-(Fusagasugá) –

ANEXO ESPECIFICACIONES TÉCNICAS AL PROYECTO: "CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA 2025-2026 "

TABLA DE CONTENIDO

1. FUNDAMENTACIÓN DEL SERVICIO DE SEGURIDAD PERIMETRAL:

Debido al contexto de la Transformación Digital actual y el crecimiento sostenido de usuarios conectados a la red, la Universidad se ha visto en la necesidad de adaptarse y evolucionar para satisfacer las demandas cambiantes de su comunidad académica y administrativa. En este sentido, se han identificado una serie de servicios esenciales, como los servicios multiplataforma, Acceso a CMA, proyecciones vía streaming, video llamadas, accesos remotos y conexiones VPN, que han experimentado un aumento significativo en su utilización.

Conscientes de la importancia de proteger la integridad de los datos y la seguridad de la red ante posibles amenazas cibernéticas, se ha mejorado sustancialmente en la arquitectura e infraestructura de la red universitaria. Este proceso de fortalecimiento y actualización tiene como objetivo no solo mejorar la capacidad de procesamiento, sino también garantizar un sistema redundante, seguro, protegido, automatizado, monitorizado y con gestión centralizada.

En este contexto, se puso un énfasis en la visibilidad en tiempo real del tráfico y las aplicaciones en cada sede universitaria. Esta capacidad de monitorización permitirá a la Universidad identificar y abordar de manera proactiva cualquier anomalía o incidente en la red, asegurando así un entorno digital seguro y eficiente para toda su comunidad.

El alcance del contrato se resume en suministrar, administrar, gestionar y operar los servicios TIC relacionados a continuación, que debe proveer el Contratista, de acuerdo con lo detallado en el presente documento

1.1. Referenciación de requisitos para el proceso de implementación:

A continuación, se describen las sedes y el detalle de las sedes a cubrir en el presente proceso:

Tabla 1. Requerimientos Técnicos - Fuente: Elaboración Propia.

ÍTEM	UBICACIÓN	DIRECCIÓN	COORDENADAS	INTERNET DEDICADO		TIPO CONEXIÓN	TECNOLOGIA	SEGURIDAD PERIMETRAL (NGFW)		Sesiones concurrentes
				CANAL 1	CANAL2			Total de usuarios UCundinamarca	Concurrencia de Usuarios	
1	Sede Fusagasugá	Diagonal 18 # 20-29	4,334618 -74,369719	600	600	SDWAN	Fibra Óptica	4500	3000	+/- 300.000
2	Seccional Girardot	Calle 19 # 24-209	4,306471 -74,80653	400	400	SDWAN	Fibra Óptica	1700	1100	
3	Extensión Soacha	DIAGONAL 6 BIS # 5 95	4,578535 -74,223378	400	400	SDWAN	Fibra Óptica	1900	1025	
4	Extensión Facatativá	Calle 14 con Av. 15	4,829092 -74,355371	450	450	SDWAN	Fibra Óptica	3400	2000	
5	Extensión Chía	Av. Los Zipas Sector el 4 Frente a Santa Ana	4,874015 -74,038119	400	400	SDWAN	Fibra Óptica	1900	900	
6	Extensión Zipaquirá Sede Nueva	Avenida Carrera 15 No 2 Sur - 200	5.01080 - 74.00192	400	400	SDWAN	Fibra Óptica	400	190	
7	Extensión Zipaquirá Sede Antigua	Carrera 7 # 1-31	5,021682 -74,005715	150	-	SDWAN	Fibra Óptica	400	190	
8	Seccional Ubaté	Calle 6 # 9-80	5,30933 -73,817412	400	400	SDWAN	Fibra Óptica	1320	800	
9	Unidad Agroambiental El Vergel - Facatativá	Vereda de Mancilla Sector puente pino - Finca El Vergel (Facatativa)	4,829092 -74,355371	30	-	SDWAN	Radio Enlace	120	30	
10	Unidad Agroambiental La Esperanza - Fggá	Vereda Guavio Bajo (Fusagasugá)	4,276072 -74.386612	30	-	SDWAN	Radio Enlace	150	30	
11	Unidad Agroambiental El Tibar - Ubaté	Vereda Palogordo, sector Novilleros (Ubaté)	5,327192 -73,792056	30	-	SDWAN	Radio Enlace	120	20	
12	Oficina de Proyectos Especiales y Relaciones Interinstitucionales de Bogotá	Carrera 20 # 39-32	4,627996 -74,073622	50	-	SDWAN	Fibra Óptica	25	40	
13	Centro Académico Deportivo CAD - Fusagasugá	Carrera 17ª No. 19-65 Piedra Grande, Fusagasugá	433646 - 74,36378	100	100	SDWAN	Fibra Óptica	100	80	
TOTAL								**16035**	**9405**	

Tabla 2. Cantidad de Usuarios - Fuente: Elaboración Propia

Tabla 2. CANTIDAD DE USUARIOS								
TIPO DE USUARIO	FUSAGASUGÁ	GIRARDOT	UBATÉ	BOGOTÁ	CHÍA	FACATATIVÁ	SOACHA	ZIPAQUIRÁ
ADMINISTRATIVOS	302	46	35	12	32	43	43	14
ESTUDIANTES	3235	1208	1228	0	1665	2885	1534	226
DOCENTES	242	137	67	0	85	169	93	56
TOTAL USUARIOS	**3779**	**1391**	**1330**	**12**	**1782**	**3097**	**1670**	**296**

1.2. Consideraciones para tener en cuenta:

- **Nivel General:**
  - La solución deberá ser dedicada para la universidad y no compartir recursos con otras organizaciones.

- **Nivel Funcional:**
  - La solución debe apoyar tareas de NOC dentro de la misma plataforma.
- **Nivel Administración:**
  - La solución para entregar debe contar con una interfaz gráfica Web.

- **Nivel de Monitorización:**
  - La solución debe configurarse para realizar el monitoreo y correlación de eventos de procesos de negocio de la Universidad.

- **Nivel de Arquitectura:**
  - 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.

- **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.

- **Nivel de Análisis e investigación:**

  - Debe incluir un sistema de tickets incorporado para administrar incidentes a través de dicha herramienta. Admitir el ciclo de vida completo del boleto de apertura, escalado, cierre, reapertura y creación de casos con archivos adjuntos para evidencia.

