ANEXO ESPECIFICACIONES TÉCNICAS CONECTIVIDAD UCUNDINAMARCA 2021
NECESIDADES Y ESPECIFICACIONES TÉCNICAS AL PROYECTO: "SERVICIO DE CONECTIVIDAD HIBRIDA POR MEDIO DE SD-WAN Y MPLS, INTERNET DEDICADO, COLOCATION Y SEGURIDAD PERIMETRAL EN ALTA DISPONIBILIDAD CENTRALIZADA EN DATA CENTER PARA LA UNIVERSIDAD DE CUNDINAMARCA"

Actualmente, la Universidad de Cundinamarca, institución de Educación Superior ubicada Geográficamente en siete municipios del Departamento de Cundinamarca, cuenta con más de 14 mil miembros entre estudiantes docentes y administrativos, los cuales hacen usos de servicios como Plataforma Institucional, prácticas académicas, correo electrónico institucional, Moodle, Teams, servicios de streaming, voz y accesos VPN's entre sedes, generando gran cantidad de tráfico local, adicional al intercambiando y uso de recursos y accesos a los diferentes sistemas de información ofrecidos por la institución a nivel WAN desde y hacia la red externa. Por tanto, contar con una red segura, redundante, confiable, automatizada, con gestión centralizada y sobretodo, que mejore la experiencia final del usuario, es uno de los propósitos fundamentales de este proyecto.
Así las cosas, este proyecto se compone en tres grandes partes:

- Servicio de Conectividad
- Servicio de Datacenter en modalidad Colocation
- Servicio de Seguridad Perimetral Centralizada en Data Center

Es importante mencionar que los tres (componentes) solicitados son servicios importantes y primordiales para continuidad del negocio, estos servicios se contratan bajo la modalidad de contratación PRESTACIÓN DE SERVICIOS F-CPS, este tipo de contratación le permite a la Universidad de Cundinamarca desde el área técnica contar con un mejor manejo desde la administración de los servicios, implementación y seguimiento, toda vez que, para la Institución cubre la demanda de uso de las TIC's requeridas por la comunidad en cada una de las unidades regionales, de igual manera, con la publicación de todos los servicios institucionales (Plataforma, Moodle, Pagina institucional, Licenciamientos académicos, etc.) le va a permitir a los usuarios conectarse desde su redes externas o redes internas para el ingreso, consulta de los diferentes sistemas de información ofertados por la Universidad, adicionalmente contar con un proceso de contratación unificado nos permite garantizar que seguridad requerida en la navegación y evitar ataques o rodo de información en los servidores de la Universidad. Por tal motivo, separar el servicio de conectividad de esta modalidad contractual frente a los otros dos servicios mencionados ocasionará que la sinergia entre estos afecte de

manera directa la calidad y seguridad de todos los servicios degradando de manera significativa la experiencia del usuario.

A continuación, se explicará brevemente lo requerido en cada parte, con el fin de lograr un acercamiento a lo esperado por la Universidad:

1. SERVICIO DE CONECTIVIDAD

Actualmente la Universidad se encuentra interconectada en sus siete sedes por una red MPLS centralizada, con canales de internet dedicados y redundantes en Fibra óptica para seis (6) de sus ocho sedes. Las dos (2) sedes restantes también cuentan con un canal dedicado de internet en Fibra Óptica (sin redundancia). Adicional, existen dos (2) Centros Agroambientales ubicados en zona rural los cuales se encuentra conectados por medio de Radio Enlaces dedicados y un (1) centro Administrativo Deportivo ubicado en zona urbana pero que también está conectado por medio de radio enlace.
Estas conexiones van centralizadas hacia el Datacenter del proveedor actual, lugar en donde se encuentran alojados los servidores propios de la universidad en modalidad de Colocation. Desde allí, se ofrecen y se administran todos los servicios y Sistemas de Información propiedad de la Universidad a los cuales se accede por la red local (MPLS) o por la red externa por medio de NAT's públicas.
En el Datacenter se encuentra también un equipo de Seguridad Perimetral en alta disponibilidad el cual se encarga no solo de proporcionar la protección del tráfico que circula por la red, sino también la seguridad de los servidores alojados en Datacenter y el tráfico proveniente desde y hacia internet de cada una de las sedes.
A continuación, se relaciona el diagrama de red actual, con el fin de orientar gráficamente lo anteriormente expuesto:

