuración de la red, siguiendo los lineamientos establecidos por el estándar *ANSI*/*TIA*/*EIA-568-B* para cableado estructurado.

11.5.16 Centros de procesamiento de datos:

Los centros de datos donde se hospeda todo el equipo de cómputo dedicado a la prestación de servicios de la red institucional y la ejecución de procesos, deberán contar con al menos una serie de regulaciones mínimas para el establecimiento de un ambiente de operación adecuado:

a) **Área de operación**: Deberá asegurarse la disponibilidad de un espacio amplio y adecuado para la manipulación del equipo de cómputo, así como de los insumos y mecanismos para un seguro y ágil manejo de estos, disminuyendo el riesgo de causar un daño y sufrir una lesión.

b) **Sistema eléctrico:** Debe existir un circuito eléctrico independiente de cualquier otro circuito y dedicado exclusivamente para la conexión de equipo eléctrico sensible. Este debe contar con sus propios tableros y medidor si es posible. Su capacidad deberá dimensionarse de acuerdo con la estimación de consumo del equipo a instalar en el sitio.

c) **Sistema de enfriamiento:** El centro de datos deberá contar con un sistema de enfriamiento de precisión, de alta disponibilidad y tolerancia a fallos, que permita medir la temperatura y humedad relativa; y realizar notificaciones de alarmas remotas vía correo o *sms*.

d) **Cableado estructurado:** Dentro del centro de datos, todos los componentes pasivos de la red deberán acatar los estándares definidos por la *IEEE* en la norma *ANSI*/*TIA*/*EIA*/*568* para cableado estructurado.

e) **Sistema de detección y supresión de incendio:** Deberá asegurarse que exista un sistema de detección y supresión de incendio que utilice un agente supresor no dañino para el equipo ni para el ambiente; con controles de operación automáticos y manuales, así como capacidad de reportar alertas vía *email* y *sms*.

f) **Sistema de respaldo eléctrico:** El centro de procesamiento de datos deberá estar provisto con unidades de potencia interrumpida, en caso de falla eléctrica y con conexión a una planta eléctrica que garantice la continuidad del fluido eléctrico sin dependencia del proveedor externo. La capacidad de la planta eléctrica y las *UPS*, deberán calcularse en función de la densidad de consumo del equipo colocado y considerando aspectos de crecimiento y escalabilidad. Además, debe permitir la notificación de alertas vía *email* o *sms*.

g) **Sistema de monitoreo y seguridad:** El centro de datos deberá contar con mecanismos de control para el ingreso y manipulación de los equipos, desde listas de control de acceso hasta cámaras de vigilancia, tarjetas de identidad y claves de acceso. Además, debe tener la capacidad para notificar incidencias vía *email* o *sms*.

11.6 Estándares para la adquisición de licenciamiento base para equipo de cómputo y servidores

La determinación del licenciamiento base para el equipo de cómputo y servidores, obedecerá a los requerimientos técnicos y/o procesos a soportar.

La Dirección de Informática de Gestión dará soporte técnico exclusivamente a aquel *software* que haya sido adquirido formalmente por la Administración para el desarrollo de una actividad vinculante con los objetivos institucionales. Adicionalmente, se debe prever que al realizar la adquisición de equipos de cómputo por medio de la modalidad de arrendamiento, debe garantizarse que estos cuenten con sus licencias incorporadas.

a) **Modalidades de licenciamiento:** Para toda adquisición de *software*, la modalidad de licenciamiento debe determinarse en función de una estimación de usuarios potenciales de la aplicación y ésta deberá permitir su crecimiento en el tiempo, de acuerdo con las características de demanda asociadas a los procesos soportados por dicho licenciamiento.

b) **Sistemas operativos para equipo de cómputo:** La definición de las especificaciones del licenciamiento para las terminales de trabajo, estará sujeta a los requerimientos técnicos suministrados por los usuarios finales.