Tabla 2. Contratación del Servicio de Seguridad Perimetral - Fuente: Elaboración Propia

Marca	Modelo	Unidades de rack	"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
Servicio de SEGURIDAD PERIMETRAL en Alta Disponibilidad (Firewalls de Nueva Generación) en modo ACTIVO-ACTIVO PARA EL DATACENTER DE LA UNIVERSIDAD DE CUNDINAMARCA.														
Servicio de WEB APLICATTION FIREWALL (WAF) para proteger aplicaciones propias y de terceros alojadas en servidores de la Universidad de Cundinamarca en datacenter propiedad del proveedor.											99.98%	Tier III	40	7x24x365 Manos Remotas
SERVICIO DE DE GESTIÓN CENTRALIZADA DE LOGS Y REPORTES PARA PROPORCIONAR UNA MEJOR PROTECCIÓN DE CIBERSEGURIDAD														
SERVICIO DE SIEM (Gestión de informes y eventos de seguridad)														

2. CONFIGURACIÓN DE LA RED DE INTERNET MEDIANTE TECNOLOGÍA SD- WAN

Actualmente la Universidad de Cundinamarca requiere de 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 Unidades Regionales deben contar con 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.

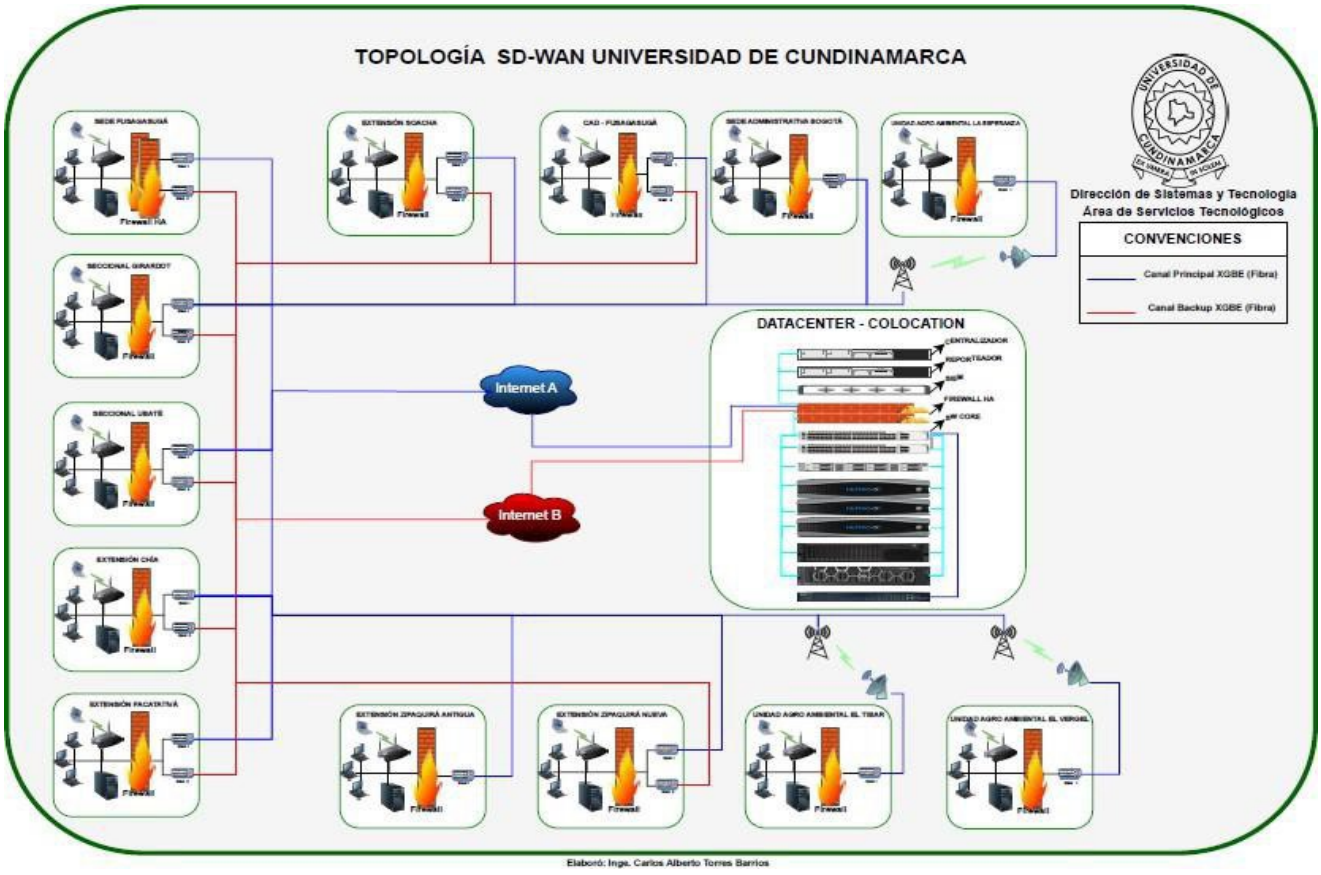
Nota Aclaratoria N°1: Actualmente, la sede FUSAGASUGÁ cuenta con el NGFW de marca FORTINET de referencia FG-600E, el cual debe ser configurado como Switch Core en la SEDE FUSAGASUGÁ, adicionalmente el contratista debe proporcionándole el licenciamiento y soporte con fabricante para su correcto funcionamiento.

Nota Aclaratoria N°2: Todos los firewalls deben tener licenciamiento que incluya IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, soporte de fábrica. y orquestación central.

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, obteniendo la siguiente topología de red.

-(Fusagasugá) –

Ilustración 1 - Topología Deseada - Fuente: Elaboración Propia.



a. SERVICIO DE SEGURIDAD PERIMETRAL Y SD-WAN

i. Appliance de seguridad perimetral deben tener la funcionalidad nativa de SD-WAN. Éstos irán ubicados en las Unidades Regionales de la Universidad de Cundinamarca: SEDE FUSAGASUGÁ (DOS (2) Appliance en HA), EXTENSIÓN CHÍA, EXTENSIÓN ZIPAQUIRÁ SEDE NUEVA, EXTENSIÓN ZIPAQUIRÁ SEDE ANTIGUA, SECCIONAL GIRARDOT, EXTENSIÓN SOACHA, EXTENSIÓN FACATATIVÁ, SECCIONAL UBATÉ, OFICINA DE PROYECTOS ESPECIALES BOGOTÁ, UNIDAD AGROAMBIENTAL EL TIBAR (UBATÉ), UNIDAD AGROAMBIENTAL LA ESPERANZA (FUSAGASUGÁ), UNIDAD AGROAMBIENTAL EL VERGEL (FACATATIVÁ) y CENTRO ACADÉMICO DEPORTIVO – CAD (FUSAGASUGÁ)(corresponde a la especificación técnica item 2) y DATACENTER (BOGOTÁ O ALREDEDORES) (corresponde a la especificación técnica item 6); su distribución, cantidad por sede, seccional o extensión y características mínimas de los equipos se encuentran en el ***ítem b. especificaciones técnicas mínimas.***
ii. Todas las sedes, deberán ir conectadas hacia Datacenter por medio de la red de SD-WAN con el NGFW de alta disponibilidad que debe ir en Datacenter.
iii. 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.
iv. Enrutamiento por Aplicaciones, definiendo cuales son las más críticas y sobre las que se dará prioridad en el tráfico desde y hacia Datacenter.
v. 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.
vi. Gestión centralizada por medio de una herramienta que administre todo el conjunto de NGFW, para garantizar una visión completa de la solución.
vii. Gestión centralizada por medio de una herramienta que administre todo el conjunto de NGFW, para garantizar una visión completa de la solución.
viii. Detección y prevención coordinadas en tiempo real contra contenido, aplicaciones, personas y dispositivos conocidos y desconocidos.
ix. Identificación y control de aplicaciones: 5000+ firmas de aplicaciones, identificación del primer paquete, inspección profunda de paquetes, firmas de aplicaciones personalizadas, descifrado SSL, TLS1.3 con cifrados obligatorios e inspección profunda.
x. SD-WAN (control de tráfico con reconocimiento de aplicaciones): Políticas de aplicaciones granulares, selección de rutas basada en SLA de aplicaciones, medición dinámica del ancho de banda de rutas SD-WAN, reenvío activo/activo y activo/en espera, soporte de superposición para transporte cifrado, dirección basada en sesión de aplicaciones, mediciones de SLA basadas en sondas
xi. SD-WAN avanzada (corrección de WAN): Corrección de errores de reenvío (FEC) para la compensación de pérdida de paquetes, duplicación de paquetes