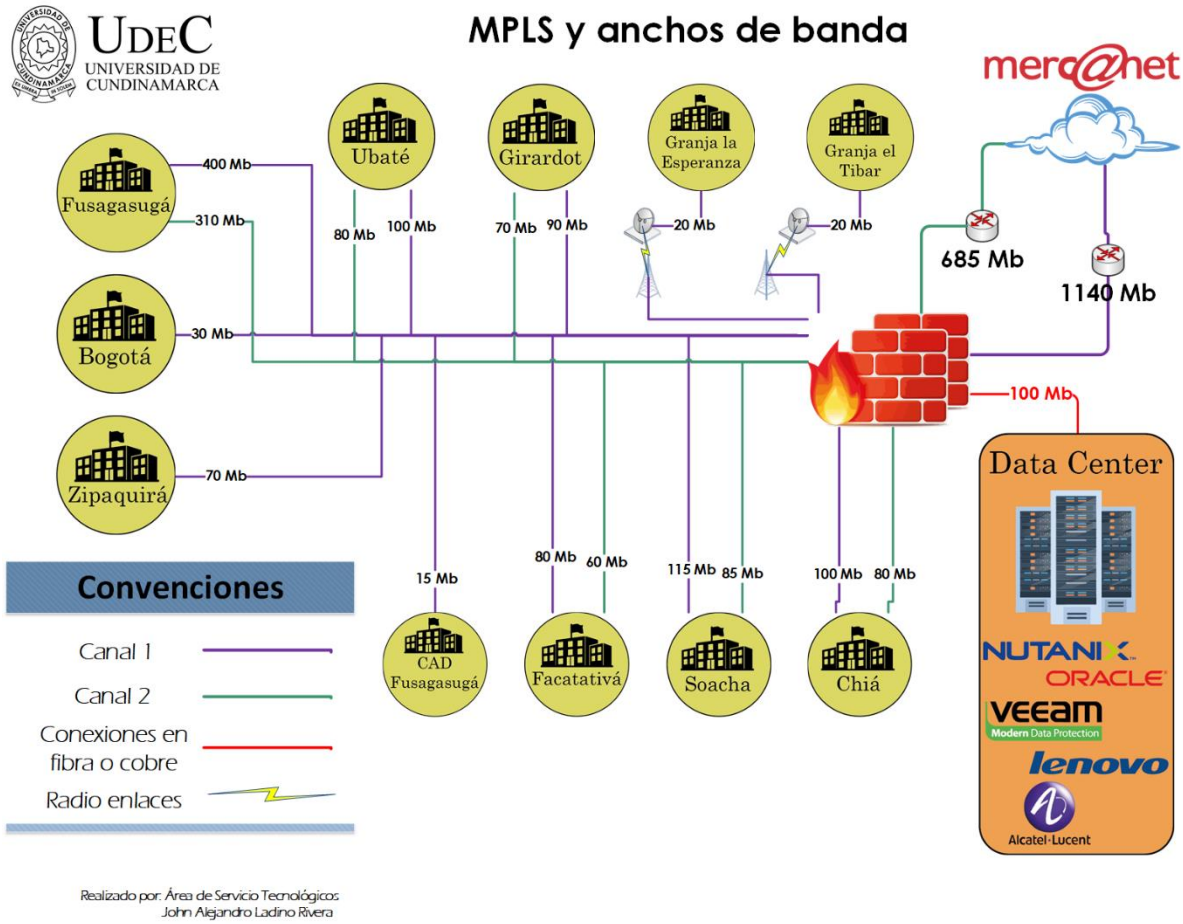

Figura 1 Diagrama de Red Actual - Fuente: Elaboración Propia.

Proyección Conectividad Híbrida: MPLS- SDWAN

Debido a la Transformación Digital actual, el crecimiento exponencial de usuarios conectados a la red, los servicios multiplataforma cada vez más utilizados por los usuarios, el teletrabajo, las proyecciones vía streaming, video llamadas, accesos remotos, conexiones VPN, entre otros recursos que la Universidad provee y ofrece, además de la protección ante posibles ataques a los que se encuentra expuesta, se contempla la necesidad de fortalecer y actualizar su arquitectura e infraestructura de red, con el fin de mejorar no solamente la capacidad de procesamiento, sino además el poder garantizar un sistema redundante, seguro, protegido, automatizado, monitorizado y con gestión centralizada, que permita la visibilidad en tiempo real del tráfico y las aplicaciones de cada una de las sedes.

Por lo anterior, se espera implementar una solución Híbrida entre red MPLS y equipos SDWAN haciendo necesario clasificar las sedes existentes en dos tipos:

- SEDES TIPO A
- SEDES TIPO B

En las SEDES TIPO A se encuentran aquellas que, por sus características demográficas, técnicas y de comportamiento alto en consumos de ancho de banda y uso de servicios, requieren la implementación de un equipo SDWAN:

- Fusagasugá
- Girardot
- Soacha
- Chía
- Facatativá
- Ubaté

La Sedes TIPO B, son sedes que en comparación con las TIPO A, no requieren de un equipo independiente para su gestión, se estima que estas deben ir conectadas por la RED MPLS directamente al Firewall de nueva generación proyectado en el Datacenter.

Topología De Red Deseada:

A continuación, se relaciona la topología deseada con este proyecto:

