ANEXO ESPECIFICACIONES TÉCNICAS CONECTIVIDAD UCUNDINAMARCA 2022 – 2023 NECESIDADES Y ESPECIFICACIONES TÉCNICAS AL PROYECTO: "SERVICIO DE CONECTIVIDAD POR MEDIO DE SD-WAN, INTERNET DEDICADO, COLOCATION Y SEGURIDAD PERIMETRAL EN ALTA DISPONIBILIDAD CENTRALIZADA EN DATA CENTER PARA LA UNIVERSIDAD DE CUNDINAMARCA"

1. SERVICIO DE CONECTIVIDAD:

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 fortaleció y se actualizo la arquitectura e infraestructura de red, con el fin de mejorar no solamente la capacidad de procesamiento, sino además de 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.

Es así, como actualmente la Universidad de Cundinamarca necesita una solución como servicio de NGFW que cuenten con la capacidad de conexión SDWAN con visibilidad de aplicaciones y balanceo de canales basado en diferentes métricas, aplicaciones y necesidades puntuales para cada sede es por esto que todas las sedes contaran con canales de internet dedicado (sin reusó) y un equipo de seguridad que provea la capacidad de conexión por medio de SD-WAN, adicional de poder ser la capa de enrutamiento de la red (capa 3) para poder monitorea, filtrar y brindar seguridad a todas las redes en cada una de las sedes seccionales y extensiones de la Universidad de Cundinamarca.

Por lo anterior, y teniendo en cuenta las características demográficas, técnicas y de comportamiento en alto consumos de ancho de banda y uso de servicios, se requiere la implementación como servicio de los equipos NGFW:

Tabla 1. Relación de Equipos SDWAN			
ítem	Unidad Regional	SDWAN - ESPECIFICACIONES TÉCNICAS MÍNIMAS	CANTIDAD
1	Sede Fusagasugá	FortiGate 600E (Equipo propiedad de la Universidad, con licenciamiento.)	-
2	Extensión Facatativá	• Rendimiento de Firewall 36 Gbps • Rendimiento de IPS 10 Gbps • Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 9,5 Gbps • Rendimiento Protección 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 • Debe soportar 2 interfaces 10 GE SFP+	1
3	Extensión Soacha		1
4	Extensión chía		1
5	Extensión Zipaquirá		1
6	Seccional Ubaté		1
7	Seccional Girardot		1
8	Unidad Agroambiental Tibar	• Rendimiento de IPS 1.4 Gbps • Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 1 Gbps • Rendimiento Protección de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 700 Mbps • Rendimiento IPSec VPN 6.5 Gbps • Soporte de 700 000 sesiones concurrentes • Rendimiento de Inspección SSL 630 Mbps • Soporte de 55000 usuarios VPN SSL • Rendimiento de VPN SSL 900 Mbps • Debe soportar 5 interfaces 1GE RJ45, 2 puerto WAN y 1 puerto DMZ • Firewall Throughput (1518 / 512 / 64 byte UDP packets): 10/10/6 Gbps • Firewall Latency (64 byte UDP packets): 3.3 µs • Firewall Throughput (Packets Per Second): 9Mpps	1
9	Unidad Agroambiental La Esperanza		1
10	Oficina de Proyectos Especiales - Bogotá		1

Tabla 1 - Relación de Equipos SDWAN a solicitar - Fuente: Elaboración Propia.

Con la implementación de este proyecto se espera obtener la siguiente topología de Red:

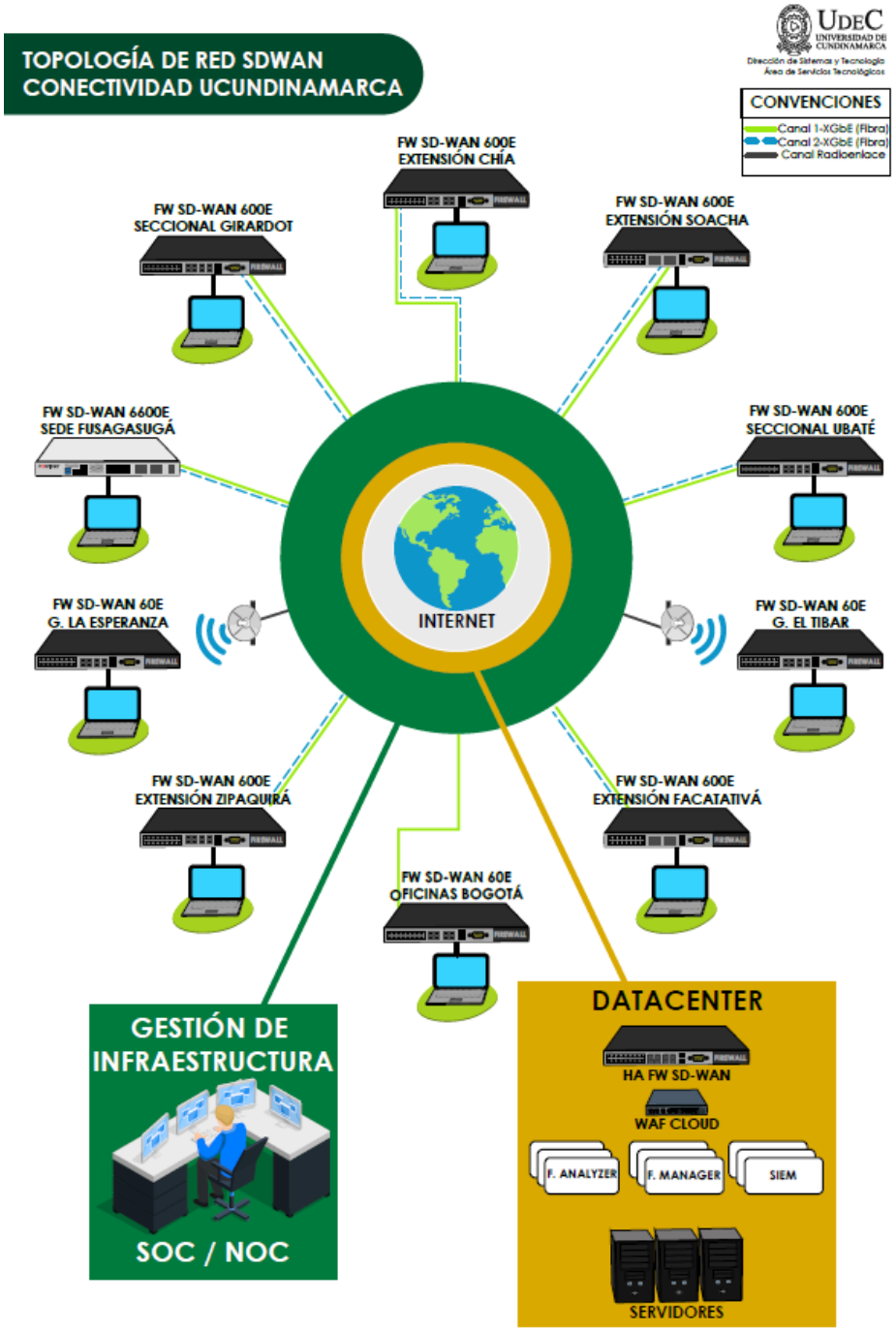

Imagen 1, Topología Deseada - Fuente: Elaboración Propia.

1.1 Canales de Internet:

Los canales de Internet deber ser considerados en medio físico de Fibra Óptica en nueve (9) Unidades Regionales y dos (2) con tipo de conexión por medio de Radio Enlace, como se evidencia en la siguiente tabla.