para el mejor rendimiento de las aplicaciones en tiempo real, integración de Active Directory para políticas de dirección SD-WAN basadas en el usuario, agregación de enlaces por paquete con distribución de paquetes entre miembros agregados

xii. Implementación de SD-WAN: Implementación flexible hub-to-spoke (malla parcial), spoke-to-spoke (malla completa), multi-WAN.

xiii. Modelado del tráfico QoS basado en límites de ancho de banda por aplicación y enlace WAN, límites de velocidad por aplicación y enlace WAN, priorización del tráfico de aplicaciones por enlace WAN, marca/remarca bits DSCP para influir en la QoS del tráfico en dispositivos de salida, dirección de aplicaciones basada en el marcado ToS.

xiv. Enrutamiento avanzado (IPv4/IPv6): Enrutamiento estático, puerta de enlace interna (iBGP, OSPF v2/v3, RIP v2), puerta de enlace externa (eBGP), VRF, redistribución de rutas, fuga de rutas, confederación BGP, reflectores de enrutador, resumen y agregación de rutas, asimetría de rutas.

xv. VPN/Overlay: Site-to-site ADVPN - túneles VPN dinámicos, VPN basado en políticas, IKEv1, IKEv2, DPD, PFS, ESP y soporte ESPHMAC, Compatibilidad con cifrado simétrico (IKE/ES P): AES- 128 y AES-256 modos: CBC, CNTR, XCBC, GCM, Pre-shared and PKI authentication con certificados RSA, intercambio de claves.

xvi. Diffie-Hellman (Group 1, 2, 5, 14 through 21 and 27 through 32), MD5, y SHA-based HMAC.

xvii. Multicast: Multicast forwarding, PIM spare (rfc 4601), dense mode (rfc 3973), PIM rendezvous point.

xviii. Networking Avanzado: DHCP v4/v6, DNS, NAT - source, destino, NAT estático, destination NAT, PAT, NAPT, Soporte Full IPv4/v6.

xix. Seguridad On-premise: - Inspección SSL, control de aplicaciones, prevención de intrusiones, antivirus, filtrado web, DLP y protección avanzada contra amenazas. Segmentación: micro, macro, VDOM de una sola tarea, VDOM múltiple.

xx. La herramienta de administración de SD-WAN debe proporcionar aprovisionamiento sin contacto (zero tocuh), configuración centralizada, gestión de cambios, panel de control, políticas de aplicaciones, QoS, políticas de seguridad, SLA específicos de la aplicación, configuración de sonda activa, RBAC, multiusuario. Además, debe proporcionar analítica mejorada que inclya: Consumo de ancho de banda, métricas de SLA: fluctuación, pérdida de paquetes y latencia, monitoreo en tiempo real, filtro basado en intervalo de tiempo, informes de SLA de enlace WAN, uso de sesión por aplicación, información de amenazas: firma de malware, dominio o URL de malware, host infectado, nivel de amenaza, categoría de malware, indicador de compromiso.

xxi. Integraciones de la solución de SD-WAN: RESTful API/Ansible para configuración, aprovisionamiento sin intervención, informes e integración de terceros.

xxii. La solución de SD-WAN debe figurar como líder en el cuadrante mágico de Garner para SD-WAN de 2024.

b. Especificaciones Técnicas Mínimas para equipos SD-WAN

i. Se requieren CINCO (5) NGFW que se instalarán de la siguiente manera: en la **SEDE FUSAGASUGÁ** DOS (2) NGFW en HA, para el **DATA CENTER** DOS (2) NGFW en HA y UNO (1) NGFW para la **EXTENSIÓN FACATATIVÁ**. Cada dispositivo debe cumplir con las siguientes características mínimas:

Rendimiento
El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:
• Rendimiento de Firewall 100 Gbps
• Rendimiento de IPS 12 Gbps
• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 11 Gbps
• Rendimiento Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 10 Gbps
• Rendimiento IPSec VPN 50 Gbps
• Soporte de 7 Millones sesiones concurrentes
• Rendimiento de Inspección SSL 3 Gbps
• Soporte de 5000 usuarios VPN SSL concurrentes
• Rendimiento de VPN SSL 3 Gbps
Conectividad
El equipo deberá contar con las siguientes interfaces de conexión:
• 16 interfaces de 1 GE RJ45
• 8 interfaces de 1 GE SFP
• 4 interfaces de 10 GE SFP+. Cada equipo debe incluir dos (2) Transceivers 10GE SFP+ LC

Para los equipos del DATACENTER se deben tener en cuenta:

- 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.
- Por otro lado, se espera obtener un usuario con permisos capaces de Administrar usuarios, configurar de políticas de seguridad, control de aplicaciones, administración de dispositivos, monitoreo y generación de informes con el fin de tener una administración compartida del firewall junto al oferente adjudicado del presente proyecto.
- El oferente que resulte adjudicado debe instalar, configurar e implementar los

equipos en el Data Center bajo modalidad de Colocation, de acuerdo con la necesidad de la Universidad.

- La Universidad de Cundinamarca, gestionará todos los permisos de ingreso y demás procesos que se requieran al proveedor que resulte adjudicado en la contratación del servicio de colocation para que se realice el despliegue e implementación de la seguridad perimetral en las diferentes Unidades Regionales donde hace presencia la Universidad.
- Se deberán realizar como mínimo dos pruebas de conmutación de los firewalls de Datacenter durante la vigencia del contrato, esto con la finalidad de asegurar que él HA se encuentra funcionando correctamente. Estas pruebas deberán ser coordinadas con la Dirección de Sistemas y Tecnología y no pueden generar indisponibilidad en los servicios prestados a la Universidad de Cundinamarca

ii. Se requieren CUATRO (4) NGFW que se instalarán en las Unidades Regionales SECCIONAL GIRARDOT y UBATÉ, EXTENSIÓN SOACHA y CHIA. Actualmente, la sede FUSAGASUGÁ cuenta con el NGFW de marca FORTINET de referencia FG-600E, el cual debe ser configurado como Switch Core en la SEDE FUSAGASUGÁ, adicionalmente el contratista debe proporcionándole el licenciamiento y soporte con fabricante para su correcto funcionamiento.