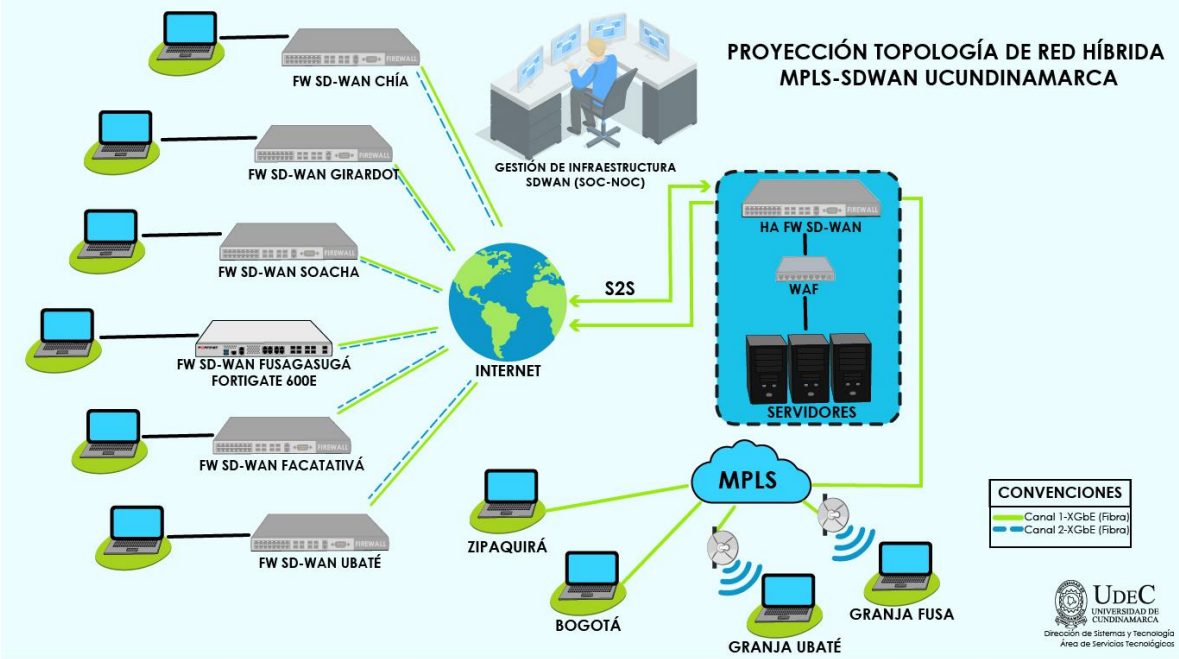

Figura 2 Topología Deseada - Fuente: Elaboración Propia.

Para llevar a cabo esta nueva topología se requiere:

- Cinco (5) appliance de seguridad perimetral deben tener la funcionalidad nativa de SD-WAN. Éstos irán ubicados en las sedes de: CHÍA, GIRARDOT, SOACHA, FACATATIVÁ Y UBATÉ
- Actualmente, la sede FUSAGASUGÁ cuenta con el NGFW de marca FORTINET de referencia FG600E, el cual debe ser incluido dentro de la solución a ofertar.
- Las seis (6) sedes TIPO A deberán contar cada una con dos (2) canales de internet en Fibra Óptica, dedicados e independientes, conectados directamente a internet
- Dos de las sedes TIPO B (Bogotá y Zipaquirá) deberán tener cada una, un (1) canal de Internet/datos en Fibra Óptica conectados directamente a la MPLS.
- Las otras dos (2) sedes TIPO B (granjas la esperanza y el Tibar) deberán ir conectadas a la MPLS por Radio enlace (Estos radio enlaces deben trabajar en las frecuencias de uso libre radioeléctrico de 2.4Ghz o 5Ghz)
- Tanto las sedes TIPO A como las sedes TIPO B, deberán ir conectadas a Datacenter por medio del NGFW en alta disponibilidad que debe ir en este espacio
- Se deberán definir VPN’s tipo Site to Site para la comunicación entre sedes
- Deberá existir una Gestión centralizada, monitorizada y con análisis de comportamiento por parte del proveedor para la nueva solución.
- Para la conexión en Datacenter entre el firewall y los switches Alcatel de la Universidad, se deben incluir dos puntos de red a 1GB o 10 GB en F.O. con conector LC con sus respectivos patch cord y transceivers, Es importante aclarar que los switches Alcatel cuentan con sus transceivers multimodo para esta conexión.

SEDES TIPO A CONECTADAS POR TECNOLOGÍA SDWAN:

- Las sedes deberán contar con dos (2) canales de internet dedicados conectados directamente a la red de Internet
- Los canales de Internet deberán ser en Fibra Óptica
- Se deberá estimar en cada sede un equipo SDWAN con funciones de Seguridad para la protección de los canales dedicados de cada sede

- Balanceo de rutas que garantice una óptima operación, evaluando siempre cual es el mejor camino para enrutar el tráfico generado
- Enrutamiento por Aplicaciones, definiendo cuales son las más críticas y sobre las que se dará prioridad en el tráfico desde y hacia Datacenter
- La conexión hacia Datacenter será única y exclusivamente para acceder a los servicios y aplicativos alojados en nuestros servidores
- Monitoreo y Analítica detallada de la red WAN para el tráfico de internet y de las aplicaciones propias: estadísticas de usos, visibilidad de las aplicaciones, ajuste en tiempo real del uso de las aplicaciones
- Cifrado de datos
- Gestión Centralizada
- Motor de Análisis en Tiempo Real
- Conexiones VPN Site-to-Site con las SEDES TIPO B
- Conexión directa con NGFW ubicado en Data Center
- La solución SDWAN deberá permitir y transportar tráfico en IPV6

Funciones Básicas necesarias para equipos SDWAN

- Los Firewall de Nueva Generación deberán ser dual stack, y deberán contar con la funcionalidad de tener unificadas en una única configuración y vista las reglas de firewall de IPv4 e IPv6.
- Los equipos deben entregar en tiempo real estadísticas de usuarios, aplicaciones, seguridad. Presentar en un formato donde sea posible por el usuario verificar que aplicaciones, sitios, categorías y amenazas de seguridad se han tenido en un tiempo de 24 horas.
- Los dispositivos deben traer activas y licenciadas las funcionalidades de IPS, Filtrado Web, Control de Aplicaciones, VPN IPSec, VPN SSL, DLP, Antimalware, Inspección SSL/SSH
- La plataforma debe tener la capacidad de permitir observar el consumo de ancho de banda en tiempo real por usuario, fuente IP, aplicación y páginas web. Con el fin de detectar algún tipo de problema referente a consumos altos de ancho de banda.
- Debe tener la capacidad de generar un widget de visualización, una vez se realiza el filtro de algún tipo de búsqueda especifica
- La solución deberá pertenecer al cuadrante de líder de gartner para Enterprise Network Firewall
- La solución SD-WAN debe soportar micro segmentación de tráfico donde sea posible, aplicar políticas de IPS y Antivirus entre segmentos de LAN
- La solución SD-WAN debe admitir NAT en el contexto de salida (NAT Outbound) a un grupo de IP públicos