TABLA 4. REQUERIMIENTOS TECNICOS CONECTIVIDAD UCUNDINAMARCA 2022-2023									
UBICACIÓN	DIRECCIÓN	COORDENADAS	INTERNET DEDICADO		TIPO CONEXIÓN	TECNOLOGIA	SEGURIDAD PERIMETRAL (NGFW)		Sesiones concurrentes
			CANAL 1	CANAL2			Total de usuarios UCundinamarca	Concurrencia de Usuarios	
Sede Fusagasugá	Diagonal 18 # 20-29	4,334618 -74,369719	300	300	SDWAN	Fibra Óptica	4300	2800	+/- 300.000
Seccional Girardot	Calle 19 # 24-209	4,306471 -74,80653	120	90	SDWAN	Fibra Óptica	1630	1100	
Extensión Soacha	DIAGONAL 6 BIS # 5-95	4,578535 -74,223378	120	90	SDWAN	Fibra Óptica	1900	1025	
Extensión Facatativá	Calle 14 con Av. 15	4,829092 -74,355371	120	90	SDWAN	Fibra Óptica	3400	2000	
Extensión Chía	Av. Los Zipas Sector el 4 Frente a Santa Ana	4,874015 -74,038119	120	90	SDWAN	Fibra Óptica	1900	900	
Extensión Zipaquirá	Carrera 7 # 1-31	5,021682 -74,005715	90	70	SDWAN	Fibra Óptica	400	190	
Seccional Ubaté	Calle 6 # 9-80	5,30933 -73,817412	120	90	SDWAN	Fibra Óptica	1320	800	
Unidad Agroambiental La Esperanza - Fggá	Vereda Guavio Bajo (Fusagasugá)	4,276072 -74.386612	30	-	SDWAN	Radio Enlace	150	30	
Unidad Agroambiental El Tibar - Ubaté	Vereda Palogordo, sector Novilleros (Ubaté)	5,327192 -73,792056	30	-	SDWAN	Radio Enlace	120	20	
Oficina de Proyectos Especiales y Relaciones Interinstitucionales de Bogotá	Carrera 20 # 39-32	4,627996 -74,073622	35	-	SDWAN	Fibra Óptica	25	40	
Datacenter	Bogotá D.C	-	120	-	SDWAN	Fibra Óptica	**15145**	**8905**	

Tabla 2, Requerimientos Técnicos de Conectividad - Fuente: Elaboración Propia.

- Garantizar una disponibilidad mínima de todos los enlaces de 99.7%
- Las conexiones de las Unidades Regionales deberán ser simétricas y con Nivel de Reuso 1:1.
- Interconexión con NAP Colombia directa y redundante, con interfaces de 10Gbps.
- El oferente deberá configurar, mantener y soportar requerimientos y de calidad de servicio para integrar las conexiones entre los protocolos IPV6 e IPV4.
- El canal de internet debe garantizar QoS para las conexiones, transmisiones y recepción de Streaming punto a punto y/o multipunto con destinos nacionales e internacionales.

1.2 Direccionamiento

- El oferente debe garantizar el reconocimiento de la Red de la UCundinamarca en internet.
- El oferente debe suministrar direccionamiento IPv4 valido para mínimo 40 direcciones públicas.
- La Universidad de Cundinamarca ya adquirió ante LANIC su Direccionamiento Ipv6, por lo tanto, el oferente que resulte adjudicado se le suministrará dicho direccionamiento para realizar

la publicación hacía internet de todas las sedes incluyendo Datacenter.

1.3 DNS

El Oferente deberá suministrar el servicio de resolución de nombres de dominio primario y secundario en los protocolos IPv4 e Ipv6 para los dominios que requiera la Universidad dentro de su dominio principal **ucundinamarca.edu.co.**

1.4 Consideraciones para tener en cuenta:

- Nueve (9) appliance de seguridad perimetral deben tener la funcionalidad nativa de SD-WAN. Éstos irán ubicados en las sedes de: CHÍA, ZIPAQUIRÁ, GIRARDOT, SOACHA, FACATATIVÁ, UBATÉ, UNIDAD AGROAMBIENTAL TIBAR, UNIDAD AGROAMBIENTAL LA ESPERANZA y OFICINA DE PROYECTOS ESPECIALES - BOGOTÁ.
- 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, este NGFW ya cuenta con el respectivo licenciamiento para su funcionamiento.
- Las SIETE (7) sedes CHÍA, ZIPAQUIRÁ, GIRARDOT, SOACHA, FACATATIVÁ, UBATÉ y FUSAGASUGÁ deberán contar cada una con dos (2) canales de internet en Fibra Óptica, dedicados e independientes, conectados directamente a internet.
- La sede de Bogotá deberá tener un (1) canal de Internet en Fibra Óptica dedicado, conectado directamente a internet.
- Las otras dos (2) sedes -Unidades Agroambientales esperanza y el Tibar deberán ir conectadas por Radio enlace (Estos radios enlaces deben trabajar en las frecuencias de uso libre radioeléctrico de 2.4Ghz o 5Ghz) con clave de cifrado de mínimo 114bits entre las antenas y el canal debe ser conectado directamente a internet y dedicado.
- Todas las sedes, deberán ir conectadas hacia Datacenter por medio del de la red de SD-WAN con el NGFW de alta disponibilidad que debe ir en Datacenter.
- Para la 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.
- Balanceo de rutas, métricas, automático, por direccionamiento, etc, que garantice una óptima operación, de los canales y evitar en todo momento la saturación de estos.