Rendimiento
El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:
• Rendimiento de Firewall 35 Gbps
• Rendimiento de IPS 8 Gbps
• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 7 Gbps
• Rendimiento Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 6 Gbps
• Rendimiento IPSec VPN 10 Gbps
• Soporte de 3 Millones sesiones concurrentes
• Rendimiento de Inspección SSL 3 Gbps
• Soporte de 500 usuarios VPN SSL concurrentes
• Rendimiento de VPN SSL 2 Gbps
Conectividad
El equipo deberá contar con las siguientes interfaces de conexión:
• 8 interfaces de 1 GE RJ45
• 2 interfaces de 10 GE SFP+. Cada equipo debe incluir un (1) Transceiver 10GE SFP+ LC

iii. Se requieren SIETE (7) NGFW que se instalarán en las unidades regionales EXTENSIÓN ZIPAQUIRÁ SEDE NUEVA, EXTENSIÓN ZIPAQUIRÁ SEDE ANTIGUA, OFICINA DE PROYECTOS ESPECIALES - BOGOTÁ, UNIDAD AGROAMBIENTAL TIBAR (UBATÉ), UNIDAD AGROAMBIENTAL LA ESPERANZA (FUSAGASUGÁ), UNIDAD AGROAMBIENTAL EL VERGEL (FACATATIVÁ) y CENTRO ACADÉMICO DEPORTIVO – CAD (FUSAGASUGÁ).

Rendimiento
El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:
• Rendimiento de Firewall 25 Gbps
• Rendimiento de IPS 5 Gbps
• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 3 Gbps
• Rendimiento Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 2.5 Gbps
• Rendimiento IPSec VPN 10 Gbps
• Soporte de 2 Millones sesiones concurrentes
• Rendimiento de Inspección SSL 1 Gbps
• Soporte de 200 usuarios VPN SSL concurrentes
• Rendimiento de VPN SSL 1 Gbps
Conectividad
El equipo deberá contar con las siguientes interfaces de conexión:
• 16 interfaces de 1 GE RJ45
• 2 interfaces de 10 GE SFP+. Cada equipo debe incluir un (1) Transceiver 10GE SFP+ LC

c. Funcionalidades Generales de los NGFW Ofertados

Cada uno de los NGFW ofertados para el DATACENTER y sedes descritas deben cumplir mínimo con las siguientes funcionalidades:

Adquisición de Appliance de seguridad informática perimetral por sede con sistema operativo propietario del fabricante, que sea del tipo Firewall de Nueva Generación, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento.
La solución debe estar en la capacidad de soportar alta disponibilidad.
El dispositivo debe ser equipos de propósito específico.
El dispositivo debe contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de trafico
La solución deberá pertenecer al cuadrante de líder de Gartner para su última edición de Network Firewall
La solución deberá estar calificada como recomendada en el SVM de firewall de NSS LABS
Address Traslation
La plataforma debe soportar lo siguiente tipos de traducción de direcciones:
• NAT y PAT
• NAT estático

• NAT: destino, origen
• NAT, NAT64 persistente
Funciones básicas de Firewall
Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
La solución debe integrarse con el directorio activo y soportar políticas basadas en idUniversidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada
Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS,Azure,Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP,TAG etc) de la instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall
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 trafico 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.
Conectividad y Enrutamiento
Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP
La solución podrá habilitar políticas de ruteo en IPv6
La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.
La Solución deberá soportar balanceado de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)
VPN IPSEC
El equipo deberá soportar las siguientes características:
Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
Soporte para IKEv2 y IKE Configuration Method.
Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES
Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits
VPN SSL
Capacidad de realizar SSL VPNs por usuarios sin incurrir en costos adicionales.
Soporte a certificados PKI X.509 para construcción de VPNs SSL.
Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
Autenticación
El dispositivo deberá manejar los siguientes tipos de autenticación:

Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+.
Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”.
Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID.
Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo.
Manejo de tráfico y calidad de servicio.
Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente
Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión
Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general.
Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo
Antimalware
Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.MAPI
El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma.
Debe soportar la inspección de archivos comprimidos como los son: GZIP,RAR,LZH,IHA,CAB,ARJ;ZIP entre otros con el fin de proteger contra estas técnicas de evasión.
El Antivirus deberá integrarse de forma nativa con una solución sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.
Filtrado WEB
Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos.
Debe poder categorizar contenido Web requerido mediante IPv6.
Será posible exceptuar la inspección de HTTPS por categoría.
Debe contar con la capacidad de bloquear contenido de youtube usando el Channel ID
El filtrado debe ser sobre tráfico http y https.
Protección contra intrusos (IPS)
El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.
Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.
Capacidad de detección de más de 7000 ataques.
El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, 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.
Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.
Control de Aplicaciones
La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante.
Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión
Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.
Inspección de Contenido SSL/SSH
La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura
Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad.
La inspección deberá realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection.
Alta Disponibilidad
El dispositivo deberán soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6
Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico.
El equipo debe soportar hasta 2 equipos en esquema de HA.
Visibilidad
La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional.
Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma.
De las aplicaciones Cloud como Dropbox que permiten compartir archivos, debe ser posible ver que archivos fueron subidos y descargados por los usuarios.
Características de Administración
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)
Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión
Debe estar en capacidad de administrar switches y Access point para generar una red SD-LAN administrada y gestionada desde el mismo Firewall.

Virtualización
El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”
Debe soportar e incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer.
Cada instancia virtual debe poder tener un administrador independiente
Licenciamiento y actualizaciones
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.
El licenciamiento debe incluir servicios de IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, y soporte de fábrica durante la vigencia del contrato.

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, en alta disponibilidad (HA), 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 de 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.

A continuación, los requerimientos mínimos:

Requerimiento Técnico Mínimo (de obligatorio cumplimiento)
GENERALIDADES
La solución debe permitir fácil y rápidamente implementar controles basado en políticas internas hacia los servidores web de la Universidad.
La solución debe poder restaurar los portales web de forma automática en caso de presentarse una modificación no autorizada.
La plataforma propuesta debe identificar vulnerabilidades a un número ilimitado de aplicativa web de la Universidad, sin requerir licenciamiento adicional.
La solución debe contar con sus respectivas actualizaciones periódicas a nivel de firmas de seguridad durante el periodo contratado.
La solución debe ser totalmente compatible con IPv6.