   La Dirección de Informática de Gestión determinará la viabilidad técnica de los requerimientos, con el propósito de establecer los parámetros de adquisición que mejor se ajusten a estas necesidades, permitiendo hacer un uso óptimo y eficiente de las tecnologías de información y satisfaciendo las necesidades implicadas.

c) **Sistemas operativos para servidores:** La definición de las especificaciones del licenciamiento para servidores, estará sujeta a los requerimientos técnicos analizados por los profesionales a cargo del proceso de adquisición tecnológica. Estos deberán ser el resultado de una investigación previa que garantice la solución más óptima a la necesidad planteada, haciendo un uso racional de las tecnologías de punta.

d) **Software *suite* para oficina:** Deben automatizar, optimizar y mejorar las tareas diarias de los funcionarios en pro de lograr los objetivos institucionales. Éstas deberán contar con características de compatibilidad entre los formatos de archivos más comunes, permitiendo al usuario hacer un uso amigable y sencillo de sus propiedades. Además, debe poder interactuar correctamente con otros recursos (*software* y/o *hardware*). Entre sus aplicativos deberán encontrarse al menos los siguientes elementos:

   a. Procesadores de textos.

   b. Hojas de cálculo.

   c. Administradores de imágenes.

d. Administradores de presentaciones.
e. Diagramadores.
f. Planificadores de tareas.

e) **Herramientas para administración de bases de datos**: Debe permitir la creación, mantenimiento y uso de las bases de datos de la Institución y de sus usuarios finales.

La definición de sus especificaciones debe ser resultado de un análisis de requerimientos, que permita comprobar cuál es la mejor solución posible a las necesidades planteadas, haciendo un uso racional de la tecnología de punta existente en el mercado. Ésta debe operar e interactuar en las múltiples plataformas de *hardware* y *software* con que cuenta el Ministerio.

f) **Herramientas para desarrollo de software:** Debe permitir diseñar, crear, depurar, gestionar y brindar mantenimiento al *software* desarrollado. La definición de sus especificaciones debe ser resultado de un análisis de requerimientos, que permita comprobar cuál es la mejor solución posible a las necesidades planteadas, haciendo un uso racional de la tecnología de punta existente en el mercado. Ésta debe operar e interactuar en las múltiples plataformas de *hardware* y *software* con que cuenta el Ministerio.

g) **Herramientas para la administración de redes:** Debe permitir la administración de redes y del dominio, correos, monitoreo de equipos, así como otros aspectos relacionados al área de redes e infraestructura.

Deberán contar con características técnicas determinadas, esto en función de la plataforma tecnológica existente en la Institución. Permitiendo el mayor nivel de integración y compatibilidad multiplataforma, en procura que su implementación y uso satisfaga las necesidades inicialmente planteadas; y haciendo uso siempre de la tecnología de punta en una forma racional.

h) **Software especializado:** Es todo aquel *software* destinado a un grupo específico de usuarios y/o para cubrir una necesidad específica.

Su justificación deberá estar respaldada en un análisis de requerimientos sobre la necesidad de la población involucrada, un análisis técnico sobre las alternativas de solución y un análisis sobre la factibilidad económica para la implementación de las soluciones técnicamente posibles. Deberá considerarse la utilización de la mejor tecnología que permita solventar de manera eficiente el requerimiento. Cabe indicar, que siempre deberán considerarse los aspectos de soporte y escalabilidad del producto.

11.7 Estándar para las Bases de Datos

El Departamento de Base de Datos y Seguridad cuenta con un Manual de estándares para la nomenclatura de los objetos de base de datos, el cual se encuentra en la siguiente dirección: \\dominiomep\compartidas\Manuales y Estandares\Vigente\Manuales.

11.8 Estándar para el proceso institucional de desarrollo y mantenimiento de Software

El Departamento de Sistemas de Información cuenta con un estándar que es una guía de cumplimiento en el desarrollo de sistemas o aplicaciones informáticas. Este es utilizado por los funcionarios de la Dirección de Informática de Gestión y empresas desarrolladoras que sean contratados para realizar un sistema específico. Este estándar se encuentra en la siguiente dirección: \\dominiomep\compartidas\Manuales y Estandares\Vigente\Manuales.

11.9 Estándar documental

La Dirección de Informática de Gestión cuenta con un Manual de Estándares para Documentación, el cual está basado en el cumplimiento del estándar *ISO/TR10013* “Directrices para la documentación de sistemas de gestión de la calidad” y a estándares internos como el Manual de Gestión documental de Archivo Central. Esto con el objetivo de definir la estructura, forma, contenido o el método de presentación de la documentación del sistema de gestión de la calidad de la DIG. Este estándar se encuentra en la siguiente dirección: \\dominiomep\compartidas\Manuales y Estandares\Vigente\Manuales.