- La solución SD-WAN debe proveer la capacidad de realizar inspección SSL para el tráfico https, bloqueo de malware y reconocimiento en capa 7 de aplicaciones en cada una de las sedes
- La solución debe ser capaz de proporcionar Zero Touch provisioning (Se debe contemplar el equipo existente en la sede de Fusagasugá).
- La solución de Zero Touch provisioning debe ser capaz de admitir direccionamiento estático y dinámico y que se admite en varios vínculos WAN.
- La solución de Zero Touch debe ser escalable, soportando un mínimo de 15 dispositivos en una misma comunidad VPN
- La solución debe ser capaz de proveer una arquitectura de comunicación entre las sedes, de tal manera que puedan utilizar su canal local de internet para establecer una VPN con cualquier elemento de SD-WAN
- La solución, independiente en su modalidad física o virtual, debe soportar los siguientes requisitos:
    - IPv6
    - VRRP o Equivalente
    - VRF
    - BGP
    - OSPF
    - RIPv2
    - Dynamic Multipath
    - Policy Based Routing
    - Reconocimiento en capa 7
    - Debe, de forma alternativa, contar con una base de datos interna, donde sea posible atar una aplicación a un determinado IP / rango de IPs de destino
- El reconocimiento de aplicaciones debe actualizarse de forma dinámica y totalmente transparente en el dispositivo
- El reconocimiento de aplicaciones debe realizarse independientemente de puerto y protocolo
- La solución debe proporcionar el reconocimiento por defecto en la capa 7, de al menos 4000 aplicaciones ampliamente utilizadas en contextos de SaaS, Aplicaciones en la nube, aplicaciones multimedia (Vimeo, YouTube, Facebook, etc.)
- La solución, en su modalidad física y / o virtual, debe considerar los siguientes:
- 802.1Q
- BFD para BGP

- La solución SD-WAN debe admitir Enrutamiento dinámico BGP con compatibilidad con IPv6
- La solución debe ser capaz de medir el estado de salud del enlace basándose en criterios mínimos de: Latencia, Jitter y Packet Loss, donde sea posible configurar un valor de Theshold para cada uno de estos ítems, donde será utilizado como factor de decisión en las reglas de SD-WAN
- La solución debe ser capaz de medir el estado de salud con soporte para múltiples servidores.
- La solución debe permitir la configuración de políticas de QoS en la capa 7, asociadas porcentualmente al ancho de banda de la interfaz SD-WAN
- La solución debe permitir la configuración de políticas de QoS en valores donde el máximo corresponda a la totalidad del ancho de banda disponible en el equipo
- La solución debe permitir la consulta vía SNMPv2 / v3 referente a los siguientes datos:
    - Estado actual de los enlaces SD-WAN
    - Latencia
    - Jitter
    - Packet Loss
    - Paquetes enviados / paquetes recibidos
    - Link Bandwitdh
    - VRF asociado
- La solución debe posibilitar la distribución de peso en cada uno de los enlaces que componen el SD-WAN, a criterio del administrador, de forma que el algoritmo de equilibrio utilizado pueda basarse en:
    - Número de sesiones,
    - Volumen de tráfico,
    - IP de origen y destino
    - desbordamiento de Enlace (Spillover)
- La solución debe ser capaz de admitir una arquitectura de transporte multidifusión IPv4 e IPv6 a través de túneles VPN IPSEC.

Especificaciones Técnicas para equipos SD-WAN

- Se requieren cinco (5) NGFW que se instalarán en las sedes Facatativá, Girardot, Chía, Ubaté y Soacha de LA UNIVERSIDAD DE CUNDINAMARCA (sedes TIPO A), deberán ser totalmente compatibles con el equipo que actualmente posee la sede de Fusagasugá (Fortigate

600E), los cuales deberán cumplir con las siguientes características mínimas de desempeño ya activas y funcionales en cada Appliance:

- Rendimiento de Firewall 36 Gbps
- Rendimiento de IPS 10 Gbps
- Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 9,5 Gbps
- Rendimiento Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 7 Gbps
- Rendimiento IPSec VPN 20 Gbps
- Soporte de 8 Millones sesiones concurrentes
- Rendimiento de Inspección SSL 8 Gbps
- Soporte de 10000 usuarios VPN SSL
- Rendimiento de VPN SSL 7 Gbps
- Debe soportar 10 interfaces 1GE RJ45
- Debe soportar 8 interfaces 1 GE SFP, y se deben incluir 4 tranceivers 1 GE SFP
- Debe soportar 2 interfaces 10 GE SFP+, y se deben incluir 2 tranceivers 10 GE SFP+

Nota: Para la Sede Tipo A Extensión Soacha, el proveedor deberá incluir como dispositivos adicionales a los equipos de border de la solución en general, **UN (1) Switchs** capa 3 con el fin de proveer la conexión LAN.