- Enrutamiento por Aplicaciones, definiendo cuales son las más críticas y sobre las que se dará prioridad en el tráfico desde y hacia Datacenter.
- 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.
- Gestión centralizada por medio de una herramienta que administre todo el conjunto de NGFW, para garantizar una visión completa de la solución.
- Un sistema de monitoreo y gestión de incidentes de nueva generación dedicado, basado tecnologías de recolección, gestión, correlación y análisis de eventos tipo SIEM.
- Cifrado de datos
- Motor de Análisis en Tiempo Real
- Conexiones VPN Site-to-Site o por medio de la malla de SD-WAN que permita la visibilidad de todas las sedes entre sí y poder mantener los servicios que actualmente se comparten entre sí.
- Conexión directa con NGFW ubicado en Data Center y los servidores de virtualización propiedad de la Universidad.
- La solución completa (SD-WAN, NGFW, canales de internet, Colocation, etc.) deberá permitir y transportar tráfico en IPV6 y trabajar en dual stack.
- 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 microsegmentación 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 IP’s 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.
- Por cada equipo de NGFW instalado en cada sede se debe entregar un usuario de lectura para uso de la Universidad capaces de soportar y generar investigaciones, búsquedas avanzadas, generación de reportes, monitoreo completo de los eventos de seguridad sin necesidad de contar con un tercero.

1.5 Especificaciones Técnicas para equipos SD-WAN

- Se requieren seis (6) NGFW que se instalarán en las sedes Facatativá, Zipaquirá, Girardot, Chía, Ubaté y Soacha de LA UNIVERSIDAD DE CUNDINAMARCA, 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 8 interfaces 1GE RJ45
    - Debe soportar 8 interfaces 1 GE SFP
    - Debe soportar 2 interfaces 10 GE SFP+

- Se requieren seis (3) NGFW La unidad agroambiental tíbar, unidad agroambiental la esperanza y oficina de proyectos especiales - Bogotá estarán gestionados y protegidos por el NGFW ubicado en sitio con las siguientes características:

    - Rendimiento de IPS 1.4 Gbps
    - Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 1 Gbps
    - Rendimiento Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 700 Mbps
    - Rendimiento IPSec VPN 6.5 Gbps
    - Soporte de 700 000 sesiones concurrentes
    - Rendimiento de Inspección SSL 630 Gbps
    - Soporte de 55000 usuarios VPN SSL
    - Rendimiento de VPN SSL 900 Gbps

- Debe soportar 10 interfaces 1GE RJ45 (debe incluir 7 puertos internal Ports, 2 puertos WAN y 1 puerto DMZ)

1.6 DISMINUCIÓN DE LOS CANALES

La Universidad de Cundinamarca podrá solicitar al proveedor la disminución hasta un valor mínimo establecido en el anexo: "**ANEXO ESPECIFICACIONES TÉCNICAS CONECTIVIDAD UCUNDINAMARCA"** en la Tabla 3, Disminución de BW - Fuente elaboración propia, 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.

Esta disminución de capacidades de los canales será notificada con un mes de anticipación por parte del supervisor del contrato para los efectos del pago.

TABLA 2. DISMINUCIÓN DE BW		
Clasificicón Sedes	INTERNET DEDICADO	
	CANAL2 / BW ACTUAL	CANAL2 / DISMINUIR A
Sede Fusagasugá	300	150
Seccional Girardot	90	50
Extensión Soacha	90	50
Extensión Facatativá	90	50
Extensión Chía	90	50
Extensión Zipaquirá	70	40
Seccional Ubaté	90	50
TOTAL BW	**820**	**440**

Tabla 3, Disminución de BW - Fuente elaboración propia

2. SERVICIO DE DATACENTER EN MODALIDAD COLOCATION

Actualmente la Universidad cuenta con una granja de servidores 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 (15) 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.

TABLA 3. 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	15	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							

Tabla 4, 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
-

3. 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.
Por otro lado, se espera obtener dos usuarios lectura capaces de soportar y generar investigaciones, búsquedas avanzadas, generación de reportes, monitoreo completo de los eventos de seguridad sin necesidad de contar con un tercero.