La solución debe poderse implementar en modo proxy reverso, transparente o monitoreo. Sin embargo, en conjunto con la Universidad se definirá la mejor opción a nivel de configuración de seguridad.
Integrarse de forma nativa a la actual solución de Gestión de Logs y reportes de la Universidad.
La solución debe contar con características de Machine Learning.
La solución debe soportar alta disponibilidad Activo/Pasivo y Activo/Activo
Cebe incorporar funcionalidad de análisis de amenazas
Debe incorporar funcionalidad de Sandbox Cloud
La solución de Web Application Firewall debe tener la capacidad de enviarle las IP detectadas como maliciosas sean informadas y sea adicionada automáticamente a un grupo de direcciones IPs para que puedan ser utilizadas en las políticas de la plataforma de NGFW.
CARACTERISTICAS MINIMAS DE DESEMPEÑO
Throughput WAF HTTP mínimo de 100 Mbps, este rendimiento deberá ser verificable por documentación pública, por lo cual no se aceptarán cartas de fabricante para cumplir con este ítem.
Latencia mínimo 5 ms
Interfaces: 4 puertos 10/100/1000 RJ45
Licencias de aplicaciones: Ilimitadas El número de Aplicaciones a proteger no deberá estar limitado por licenciamiento.
FIREWALL DE APLICACIONES WEB
La solución debe integrar firmas de amenazas y ataques conocidos y deberá proteger de ataques nuevos o de día cero actualizándose durante el tiempo de la garantía.
Cross-Site Scripting (XSS)
SQL Injection
Remote File Inclusión
Local File Inclusión
OS Commands
Troyanos y virus
Exploits
Información Sensible del servidor
Fujas de Información
Firmas personalizadas
Con esto la herramienta debe ser capaz de proteger de las siguientes amenazas:
- Adobe Flash Binary (AMF) protocol Attack.
- Botnet
- Browser Exploit Against SSL /TLS
- Clickjacking
- Cookie Tampering
- Credit Card Theft
- Cross Site request forgery
- Cross site Scripting
- DoS
- HTTP Header Overflow

-	Local File Inclusion
-	Malicious Robots
-	Man in the Middle
-	Remote File Inclusion
-	Server information leakage
-	SQL Injection
-	Malformed XML

PROTECCION DE WEB DEFACEMENT

Con el fin de garantizar la reputación de la Universidad y la integridad de las aplicaciones web, la solución deberá contar con un módulo de anti-defacement el cual permita monitorear las aplicaciones, alertar y de ser necesario restaurar de forma automática en caso de modificaciones no autorizadas de las aplicaciones web protegidas, la solución deberá poder monitorear la integridad de los archivos por medio de FTP, SSH o SMB, por lo tanto no se acepta soluciones que requieran la instalación de agentes, los cuales agreguen más carga a los servidores.

ANALISIS DE VULNERABILIDADES

La solución debe realizar análisis de vulnerabilidades sobre las aplicaciones web protegidas, de tal forma que se identifiquen vulnerabilidades existentes en los aplicativos webs de la Universidad de forma ilimitada, sin requerir licenciamiento adicional.

PROTECCION DE DDOS (DENEGACION DE SERVICIO)

La solución debe contar con un módulo de prevención contra ataques de denegación de servicio en http y https de tal forma que proteja a las aplicaciones web contra este tipo de ataques, dicho módulo deberá permitir como mínimo las siguientes acciones:

-	Alertar.
-	Denegar.
-	Bloquear por un Periodo de Tiempo.

MACHINE LEARNING

La solución deberá contar con la funcionalidad de auto aprendizaje de aplicaciones, la cual permita crear una línea base del comportamiento de la aplicación para creación de diferentes políticas de protección de un número ilimitado de aplicaciones web.

ANTIMALWARE

La solución deberá contar con un módulo de escaneo AntiMalware para hacer una revisión de los archivos que sean posteados o subidos a las aplicaciones web, permitiendo ejecutar Detección y bloqueo de malware conocido a nivel de los archivos que se suben a las aplicaciones web.

PROTECCION DE GEOLOCALIZACION

La solución debe contar con protección de ataques basados en la localización geográfica del atacante

PROTECCION DE FUGA DE INFORMACION

La solución debe contar con un módulo para la prevención de fuga de información, la cual permite crear reglas personalizadas basadas en patrones, este módulo deberá ser completamente funcional sin requerir licencias adicionales o integraciones con plataformas de terceros.

AUTENTICACION

La solución debe permitir la creación de reglas de autenticación, dichas reglas de autenticación deberán permitir:	
Autenticación por medio de LDAP o Radius.	
Autenticación de doble factor por medio de Token.	
(SSO) Single Sign-On para portales tales como OWA, SharePoint, etc.	
PREVENCION DE FUERZA BRUTA	
La solución debe contar con un módulo que prevenga ataques de fuerza bruta contra los portales de autenticación de la Universidad, el cual permita bloquear por un periodo de tiempo al atacante, dicho periodo de tiempo deberá poder ser parametrizado por la Universidad.	
VALIDACION DEL PROTOCOLO HTTP	
La solución debe tener la capacidad de validar el protocolo HTTP, haciendo una revisión como mínimo de los siguientes parámetros:	
-	Hostname.
-	Versión Http.
-	Método del Request.
-	Tamaño del Request.
-	Tamaño del Contenido.
-	Tamaño del Body.
-	Tamaño del Header.
-	Numero de Cookies en el request.
-	Numero de Parámetros en la URL.
ADMINISTRACION Y GESTION DE PLATAFORMA	
Gestión vía HTTPS y CLI.	
Deberá contar con API por medio del método RESTful sobre HTTPS.	
La solución debe contar con dashboards, que muestren como mínimo información en tiempo real del tráfico, Historia de Ataques, sesiones por política e información del sistema.	
Menú tipo dropdown para navegar por la información	
Mostrar los orígenes del tráfico o usuarios que generan tráfico.	
Mostrar las aplicaciones y su categorización según riesgo.	
Visibilidad de destinos del tráfico.	
Visibilidad de los sitios web más consultados por los usuarios.	
Visibilidad de las amenazas que han ocurrido en la red.	