SEDES TIPO B CONECTADAS POR MPLS

- Las Sedes TIPO B tendrán un (1) único canal de conexión centralizado por medio de una MPLS al Firewall ubicado en DATACENTER
- Las Granjas: La Esperanza y El Tíbar (SEDES TIPO B) serán conectadas por medio de radio enlaces
- Las sedes: Zipaquirá y Bogotá (SEDES TIPO B) Tendrán un canal dedicado por Fibra Óptica conectado a la MPLS.
- Las sedes TIPO B estarán gestionados y protegidos por el NGFW ubicado en Datacenter
- Se debe contemplar la instalación de equipos de border en calidad de prestamos adecuados a las condiciones técnicas de cada canal ofrecido, para poder recibir los canales en cada sede.

Nota: Para la Sede Tipo B Unidad Agroambiental el Tíbar - Ubaté, el proveedor deberá incluir como dispositivos adicionales a los equipos de border de la solución en general, **UN (1) Switchs** capa 3 con el fin de proveer la conexión LAN.

DISMINUCIÓN DE LOS CANALES

La Universidad de Cundinamarca podrá solicitar al proveedor la disminución hasta un valor mínimo establecido en el anexo: "**ANEXOS CONECTIVIDAD UDEC"** en la ***TABLA 2. REQUERIMIENTOS TECNICOS CONECTIVIDAD UCUNDINAMARCA 2021-2022,*** teniendo en cuenta la demanda del servicio dentro del periodo contractual. Esta disminución se verá reflejada en los servicios solicitados y el costo de facturación mensual.

TABLA 3. DISMINUCIÓN DE BW			
Clasificicón Sedes	UBICACIÓN	INTERNET DEDICADO	
		CANAL2 / BW ACTUAL	CANAL2 / DISMINUIR A
SEDES TIPO A	Sede Fusagasugá	250	125
	Seccional Girardot	80	40
	Extensión Soacha	80	40
	Extensión Facatativá	80	40
	Extensión Chía	80	40
	Seccional Ubaté	80	40
TOTAL		650	325

Tabla 1 DISMINUCIÓN DE BW – FUENTE ELABORACIÓN PROPIA

2. SERVICIO DE DATACENTER EN MODALIDAD COLOCATION

Actualmente la Universidad cuenta con una granja de servidores avalados alojados en el Datacenter de su proveedor de servicios en modalidad Colocation (Housing). Por tanto, se espera continuar con este tipo de alquiler. En total, se requiere el alquiler de un espacio en rack, que tenga la capacidad para trece (13) Unidades de rack, 105.26 Kg y un consumo máximo aproximado de 7KVA de potencia. Se espera con el servicio de colocation obtener un espacio flexible (que se adapte a las necesidades de la Universidad), con disponibilidad (alto grado de continuidad operacional), escalabilidad (capacidad de crecer los servicios rápidamente) y con el cumplimiento de altos estándares de seguridad física, control de temperatura, suministro de energía, entre otros.

ESPECIFICACIONES COLOCATION UNIVERSIDAD DE CUNDINAMARCA															
Marca	Modelo	Unidades de rack	Rackeable	"Dimensiones (h x w x d) centímetros"	Peso (kg)	Voltaje de alimentación	Consumo máximo especificado (Watts)	Número de fuentes	Conector de la fuente	Unidades de rack	Potencia	Disponibilidad del Servicio	Tipo Datacenter	Cant. Dir IP Públicas Requeridas	Soporte
Nutanix	NX-3060-G7	4	SI	8.9cm x 45.1cm x 77.8cm	47.6 kg	110	2118 W	4	nema 5-15	13	7KVA	99,98%	Tier III	40	7x24x365 Manos Remotas
Lenovo	ThinkSystem SR590	2	SI	87cm x 44.5cm x 72cm	26. kg	110	1500 W	2	nema 5-15						
Alcatel	OS6900-X72-F	1	SI	4.4cm x 43.3cm x 55.9cm	7.78 kg	110	242 W	2	nema 5-15						
Alcatel	OS6900-X72-F	1	SI	4.4cm x 43.3cm x 55.9cm	7.78 kg	110	242 W	2	nema 5-15						
Oracle	DATABASE APPLIANCE X7-2S	1	SI	4,3cm x 43.7cm x 73.7cm	16.1 kg	110	1200 W	2	nema 5-15						
				Total Peso	105.26 kg	Total	5302 W	12							

Figura 3 Especificaciones Colocation - Fuente: Elaboración Propia.

Es así como, su valor en libros actual es de SETECIENTOS MILLONES M/CTE ($700.000.000) SIN IMPUESTOS. En caso de pérdida de equipos durante el traslado o su operación los valores deberán actualizarse a precio comercial vigente que garantice la reposición del o de los equipos con las especificaciones técnicas similares o escalables a la tecnología actual.

Con el servicio de Colocation se espera:

- Mesa de Ayuda y Soporte 7x24x365 incluido servicio de Manos Remotas.
- Datacenter tipo Tier III, donde se alojarán lo servidores de la Universidad.
- La ubicación de este Data center deberá ser en la Ciudad de Bogotá o en sus alrededores
- El proveedor deberá garantizar a la institución que su dominio *ucundinamarca.edu.co* será publicado por medio de sus DNS públicos. La Universidad será quien realice el trámite ante el registrador correspondiente para la actualización de dichos DNS.
- Se requiere la publicación de las aplicaciones alojadas en nuestros servidores, las cuales requieren de 40 Direcciones IP Públicas por medio de NAT's, de igual forma deberá permitir y transportar tráfico en IPV6.
- El oferente deberá incluir el Servicio de Manos Remotas con Diez (10) horas de mensuales
- El oferente deberá incluir los conversores requeridos para las conexiones electicas de los equipos.