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

4. 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, que permita la conexión directa con las SEDES 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 4. REQUERIMIENTOS TECNICOS CONECTIVIDAD UCUNDINAMARCA 2022-2023									
UBICACIÓN	DIRECCIÓN	COORDENADAS	INTERNET DEDICADO		TIPO CONEXIÓN	TECNOLOGIA	SEGURIDAD PERIMETRAL (NGFW)		Sesiones concurrentes
			CANAL 1	CANAL2			Total de usuarios UCundinamarca	Concurrencia de Usuarios	
Sede Fusagasugá	Diagonal 18 # 20-29	4,334618 -74,369719	300	300	SDWAN	Fibra Óptica	4300	2800	+/- 300.000
Seccional Girardot	Calle 19 # 24-209	4,306471 -74,80653	120	90	SDWAN	Fibra Óptica	1630	1100	
Extensión Soacha	DIAGONAL 6 BIS # 5-95	4,578535 -74,223378	120	90	SDWAN	Fibra Óptica	1900	1025	
Extensión Facatativá	Calle 14 con Av. 15	4,829092 -74,355371	120	90	SDWAN	Fibra Óptica	3400	2000	
Extensión Chía	Av. Los Zipas Sector el 4 Frente a Santa Ana	4,874015 -74,038119	120	90	SDWAN	Fibra Óptica	1900	900	
Extensión Zipaquirá	Carrera 7 # 1-31	5,021682 -74,005715	90	70	SDWAN	Fibra Óptica	400	190	
Seccional Ubaté	Calle 6 # 9-80	5,30933 -73,817412	120	90	SDWAN	Fibra Óptica	1320	800	
Unidad Agroambiental La Esperanza - Fggá	Vereda Guavio Bajo (Fusagasugá)	4,276072 -74,386612	30	-	SDWAN	Radio Enlace	150	30	
Unidad Agroambiental El Tibar - Ubaté	Vereda Palogordo, sector Novilleros (Ubaté)	5,327192 -73,792056	30	-	SDWAN	Radio Enlace	120	20	
Oficina de Proyectos Especiales y Relaciones Interinstitucionales de Bogotá	Carrera 20 # 39-32	4,627996 -74,073622	35	-	SDWAN	Fibra Óptica	25	40	
Datacenter	Bogotá D.C	-	120	-	SDWAN	Fibra Óptica	**15145**	**8905**	

Tabla 5, Requerimientos Técnicos de Conectividad - Fuente: Elaboración Propia.

- Se debe incluir dos puntos de red a 10 GB en F.O. con conector LC con sus respectivos patch cord y transceivers desde el Firewall centralizado hasta los equipos Alcatel los cuales ya cuentan con sus transceivers Multimodo, esto debido a que los switches de la Universidad solo soportan este tipo de conexión.

Por otro lado, se espera obtener dos usuarios lectura capaces de soportar y generar investigaciones, búsquedas avanzadas, generación de reportes, monitoreo completo de los eventos de seguridad sin necesidad de contar con un tercero.

4.1 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.
- Las VPN’s creadas para los usuarios que pueden acceder a la red de la Universidad, deberán tener la capacidad de activar el **2FA (doble factor de autentificación)** nativo por la solucion de NGFW. Este 2FA debe estar disponible para mínimo 100 VPN’s.
- 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)
- Se debe entregar un usuario de lectura para uso de la Universidad.

4.1.1 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 Protección 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

4.1.2 Especificaciones Técnicas adicionales para los 2 equipos de seguridad perimetral centralizada en Datacenter (<u>en caso dado que entregue los equipos físicamente</u>):

- Debe soportar 16 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+

5. 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 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. 4 interfaces de red de 1 GE de RJ45 o Cobre
    v. Capacidad de recibir logs hasta de 180 equipos sin necesidad de licencias adicionales

d. Debe entregar los siguientes reportes mínimos 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

6. 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. 4 interfaces de red de 1Gbps RJ45
    iv. 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.

7. SIEM (Gestión de informes y eventos de seguridad)

La solución debe ser un sistema de monitoreo y gestión de incidentes de nueva generación dedicado, basado tecnologías de recolección, gestión, correlación y análisis de eventos tipo SIEM que le entreguen la entidad, la información suficiente para identificar y gestionar los incidentes de seguridad y desempeño que se presenten dentro de los procesos de la Universidad implementada en cada sede y el Datacenter.