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 y el equipo actualmente ubicado en la sede

Fusagasugá.

c. La solución de análisis de logs debe contar con las siguientes características:

Generalidades
Se requiere un (1) equipo tipo Appliance físico de propósito específico que permita registrar cada transacción de la plataforma de seguridad perimetral de la Universidad, para poder identificar y reaccionar a cualquier informe emitido por un log o registro de los dispositivos de seguridad perimetral ofertados tales como el Firewall de Nueva Generación y el Firewall de Aplicaciones web requerido.
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 el Firewall de Aplicaciones web requerido.
La solución de analítica, logs y reportes debe tener la capacidad en enviar eventos a la plataforma de NGFW y que estos actúen como triggers de acciones automáticas
Desempeño
La solución de análisis de logs debe dar soporte a las siguientes características:
- Capacidad de recibir hasta 200 GB de logs diarios.
- Capacidad de Almacenamiento de 8 Terabytes
- Tasa analítica sostenida (logs/seg): 4000
- Tasa sostenida del colector (registros/seg): 6000
Funciones y configuraciones requeridas para el analizador de red
Visor de tráfico en tiempo real.
Visor de tráfico histórico.
Visor personalizado de log de tráfico
Herramienta de búsqueda sobre los logs de tráfico.
Debe ser compatible con el equipo FG-600E que tiene la Universidad
Análisis de logs y reportes requeridos
Vista de búsqueda y manejo de logs.
Reportes basados en perfiles.
Inventario de plantillas predefinidas para reportes regulares.
Debe soportar de forma predefinida los reportes:
Eventos del sistema
Análisis de riesgo y aplicaciones
Reporte de Aplicaciones y Ancho de Banda
Reputación de Clientes
Análisis de seguridad
Reporte de Amenazas
Reportes de VPN

Reportes de uso de Web
Reporte con análisis completo de su postura de seguridad, incluidos informes de calificación de seguridad, calificación de seguridad para PCI, Secure SD-WAN, VPN, evaluaciones de amenazas cibernéticas, revisiones de seguridad 360, conciencia situacional, cumplimiento, auditoría.
Debe ser posible calendarizar los reportes
La plataforma deberá permitir integrar los logs del FG-600E que posee actualmente la Universidad.

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 cuenten 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

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.

Se deben cumplir con las siguientes especificaciones mínimas:

Requerimiento
La gestión de la solución debe soportar acceso por SSH, cliente o WEB (HTTPS) y API abierta.
Debe permitir accesos concurrentes de administradores.
Debe tener interfaz basada en línea de comando para administración de la solución de gestión;
Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos.
Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores.
Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura, creación de usuarios, cambio de configuraciones.
Generar alertas automáticas por Email:

• Generar alertas automáticas por SNMP • Generar alertas automáticas por Syslog
Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horário;
Debe ser permitido al administrador transferir los backups a un servidor FTP.
Debe ser permitido al administrador transferir los backups a un servidor SCP
Debe ser permitido al administrador transferir los backups a un servidor SFTP
Los cambios realizados en un servidor de gestión deben ser automáticamente replicados al servidor redundante;
Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuarios LOCALES
Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa TACACS
Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa LDAP
Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de base externa RADIUS
Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de Certificado Digital X.509 (PKI)
Debe soportar sincronización de reloj interno por protocolo NTP.
Debe registrar las acciones efectuadas por cualquier usuario;
Debe suportar SNMP versión 2 y la versión 3 en los equipos de gestión;
Debe permitir habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Telnet;
Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado.
La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización.
Debe soportar XML API y JSON API
FUNCIONALIDADES DE GESTION DE NGFW
La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación
La gestión debe permitir la creación y administración de políticas de IPS, Antivírus y Anti-Spyware
La gestión debe permitir la creación y administración de políticas de Filtro de URL
Permitir buscar cuáles reglas un objeto está siendo utilizado
Debe atribuir secuencialmente un número a cada regla de firewall
Permitir la creación de reglas que permanezcan activas en horario definido
Permitir backup de las configuraciones y rollback de configuración para la última configuración salva
Debe tener mecanismos de validación de políticas avisando cuando haya reglas que ofusquen o conflictúen con otras (shadowing)

Debe posibilitar la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas
Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión
Cada servidor de gestión debe ser hospedado en un equipo independiente, no ejecutando función de firewall
La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta
La solución debe permitir la distribución e instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos
Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados
Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador
Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de estos.
Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados cuando el mismo es agregado a la solución de gestión
Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware
Tener "wizard" en la solución de gestión para instalación de políticas y configuraciones de los dispositivos
Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración
Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos
Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión
Permitir configurar y visualizar balanceo de enlaces en los dispositivos gestionados de forma centralizada
Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos
Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada
Permitir la creación de reglas anti DoS de forma centralizada
Permitir la creación de objetos que serán utilizados en las políticas de forma centralizada
Permitir manejar las políticas de seguridad en entornos híbridos y multicloud con plantillas de configuración para IPSec, BGP, CLI y reglas SD-WAN
Permitir políticas de SD-WAN centradas en las aplicaciones para ajustar las decisiones de direccionamiento del tráfico en función de los objetivos del acuerdo de nivel de servicio (SLA) de rendimiento para cada proveedor de WAN

Debe permitir utilizar informes y paneles de monitoreo de SD-WAN para monitorear de cerca el rendimiento de las aplicaciones, incluidas las métricas de ancho de banda, latencia, fluctuación y pérdida de paquetes
Permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topología (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía

6. 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:

GENERALIDADES
Analítica de red en tiempo real Seguridad y conformidad listas para usar Un único panel de Administración Arquitectura a escala de la nube Autoaprendizaje del Inventario de activos (CMDB) Correlación cruzada de analítica de SOC y NOC Asignaciones de reglas de TI e ICS de MITRE ATT&CK y visibilidad de la cobertura
Debe ser un (1) Appliance de propósito específico de que debe incluir como mínimo: • Memoria: DDR4 128GB • Capacidad de almacenamiento: 7 TB • Mínimo: 4 puertos 1GE RJ45 y 2 puertos 25GE SFP28. Debe incluir 2 módulos transceiver 25 GE / 10 GE SFP28
DIMENSIONAMIENTO
Se solicita el siguiente dimensionamiento mínimo:
Numero de dispositivos licenciados: 200
Cantidad EPS (Eventos por segundo): 2000
Número de puntos de IoC: 50
CONTEXTO EN TIEMPO REAL PARA ANALISIS DE SEGURIDAD QUE INCLUYA
Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución.
Análisis del rendimiento de aplicaciones y sistemas junto con datos del entorno para identificar rápidamente problemas de seguridad.

Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de id Universidad de usuario, contexto de datos de ubicación física y geo-localización.
Infraestructura de la nube incluyendo AWS.
Dispositivos ambientales como UPS, HVAC, hardware del dispositivo.
Infraestructura de virtualización incluyendo VMware ESX, Microsoft HyperVScalable .