Observaciones Adicionales:

- El Diagrama de Interconexión de los equipos alojados en data center será proporcionado por la Universidad al oferente a quien sea asignado el contrato de la presente invitación.
- Para los equipos que se encuentren en garantía, la Universidad se encargará de contactar al Fabricante con el fin de tener en cuenta las condiciones de traslado exigidas por el mismo. Estas condiciones serán adicionales a las relacionadas en la **lista de verificación de actividades anexa a este documento ASIRr013_V5Traslado de equipos.**
- La desconexión, apagado y almacenado de los equipos para el traslado de un datacenter a otro, será por parte de la Universidad
- Traslado seguro por parte del proveedor a quien se le asigne el proyecto desde el datacenter actual a su datacenter.
- La conexión, encendido, puesta en marcha y verificación de funcionamiento de los equipos será por parte de la Universidad

EQUIPO DE SEGURIDAD DE APLICACIONES WEB (WAF)

Se requiere de igual manera el ofrecimiento de un servicio de Protección y Seguridad para las aplicaciones WEB de la Universidad que permita bloquear amenazas en tiempo real, sin bloquear a los usuarios (estudiantes, funcionarios y docentes) minimizando los falsos positivos que puedan llegar a generar demasiada gestión administrativa por parte del área de Servicios Tecnológicos. Este servicio no debe basarse solo en firmas sino además en Inteligencia Artificial.

Funciones Básicas para Equipo WAF

- Deberá proteger como mínimo 30 aplicaciones con un ancho de banda de 100Mbps
- Deberá ser implementado en la Nube del Fabricante (SaaS) o en el datacenter del oferente.
- Debe contar con módulo de Machine Learning y Autoaprendizaje
- Debe realizar Bot Mitigation
- Debe tener un módulo de API Protection
- Escaneo de vulnerabilidades web
- Balanceo de aplicaciones
- Antimalware
- Anti-Defacement

- Anti DDoS Capa 7
- Implementación Flexible
- Alta Disponibilidad
- Compatible con IPV6

3. SERVICIO DE SEGURIDAD PERIMETRAL EN DATA CENTER

Se espera contar con dos (2) equipos de seguridad Perimetral de tipo NGFW ubicados en Datacenter en Alta Disponibilidad y con funcionalidades de SDWAN, o un firewall multitenant en Alta disponibilidad y con funcionalidades de SD-WAN, que permita la conexión directa con las SEDES TIPO A Y TIPO B además de la protección del tráfico circundante desde y hacia los servidores de la Universidad.
Para identificar la capacidad del equipo, se relaciona a continuación, la cantidad de usuarios concurrentes, los anchos de banda por sede y la cantidad de aplicaciones o servicios consumidos:

TABLA 2. REQUERIMIENTOS TECNICOS CONECTIVIDAD UCUNDINAMARCA 2021-2022

Clasificicón Sedes	UBICACIÓN	DIRECCIÓN	COORDENADAS	INTERNET DEDICADO		TIPO CONEXIÓN	TECNOLOGIA	SEGURIDAD PERIMETRAL (NGFW)		Sesiones concurrentes
				CANAL 1	CANAL2			Total de usuarios UCundinamarca	Concurrencia de Usuarios	
SEDES TIPO A	Sede Fusagasugá	Diagonal 18 # 20-29	4,334618 -74,369719	250	250	SDWAN	Fibra Óptica	4252	2500	+/- 300.000
	Seccional Girardot	Calle 19 # 24-209	4,306471 -74,80653	90	80	SDWAN	Fibra Óptica	1619	1034	
	Extensión Soacha	DIAGONAL 6 BIS # 5-95	4,578535 -74,223378	90	80	SDWAN	Fibra Óptica	1974	1025	
	Extensión Facatativá	Calle 14 con Av. 15	4,829092 -74,355371	90	80	SDWAN	Fibra Óptica	3365	1878	
	Extensión Chia	Av. Los Zipas Sector el 4 Frente a Santa Ana	4,874015 -74,038119	90	80	SDWAN	Fibra Óptica	1839	838	
	Seccional Ubaté	Calle 6 # 9-80	5,30933 -73,817412	90	80	SDWAN	Fibra Óptica	1286	600	
SEDES TIPO B	Unidad Agroambiental La Esperanza - Fusa	Vereda Guavio Bajo (Fusagasugá)	4,276072 -74,386612	30	-	MPLS	Radio Enlace	130	20	
	Unidad Agroambiental El Tibar - Ubaté	Vereda Palogordo, sector Novillerps (Ubaté)	5,327192 -73,792056	20	-	MPLS	Radio Enlace	150	15	
	Extensión Zipaquirá	Carrera 7 # 1-31	5,021682 -74,005715	70	-	MPLS	Fibra Óptica	327	168	
	Oficina de Proyectos Especiales y Relaciones Interinstitucionales de Bogotá	Carrera 20 # 39-32	4,627996 -74,073622	25	-	MPLS	Fibra Óptica	15	40	
	Datacenter	Bogotá D.C	-	100	-	SDWAN	Fibra Óptica	14957	8118	

Ilustración 4 Requerimientos Técnicos de Conectividad - Fuente: Elaboración Propia.