El sistema de monitoreo y correlaciona de eventos debe cumplir mínimo con las siguientes características:

- **Nivel General:**

  - La solución debe tener la capacidad de monitorear y correlacionar los eventos de amenos 70 dispositivos y 2.800 eventos por segundo (EPS).
  - La solución y servicio deberán entregarse por un periodo de 12 meses, al final de este periodo, el proponente deberá entregar todos los backups de configuraciones, logs e información recolectada y retenida.
  - La solución deberá contar con agentes avanzados de monitoreo para los servidores. Estos agentes deberán poder monitorear actividad dentro de los equipos, conexiones, modificación de archivos críticos y autenticaciones.
  - La solución debe tener la capacidad de monitorear entre otros: Firewalls de nueva generación marca Fortinet, servidores Windows y Linux, switchs de acceso y distribución, servidores web y servidores de domino.
  - La solución debe ser instalada en los centros de datos de la institución de forma dedicada incluyendo los componentes de recolección de eventos, correlación y monitoreo, analítica, generación de reportes y gestión de incidentes.
  - La solución deberá ser dedicada para la universidad y no compartir recursos con otras organizaciones.
  - Con el objetivo de mantener completo control y seguimiento sobre la información de los equipos de la entidad y disminuir los retrasos en el

análisis de información, los eventos, logs y otra información recolectada, no deben en ningún momento salir de los centros de datos de la entidad y todas las funcionalidades de procesamiento, analítica y almacenamiento de esta información se debe realizar en soluciones instaladas en el centro de datos de la entidad.

- **Nivel Funcional:**

  - La solución debe tener la capacidad de analizar el estado de seguridad, disponibilidad y rendimiento de todos los dispositivos a integrar.
  - La solución debe apoyar tareas de SOC y NOC dentro de la misma plataforma.
  - La solución debe incluir como mínimo las funcionalidades de recolección (colectores, agentes o conectores), parseo, normalización, bases de datos de eventos y equipos, CMDB, correlación, monitoreo de proceso de negocio, generación y gestión de incidentes y reportes.
  - La solución de SIEM debe entregarse en formato de hardware incluyendo sus funcionalidades de almacenamiento y generación de reportes.
  - Los componentes de recolección (colectores, agentes o conectores), serán instalados en máquinas virtuales entregadas por la entidad.
  - El proponente deberá garantizar un mínimo de retención de logs de 2 meses.

- **Nivel Administración:**

  - La solución a entregar debe contar con una interfaz gráfica Web
  - Debe soportar acceso basado en roles enriquecidos para restringir el acceso a la GUI y datos en varios niveles
  - Debe permitir la Autenticación de usuario flexible: local, externa a través de Microsoft AD y OpenLDAP, Cloud SSO / SAML a través de Okta
  - El almacenamiento de eventos se debe realizar en el appliance a ofrecer basado en reglas o políticas de almacenamiento**.**

- **Nivel de Monitorización:**

- La solución debe configurarse para realizar el monitoreo y correlación de eventos de procesos de negocio de la Universidad.
- El monitoreo de estos procesos de negocios y aplicaciones debe incluir capas de aplicaciones, seguridad, servidores y datos, incluidos dentro de los 2.800 EPS solicitados
- Dentro de estas capas se encuentran dispositivos como:

    - Servidores web,
    - Servidores Windows y Linux
    - firewalls de nueva generación
    - Soluciones de seguridad en endpoint
    - Soluciones de antispam
    - Switchs y routers
    - Aplicaciones especificas

- **Nivel de Arquitectura:**

- El proponente deberá implementar todas las capas tecnológicas de la solución para la incluyendo colectores de eventos, correlacionador de eventos, herramienta o módulo de analítica, generador de reportes.
- Se debe contar con un tiempo de retención promedio de 2 meses, sin embargo, este tiempo debe estar limitado únicamente por los recursos de almacenamiento provistos y no por licenciamiento.
- La solución debe tener la capacidad de escalar de acuerdo a futuros requerimientos de la organización que incluyan la adición de nuevos procesos de negocio a monitorear, inclusión de nuevos proyectos, equipos y sistemas. Este escalamiento de capacidad debe realizarse de forma semi transparente, adicionando licenciamiento de eventos por segundo.
- El proponente debe implementar una arquitectura de recolección de eventos que garantice la menor perdida de eventos y latencia en recolección. Para esto, los elementos a monitorear deben ser accedidos por las redes internas de la institución y viajar de forma cifrada al centro de datos de la universidad.
- Los colectores o conectores a desplegar deben tener la capacidad de realizar cache de eventos cuando estos pierdan comunicación con las plataformas de correlación y análisis, así como limitar el ancho de banda usado para la recolección y envió de eventos.
- El SIEM debe garantizar la completa integridad de los eventos recolectados dentro de la operación, realizando una auditoria automatizada de la actividad de los usuarios y analistas.