RECOLECCION DE LOGS ESCALABLE Y FLEXIBLE
Soporte inmediato para una amplia variedad de sistemas de seguridad y APIs de proveedores - tanto locales como en la nube.
Los agentes de Windows proporcionarán una colección de eventos altamente escalable y rica, incluida la supervisión de integridad de archivos, los cambios de software instalados y la supervisión de cambios en el registro.
Agentes de Linux para la supervisión de integridad de archivos.
Capacidad de hash de ficheros vía File Integrity Monitoring utilizando SHA256.
Protección de la integridad de los logs almacenados en la plataforma utilizando SHA256.
Capacidad para modificar los analizadores directamente desde la interfaz gráfica de usuario y aplicarlos en el sistema en ejecución sin pérdida de tiempo de inactividad y de evento.
Creación de nuevos analizadores (plantillas XML) a través del entorno de desarrollo integrado y capacidad para compartir a través de la función de exportación / importación.
Recopilación segura y fiable de eventos para usuarios y dispositivos ubicados en cualquier lugar.
NOTIFICACION Y GESTION DE INCIDENTES
Framework de notificación de incidentes basado en políticas.
Posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico.
Integración basada en API a sistemas externos de ticketing - ServiceNow, Salesforce, ConnectWise, Remedy y Jira.
Sistema incorporado de ticketing.
PANALES DE CONTROL PERSONALIZADOS
Dashboards configurables en tiempo real, con desplazamiento "Slide-Show" para mostrar KPIs.
Informes y análisis exportables entre organizaciones y usuarios.
Identificación rápida los problemas críticos, por ejemplo, a través de un código de colores.
Actualización rápida mediante el cálculo en memoria, sin acceso a disco.
Dashboards especializados para servicios empresariales, infraestructura virtualizada y aplicaciones especializadas.
INTEGRACION CON FUENTES DE INTELIGENCIA EXTERNA
Búsqueda de eventos en real - sin necesidad de indexación.
Búsquedas por palabras clave basadas en atributos de eventos analizados.
Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API.
Match de patrones complejos en tiempo real.
Uso de objetos CMDB y datos de usuario/idUniversidad y ubicación en búsquedas y reglas.

Programación de informes y entregas de resultados por correo electrónico.
Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.).
Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico.
Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.
Análisis escalable mediante la adición de nodos worker en caliente.
Posibilidad de priorización de los informes de incidentes.
ANALITICA
Búsqueda de eventos en real - sin necesidad de indexación.
Búsquedas por palabras clave basadas en atributos de eventos analizados.
Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API.
Match de patrones complejos en tiempo real.
Uso de objetos CMDB y datos de usuario/id Universidad y ubicación en búsquedas y reglas.
Programación de informes y entregas de resultados por correo electrónico a los principales interesados.
Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.).
Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico.
Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.
Soporte de análisis escalable mediante la adición de nodos worker en caliente.
Posibilidad de priorización de los informes de incidentes.
DETECCION DE ANOMALIAS
Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana.
Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base.
Disparadores incorporados y personalizables sobre anomalías de comportamiento.
INTEGRACIONES DE TECNOLOGIA EXTERNA
Integración con cualquier sitio web externo para la búsqueda de direcciones IP.
Integración basada en API para fuentes externas de inteligencia de amenazas.
Integración bidireccional basada en API con sistemas de help desk – integración directa para ServiceNow, ConnectWise, Jira y Remedy.
Integración bidireccional basada en API con CMDB externas – directamente soportado para ServiceNow y ConnectWise.
Soporte de Kafka para la integración con informes mejorados de análisis, por ejemplo, ELK, Tableau y Hadoop.
API para una fácil integración con sistemas de aprovisionamiento.
API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.
ADMINISTRACION
GUI basada en web, a ser posible HTML5.

Control de acceso basada en roles para restringir el acceso a la GUI y a los datos.
Todas las comunicaciones entre módulos están protegidas por HTTPS.
Auditoría completa de la actividad del usuario.
Fácil actualización de software con un mínimo tiempo de inactividad y pérdida de eventos.
Actualización de la base de conocimientos (analizadores, reglas, informes) sencilla.
Archivado basado en políticas.
Hashing de registros a tiempo para no repudio y verificación de integridad.
Autenticación de usuario flexible – local, y externa a través de Microsoft AD y OpenLDAP, Cloud SSO/SAML a través de Okta.
ESCALABILIDAD
Escalabilidad de recolección de datos mediante la implementación de máquinas virtuales con la función de recolección (colectores virtuales).
Los recolectores deben poder almacenar en búfer eventos cuando la conexión no esté disponible.
Escalado del análisis mediante la implementación de nuevas máquinas virtuales.
Arquitectura de balanceo integrada para recoger eventos desde sitios remotos usando recolectores
SUPERVISION DE DISPONIBILIDAD
Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento.
Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP.
Monitorización del hardware y del entorno.
Calendario para la programación de las ventanas de mantenimiento.
Cálculo de SLA – consideración de las horas normales de trabajo y fuera de horas.
ALMACENAMIENTO
Posibilidad de implementar almacenamiento online vía ElasticSearch (ELK).
Soporte de archivado de logs tanto para NFS como HDFS.
Creación de políticas de retención de logs tanto por espacio como por periodos de tiempo.
INTEGRACION
La solución debe incluir conectores desarrollados con las soluciones de NGFW, WAF y SDWAN ofertadas. En caso de no ser incluidos, deben ser contemplados en la oferta servicios directos del fabricante para el desarrollo de estos.
LICENCIAMIENTO
Debe ser una solución licenciada y con soporte directo de fábrica. No se aceptan soluciones Opensource.
El fabricante ofertante deberá disponer de un método de licenciamiento escalable tanto por número de dispositivos como por EPS asociados, pudiendo elegir al menos entre licencias perpetuas y modo suscripción.
Se deberá disponer de otras suscripciones como Indicadores de Compromiso (IoC).
Se deberá poder añadir EPS adicionales sin necesidad de contratar soporte asociado a los mismos.
Se podrán desplegar tantos colectores virtuales como se quiera sin coste adicional.

Nota Técnica 1:
El oferente deberá adjuntar, junto con la propuesta económica, una carta de compromiso en la que se asegure que los equipos ofrecidos serán de uso exclusivo de la Universidad de Cundinamarca y contarán con el licenciamiento y soporte correspondiente durante toda la ejecución del proyecto. Esta carta debe garantizar que los equipos ofertados para la solución propuesta no presentarán fin de vida útil temprana al momento de su utilización, asegurando su rendimiento óptimo a lo largo del periodo establecido.

Nota Técnica 2: El oferente debe allegar junto con la propuesta económica los documentos técnicos y/o datasheet del fabricante de las soluciones ofertadas, donde se evidencie el cumplimiento de cada uno de los ítems solicitados en los requerimientos técnicos de las soluciones ofertadas.