12 FIRMAS

---------- INTENCIONALMENTE DEJADO EN BLANCO ----------

MINISTERIO DE EDUCACIÓN PÚBLICA
DIRECCIÓN DE INFORMÁTICA DE GESTIÓN

HOJA DE REVISIÓN Y ACEPTACIÓN
MANUAL DE ESTÁNDARES INFORMÁTICOS

CÓDIGO: DVM-A-DIG-MAN-08

ACTUALIZADO POR:

NOMBRE	FIRMA
Jenny Navarro Blanco	JENNY MARIA NAVARRO BLANCO (FIRMA) Firmado digitalmente por JENNY MARIA NAVARRO BLANCO (FIRMA) Fecha: 2021.10.15 14:25:45 -06'00'
Ana Chacón Guevara	ANA MELIDA CHACON GUEVARA (FIRMA) Firmado digitalmente por ANA MELIDA CHACON GUEVARA (FIRMA) Fecha: 2021.10.19 15:52:24 -06'00'
German Peraza Castro	GERMAN ALBERTO PERAZA CASTRO (FIRMA) Firmado digitalmente por GERMAN ALBERTO PERAZA CASTRO (FIRMA) Fecha: 2021.10.18 14:03:32 -06'00'
Ronny Rojas Vargas	RONNY GERARDO ROJAS VARGAS (FIRMA) Firmado digitalmente por RONNY GERARDO ROJAS VARGAS (FIRMA) Fecha: 2021.10.18 14:22:36 -06'00'
Tahyli Mondragón Fonseca	TAHYLI MONDRAGON FONSECA (FIRMA) Firmado digitalmente por TAHYLI MONDRAGON FONSECA (FIRMA) Fecha: 2021.10.15 14:57:18 -06'00'
Marlon Vásquez Vásquez	MARLON ALEXANDER VASQUEZ VASQUEZ (FIRMA) Firmado digitalmente por MARLON ALEXANDER VASQUEZ VASQUEZ (FIRMA) Fecha: 2021.10.18 15:31:42 -06'00'
Máximo Varela Castro	MAXIMO VARELA CASTRO (FIRMA) Firmado digitalmente por MAXIMO VARELA CASTRO (FIRMA) Fecha: 2021.10.18 09:39:54 -06'00'
Ana Marcela Barrantes Arias	ANA MARCELA BARRANTES ARIAS (FIRMA) Firmado digitalmente por ANA MARCELA BARRANTES ARIAS (FIRMA) Fecha: 2021.10.15 14:00:54 -06'00'

FECHA: **Noviembre, 2021**

MINISTERIO DE EDUCACIÓN PÚBLICA
DIRECCIÓN DE INFORMÁTICA DE GESTIÓN

HOJA DE REVISIÓN Y ACEPTACIÓN
MANUAL DE ESTÁNDARES INFORMÁTICOS

CÓDIGO: DVM-A-DIG-MAN-08

REVISADO POR:	
Jenny Navarro Blanco	JENNY MARIA NAVARRO BLANCO (FIRMA) Firmado digitalmente por JENNY MARIA NAVARRO BLANCO (FIRMA) Fecha: 2021.10.15 14:26:18 -06'00'
Gabriel Dennis Dennis	Gabriel Denis Denis Firmado digitalmente por Gabriel Denis Denis Fecha: 2021.10.22 13:53:43 -06'00'
Berny Salazar Rojas	BERNI SALAZAR ROJAS (FIRMA) Firmado digitalmente por BERNI SALAZAR ROJAS (FIRMA) Fecha: 2021.10.21 11:48:30 -06'00'
John Mehlbaum Ucañan	JOHN ALBERTO MEHLBAUM UCAÑAN (FIRMA) Firmado digitalmente por JOHN ALBERTO MEHLBAUM UCAÑAN (FIRMA) Fecha: 2021.10.22 11:26:37 -06'00'
Stephanie Carvajal Miranda	STEPHANIE CARVAJAL MIRANDA (FIRMA) Firmado digitalmente por STEPHANIE CARVAJAL MIRANDA (FIRMA) Fecha: 2021.10.25 10:04:57 -06'00'
Kattia Paniagua Alfaro	KATTIA MARCELA PANIAGUA ALFARO (FIRMA) Fecha: 2021.10.20 10:46:56 -06'00'
NOMBRE	FIRMA
APROBADO POR:	
José Sandí Zúñiga	JOSE MANUEL SANDI ZUÑIGA (FIRMA) Firmado digitalmente por JOSE MANUEL SANDI ZUÑIGA (FIRMA) Fecha: 2021.10.25 11:54:19 -06'00'
NOMBRE	FIRMA

FECHA: **Noviembre, 2021**