- Los logs crudos recolectados por la solución o raw logs deben ser almacenados de forma segura y la solución no debe permitir su modificación por motivos de seguimiento y auditoria.
- La solución de SIEM debe estar basada en bases de datos de alto desempeño con el objetivo de garantizar un tiempo de respuesta efectivo frente a incidentes. Estas bases de datos para los eventos deben ser de alto desempeño y no relacionales como noSQL, ElasticsSearch u otras similares.
- Los componentes de recolección de logs deberán colectar, parsear y normalizar los logs una vez sean adquiridos y transmitirlos de forma comprimida al SIEM

- **Capacidades de descubrimiento, monitoreo y correlación:**

  - La solución debe realizar monitoreo en tiempo real y continuo de los eventos de seguridad, desempeño y disponibilidad de los dispositivos.
  - La solución debe tener la capacidad de realizar monitoreo del desempeño de cada equipo o aplicación a integrar, así como de los procesos que corren dentro de este.
  - La solución debe monitorear el estado y disponibilidad de servicios incluyendo DNS, FTP, servicios TCP, JDBC, LDAP SMTP SSH y servicios o aplicaciones web HTTP y HTTPS.
  - Debe recopilar sin problemas una gran variedad de métricas de rendimiento y disponibilidad para ayudar al investigador a buscar amenazas. También puede alertar cuando las métricas están fuera del perfil normal y puede correlacionar tales violaciones con problemas de seguridad para crear alertas de alta fidelidad.
  - Debe tener la capacidad de recolectar información de contexto adicional a la entregada en los eventos con técnicas como SNMP, WMI, OPSEC, JDBC, SSH y otros.
  - Debe realizar procesos de autodescubrimiento de servidores, aplicaciones dentro de los servidores, bases de datos, servicios DHCP y DNS, aplicaciones cloud, soluciones de seguridad y red.
  - Debe tener la capacidad de auto descubrir configuraciones de equipos de red y seguridad por medio de sesiones SSH o SNMP.
  - La información de autodescubrimiento y configuraciones debe ser almacenada en una base de datos de dispositivos y configuraciones de forma automática y sus campos deben estar disponibles para ser incluidos en reglas de correlación, búsquedas, dashboards y reportes
  - Esta base de datos de equipos de permitir recolectar información de cada dispositivo como información de red, geolocalización, proceso de

negocio al que pertenece, componentes y servicios que corren sobre él.

- Las soluciones y dispositivos descubiertos deben ser asignados de forma dinámica, a procesos de negocio (grupos) definidos por la universidad.
- Debe permitir definir y mantener fácilmente un proceso de negocio.
- Descubriendo automáticamente las aplicaciones que se ejecutan en los servidores, así como la conectividad de la red y el flujo de tráfico, puede elegir fácilmente las aplicaciones y los servidores respectivos y recibir una guía inteligente para elegir el resto de los componentes del servicio comercial.
- El servicio debe permitir la integración con herramientas como directorios de identidad LDAP, servicios DHCP, controladores de dominio y otros, que le permitan validar la identidad de los usuarios en cada evento y correlacionar esta identidad con sus IP, hostnames y otros
- Debe permitir la creación de casos de uso y reglas de correlación personalizadas para la entidad, así como contar con una gran cantidad de reglas predefinidas.
- El motor de reglas debe de incluir cualquier dato en una regla, por ejemplo: rendimiento y cambio de métricas junto con registros de seguridad
- Las reglas deben tener la capacidad de generar una lista de observación dinámica que puede usarse recursivamente en una nueva regla para crear una jerarquía de reglas anidadas
- Debe ejecutar una categorización de riesgo por usuario y dispositivo que le permita a la entidad conocer el riesgo actual de procesos de negoció especifico al combinar la importancia de los activos, su rol en la organización y el riesgo de los eventos identificados
- Esta categorización y rating de riesgo debe estar disponible para la Universidad en dashboars que le permitan conocer la criticidad de cada proceso de negocio y de los equipos y usuarios asociados a estos.
- La solución debe permitir que las reglas de correlación se mapeen contra la base de conocimiento MITRE ATT&CK y entregar esta información en los reportes de incidentes
- Debe contar con una suscripción de fuentes de información de amenazas y IOC actualizados periódicamente que permita incluirlos en las reglas de correlación para identificar comportamientos sospechosos.