- Para la conexión en Datacenter entre el firewall y los switches Alcatel de la Universidad, se deben incluir dos puntos de red a 1GB o 10 GB en F.O. con conector LC con sus respectivos patch cord y transceivers, Es importante aclarar que los switches Alcatel cuentan con sus transceivers multimodo para esta conexión.

Funciones Básicas para Equipos de Seguridad Perimetral centralizada en Datacenter

- Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- Debe ser posible hacer políticas basados en usuarios, grupos de usuarios y dispositivos sobre una misma política, y ser lo más granular posible en la definición de políticas.
- Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén predefinidos
- Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface).
- La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP
- El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces
- El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.
- Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis
- Debe estar en la capacidad de dar estadísticas de uso por políticas como: Ancho de banda actual, Sesiones activas, Ultimo vez usada.

- Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS)
- Alta Disponibilidad
- VPN IPsec
- VPN SSL
- Manejo de Tráfico y Calidad de Servicio
- Antimalware
- Filtrado WEB
- Protección Contra Intrusos (IDS/IPS)
- Control de Aplicaciones
- Inspección de Contenido (SSL/SSH)

Especificaciones Técnicas para equipos de Seguridad Perimetral centralizada en Data center (NGFW)

- Rendimiento de Firewall 80 Gbps
- Rendimiento de IPS 12,5 Gbps
- Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 9,8 Gbps
- Rendimiento Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 7,1 Gbps
- Rendimiento IPSec VPN 48 Gbps
- Soporte de 8 Millones sesiones concurrentes
- Rendimiento de Inspección SSL 10 Gbps
- Soporte de 10000 usuarios VPN SSL
- Rendimiento de VPN SSL 8,4 Gbps

Especificaciones Técnicas adicionales para los 2 equipos de seguridad perimetral centralizada en Datacenter.

- Debe soportar 18 interfaces 1GE RJ45
- Debe soportar 8 interfaces 1 GE SFP, y se deben incluir 4 tranceivers 1 GE SFP
- Debe soportar 4 interfaces 10 GE SFP+, y se deben incluir 2 tranceivers 10 GE SFP+
- Debe soportar 4 interfaces 25 GE SFP28,
- Debe soportar 2 interfaces 40 GE QSFP+, y se deben incluir 1 tranceivers 40 GE QSFP+

4. PLATAFORMA DE GESTIÓN DE LOGS Y REPORTES CENTRALIZADOS

Se debe entregar una plataforma de gestión de log y reportes centralizados que cuente con las siguientes características:

a. El equipo deberá recolectar y emitir el reporte de eventos, actividades y tendencias ocurridas en las plataformas de seguridad perimetral ofertadas tales como el Firewall de Nueva Generación y la solución de SD-WAN
b. La solución deberá poderse integrar de forma nativa con los NGFW solicitados para las sedes TIPO A y el equipo actualmente ubicado en la sede Fusagasugá.
c. La solución de análisis de logs debe contar con las siguientes características:
    i. Capacidad de recibir hasta 100 GB de logs diarios.

ii. Capacidad de Almacenamiento de 8 Terabytes
iii. Capacidad de soportar una tasa sostenida de 3000 logs por segundo.
iv. Capacidad de recibir logs hasta de 180 equipos sin necesidad de licencias adicionales

d. Debe entregar los siguientes reportes minimos de NGFW y SDWAN
   i. Debe contar con reporte de cumplimiento de PCI DSS
   ii. Debe contar con reporte de utilización de aplicaciones SaaS
   iii. Debe contar con reporte de prevención de perdida de datos (DLP)
   iv. Debe contar con reporte de VPN
   v. Debe contar con reporte de Sistema de prevención de intrusos (IPS)
   vi. Debe contar con reporte de reputación de cliente
   vii. Debe contar con reporte de análisis de seguridad de usuario
   viii. Debe contar con reporte de análisis de amenaza cibernética
   ix. Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad
   x. Debe contar con reporte de tráfico DNS
   xi. Debe contar con reporte tráfico de correo electrónico
   xii. Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red
   xiii. Debe contar con reporte de Top 10 de Websites utilizadas en la red
   xiv. Debe contar con reporte de uso de redes sociales

5. PLATAFORMA DE ADMINISTRACIÓN CENTRALIZADA DE SD-WAN

Se debe entregar una plataforma o sistema de administración centralizada de dispositivos de seguridad y SD-WAN que cuente con las siguientes características:

a. Centralización de Configuración y monitoreo de todos los firewalls de nueva generación, así como todas sus funciones de protección de red y de SD-WAN.
b. La solución de administración centralizada debe dar soporte a las siguientes características:

i. Capacidad de administrar hasta 30 equipos.
ii. Capacidad de Almacenamiento de hasta 8 Terabytes
iii. Debe soportar arreglo de discos tipo RAID 0/1

c. Creación, almacenamiento e implementación automatizada de configuraciones de dispositivos.
d. Permitir tener un solo repositorio de almacenamiento centralizado y administración de configuraciones, para simplificar las tareas de administración de una gran cantidad de dispositivos de seguridad con protección completa de contenido.
e. Las comunicaciones entre la consola de administración y los dispositivos administrados deben ser cifradas (Encriptadas).
f. La interface de administración es basada en Web Seguro (HTTPS).
g. Para un eficiente almacenamiento de las configuraciones, debe incluirse una base de datos relacional integrada compatible con la solución.
h. Administración basada en roles para permitir a los administradores delegar los derechos a dispositivos específicos con los privilegios adecuados de lectura/escritura.
i. Configuración basada en scripts para una mejor flexibilidad y control. Esta funcionalidad permite la automatización de tareas operativas, cuya implementación puede ser de forma masiva, con tiempos de aplicación mínimos a los dispositivos administrados.
j. Se debe poder realizar automatización calendarizada de respaldos de la configuración y las bitácoras.
k. Se debe poder realizar operaciones sobre grupos de dispositivos, y añadir/cambiar/borrar dispositivos de esos grupos.
l. Permitir el hospedaje local de actualizaciones de firmas de AV / IPS y filtrado de contenido web y Antispam, de los firewalls de nueva generación. Esto permite el almacenamiento de forma local de las bases de datos de protección AV e IPS, además de Filtrado de Contenido y Anti-SPAM, con la finalidad de disminuir el tráfico de consultas de actualizaciones a Internet a lo mínimo, evitando el consumo innecesario de ancho de banda, permitiendo la utilización de este para los fines requeridos por los usuarios de red.
m. Capacidad de crear, exportar y almacenar versiones de configuración de los dispositivos administrados, antes de aplicar cambios a un dispositivo. De esta forma, se disminuye la

posibilidad de cometer un error no intencional al modificar una política y permite regresar a una configuración en un estado operacional después de haber aplicado una implementación con resultados no esperados.

6. CANALES DE ATENCIÓN Y TIEMPOS DE RESPUESTA

- El Oferente que resulte adjudicado debe tener la capacidad de brindar servicio de soporte técnico remoto.
- El Oferente que resulte adjudicado debe brindar soporte para evaluar y solucionar fallas e interrupciones que se presenten. El soporte será en el sitio donde se prestan los servicios sólo en los casos en que no sea posible resolver el problema de forma remota. El servicio en sitio no significa costos adicionales para la Universidad.
- Adicionalmente, el Oferente que resulte adjudicado debe brindar soporte remoto a nivel nacional a través de los siguientes canales:
    - Línea de atención telefónica gratuita con cobertura nacional.
    - Correo electrónico.
    - Chat.

- El Oferente que resulte adjudicado deberá entregarle a la Universidad de Cundinamarca una plataforma web para registro y monitoreo de tickets.

- El Oferente que resulte adjudicado debe garantizar que exista un ticket por cada reporte hecho por la Universidad sobre las fallas o interrupción del servicio. De igual manera sobre los reportes que el mismo proveedor detecte.

- Los canales de soporte deben estar disponibles 7x24x365 durante el tiempo de ejecución.

- El Oferente que resulte adjudicado tendrá 16 horas hábiles a partir del momento de un incidente crítico para reportarle a la Universidad el informe detallado en el cual deberá relacionar por lo menos: motivo de la falla, tiempo de indisponibilidad, elementos y servicios afectados, mecanismo utilizado en la solución del incidente crítico y mecanismos de prevención del incidente a futuro

- El Oferente que resulte adjudicado deberá notificar los incidentes como mínimo en dos medios diferentes de comunicación (SMS, Correo electrónico, aplicaciones como whatsapp o cualquiera que la Universidad determine) y al personal que la entidad defina.

- El Oferente que resulte adjudicado deberá contar con un servicio de Centro de Operaciones de Seguridad o Security Operations Center (SOC) 7x24x365 con las herramientas apropiadas para la gestión de seguridad de los servicios ofertados, que cuente con un centro de monitoreo de los incidentes de seguridad que se puedan presentar y de manera proactiva pueda gestionar los riesgos, asegurando así las condiciones de servicio.

- El Oferente que resulte adjudicado deberá suministrar como mínimo con el siguiente mecanismo de seguridad:
    - Principio de "los cuatro ojos": cualquier decisión de cambios administrativos, en la infraestructura o en los servicios del proveedor, deben ser aprobados por mínimo dos personas de la Universidad, esto con el fin de no afectar a uno o más de los servicios contratados.

- El oferente que resulte adjudicado deberá hacer entrega de reportes o informes mensuales enviados a través de correo electrónico reportando los incidentes de disponibilidad que hayan ocurrido en el mes, además, un informe de seguridad con observaciones y análisis, informe de incidentes de seguridad y de amenazas de seguridad.

- El oferente que resulte adjudicado deberá presentar los acuerdos de Niveles de servicio (ANS) a utilizar durante la ejecución de todo el proyecto

7. LICENCIAMIENTO, ACTUALIZACIONES Y CAPACITACIONES

- El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.

- La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos un (1) años.
- La plataforma es requerida por un periodo de un (1) años en un esquema 7x24 ante el fabricante.
- Transferencia de conocimiento de la solución WAN propuesta, conceptos técnicos y mejores prácticas para la administración de redes WAN, configuración y funcionalidades de las herramientas de monitoreo, gestión y plataforma de administración ofrecidos, configuración y funcionalidades del NGFW, SDWAN y WAF dirigido al área de servicios tecnológicos adscrito a la Dirección de Sistemas y Tecnología (10 participantes).

EDILSON MARTINEZ CLAVIJO
Director Sistemas y Tecnología
UNIVERSIDAD DE CUNDINAMARCA

PAOLA ANDREA RAMIREZ SUAZA
PROFESIONAL DIRECTOR DE ÁREA I
Dirección de Sistemas y Tecnología

JOHN ALEJANDRO LADINO RIVERA
Profesional III
Dirección de Sistemas y Tecnología

Transcriptor: Área de Servicios Tecnológicos
15.