- Debe permitir la integración nativa con fuentes de información de terceros tales como ThreatStream, CyberArk, SANS y Zeus.

- **Nivel de Análisis e investigación:**

  - La solución presentar una interfaz integrada de analítica (interfaz única de analítica e investigación) que permita la búsqueda e investigación por parte de funcionarios de la entidad.
  - Esta interfaz debe permitir la búsqueda en tiempo real y búsqueda historia de datos y patrones definidos.
  - Debe proporcionar una amplia variedad de paneles para que el usuario visualice los datos que recopila y los incidentes que se han desencadenado: paneles de resumen, paneles de widgets, panel de servicios comerciales, panel de incidentes, panel de identidad y ubicación.
  - Debe proporcionar un marco de búsqueda flexible y unificado. El usuario debe poder buscar datos basados en palabras clave o de forma estructurada utilizando atributos analizados.
  - Esta interfaz debe incluir listas de monitoreo de usuarios y equipos de alta criticidad, así como de comportamiento sospechoso.
  - Debe permitir la generación y gestión de incidentes priorizados por la criticidad del proceso de negocio afectado
  - Debe incluir un sistema de tickets incorporado para administrar incidentes a través de tickets. Admitir el ciclo de vida completo del boleto de apertura, escalado, cierre, reapertura y creación de casos con archivos adjuntos para evidencia.
  - Debe integrarse con sistemas de tickets de terceros. Cuando se produce un incidente, debe de crear un ticket en el sistema de tickets externo y vincularlo a un dispositivo existente o se puede crear un nuevo dispositivo en el sistema externo.

- **Nivel de Gestión y reportes:**

  - La solución debe tener la capacidad de implementar scripts de mitigación automáticos que pueden ejecutar una acción cuando ocurre un incidente. Los scripts pueden invocarse automáticamente cuando ocurre un incidente o pueden invocarse a pedido.
  - Debe proporcionar una gran cantidad de informes incorporados (plantillas de búsqueda), según el tipo de dispositivo y la funcionalidad, como disponibilidad, rendimiento, cambio y seguridad.

- Debe incluir una amplia cantidad de reportes predefinidos listos para usar incluyendo NERC, FISMA, ISO, SANS critical controls, NIST800-171 y otros.

- Debe permitir la configuración de nuevos informes definidos por la entidad.

- **Nivel Respuesta automatizada:**

  - Debe contar con un conjunto de respuestas pre-configuradas ante eventos de seguridad, de manera que se permita no sólo la detección sino también la remediación automatizada ante determinadas amenazas.
  - Posibilidad de ampliar esta biblioteca con desarrollo de scripts personalizados.
  - La respuesta automatizada deberá realizarla el mismo SIEM, sin requerir soluciones adicionales y deberá integrarse con las soluciones de seguridad perimetral de la Universidad, así como otras soluciones de seguridad instaladas en el ambiente IT como antimalware, EDR y otros.
  - Soportar Integración bidireccional basada en API con sistemas de help desk – integración directa para ServiceNow, ConnectWise, Jira y Remedy.

- **Componente de servicio:**

El proponente deberá contar con una malla de servicio que incluya mínimo lo siguiente:

- Implementación y configuraciones de las herramientas del SIEM incluyendo integración de los dispositivos a monitorear, creación de reglas de monitoreo y correlación, dashboards, reportes y acciones de respuesta
- Monitoreo 7 x 24 de la infraestructura del SIEM, sus componentes y los eventos que este recolecte.
- Alertamiento y gestión de los incidentes de disponibilidad detectados dentro de la herramienta
- Alertamiento y gestión de los incidentes de seguridad detectados dentro de la herramienta
- Apoyo en la investigación de incidente de seguridad que sean detectados por la herramienta

- El proponente deberá entregar a la universidad como mínimo dos (2) usuarios de monitoreo e investigación con capacidades de generar búsquedas, dashboards, monitorear e investigar detecciones y generar reportes.

8. 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

9. 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, WAF, SIEM 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 RAMÍREZ 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