7. SERVICIO DE SOC (SECURITY OPERATION CENTER)

Se requiere que el servicio de SOC cumpla las siguientes características:

Duración
Doce (12) meses, en horario 7x24
Infraestructura para monitorear
Servicios de monitoreo y correlación de eventos de seguridad sobre la plataforma SIEM adquirida por la Universidad, para un máximo de 200 dispositivos.
DISPOSITIVOS ADICIONALES: La Universidad solicitará incluir la cantidad de dispositivos adicionales que requiera hasta ocupar todo el licenciamiento de la herramienta SIEM adquirida por la Universidad.
Requerimientos generales
La Universidad requiere servicios de un Centro de Operaciones de Seguridad - SOC, el servicio de SOC será realizado sobre la herramienta de SIEM adquirida por la Universidad.
El contratista deberá realizar la correlación, monitoreo y casos de uso sobre la plataforma de la Universidad, de tal forma que todo el know how y parametrizaciones queden para la Universidad. En ningún caso la información de log deberá salir de la Universidad.
Todas las labores de configuración de la herramienta de monitoreo y correlación de eventos y la generación de los casos de uso para el monitoreo SOC deberán ser ejecutadas por el personal asignado en el contrato.
El plan de trabajo entregado por el contratista deberá contener las etapas, resultados esperados, estrategias para asegurar el logro de los productos en los tiempos establecidos y describir los procesos/procedimientos, las técnicas y herramientas que utilizará en la ejecución del contrato

Dentro del plan de trabajo deberá especificar la metodología que utilizará para administrar, configurar, monitorear y gestionar el servicio de monitoreo objeto del presente contrato, especificando etapas, recursos, entregables, herramientas y técnicas a utilizar. Nota: La Universidad se reserva el derecho de ajustar aspectos de la metodología.
Cuando un evento de seguridad ocurre o está en suceso, el servicio de monitoreo SOC deberá identificarlo y estar en la capacidad de relacionar de forma directa o indirecta con otros eventos de seguridad asociados, determinando el patrón de ataque.
El servicio debe incluir la personalización de reportes que la Universidad requiera durante la prestación del servicio.
El servicio debe permitir la integración del envío de alarmas automáticas vía correo electrónico.
Para la ejecución del contrato y el cumplimiento de los niveles de servicio solicitados, el contratista dispondrá del talento humano que él considere necesario.
Suministrar el servicio de monitoreo de la infraestructura tecnológica, utilizando para ello la solución de tipo SIEM que posee la Universidad.
Proporcionar durante el período de la operación de los servicios un esquema de escalamiento interno a la herramienta.
Los procesos de gestión y operación deben estar basados en las mejores prácticas establecidas por el modelo de procesos ISO 27001:2022.
El servicio ofrecido deberá alinearse a las políticas, procesos, procedimientos y requerimientos de seguridad definidos por la Universidad.
El servicio debe garantizar la disponibilidad, confidencialidad, integridad, no repudio, auditoria y privacidad de los datos y servicios soportados.
El servicio debe incluir apoyo en la definición de estrategias de seguridad, que permitan fortalecer las políticas y controles de seguridad de la información.
Mantener el inventario actualizado de dispositivos monitoreados de la solución.
El contratista deberá administrar la solución SIEM y demás plataformas que componen el servicio SOC incluyendo la gestión de cambios sobre la solución SIEM y otras herramientas parte del servicio de SOC.
La actividad del servicio de monitoreo SOC, se centrará en el tratamiento de eventos, identificación de incidentes, los cuales contarán con un conjunto de metodologías y atención de procesos que permitirá brindar el alertamiento oportuno a los riesgos y amenazas. Por lo anterior, el personal del servicio deberá realizar el escalamiento y las comunicaciones por medio de correo electrónico y/o telefónico con el personal de la Universidad a fin de comunicar las incidencias presentadas. Adicionalmente realizará el seguimiento a los eventos hasta que estos sean cerrados adecuada y oportunamente.

De forma permanente el servicio de monitoreo SOC realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo a la Universidad, resumiendo los resultados en Boletines o Informes extraordinarios de SOC. Los servicios de gestión de SOC realizarán seguimiento 7x24 a los ataques originados desde Internet al igual que los originados al interior de la Universidad. El SOC, debe definir la matriz de escalamiento de común acuerdo con los responsables de seguridad en la Universidad, clarificando el nivel de escalamiento según el tipo y nivel de incidente.
El contratista realizará la integración y monitoreo de los dispositivos y activos tecnológicos que conforman la infraestructura tecnológica de la Universidad, acorde con el licenciamiento del SIEM. Una vez integrada toda la plataforma tecnológica, el contratista configurará y afinará la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos: • Actividades asociadas a la administración de cuentas de usuario final (UserID) • Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator). • Ejecución de comandos especiales sobre sistemas operativos • Ejecución de comandos especiales sobre bases de datos (dump,drop, delete, insert, update) • Cambios de parámetros técnicos, de configuración o de seguridad • Cambios de configuración horaria. • Cambios no autorizados en recursos tecnológicos críticos • Actividades de conexión de cuentas de usuario final o administradores. • Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs. • Actividades asociadas a conexión de acceso remoto. • Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional.
El oferente deberá aportar los enlaces, catálogos e información técnica donde se evidencia el correcto cumplimiento de los requerimientos técnicos solicitado por la Universidad.
El proponente deberá tener un SOC Propietario.
El oferente debe tener al menos cinco (5) años, prestando el servicio, con SOC propietario, dentro del territorio nacional.
El proveedor está en capacidad de prestar el servicio en el idioma español, para la interacción de las áreas de operación y tener al menos uno de sus centros de datos en Latinoamérica
El servicio debe incluir Threat Intelligence o Inteligencia Global, que permita usar un servicio mundial de amenazas identificadas.
El contratista debe disponer de un servicio SaaS 7x24x4 (siete días a la semana, veinticuatro horas al día, con un tiempo de respuesta de cuatro horas) para la identificación de amenazas que puedan poner en riesgo a la infraestructura de la Universidad de Cundinamarca en fuentes abiertas. El servicio debe incluir como mínimo el seguimiento a redes sociales y foros (Twitter, Facebook, Noticias, Blogs, Google+, YouTube) y Blogs, Foros en línea, Sitios wiki, Sitios de opinión, sitios de noticias y en general sitios indexados de los buscadores.
Procesos Internos del SOC
El Proponente debe demostrar algún reconocimiento del centro de gestión de seguridad propuesto (SOC), acompañado de una carta por el representante legal que consta que el SOC que propone cumple con los estándares requeridos por la Universidad de Cundinamarca
El servicio de SOC debe permitir gestionar el ciclo completo de un incidente desde su detección, análisis, escalamiento, cierre y documentación (con archivos de evidencias adjuntas) con la finalidad de generar una base de conocimiento.

El SOC deberá contar con procesos de priorización de atención de incidentes, los cuales se deben basar en una metodología clara de riesgos e impacto.
El SOC deberá contar con procesos definidos para la detección, categorización y alertamiento temprano y oportuno de incidentes de seguridad.
El SOC debe disponer de procesos para la gestión de cambio sobre la plataforma que soporta el servicio.
El SOC debe disponer de herramientas colaborativas internas para el intercambio de información entre los funcionarios. Se deberá aportar una carta firmada por el representante legal del oferente evidenciando las herramientas colaborativas que se utilizan para la prestación del servicio.
Tener los roles y responsabilidades del grupo de operaciones del SOC, está claramente definido, en lo que respecta al monitoreo, atención, manejo y contención de incidentes de seguridad.
Tener los roles y responsabilidades del grupo de operaciones del SOC, está claramente definido, en lo que respecta al monitoreo, atención, manejo y contención de incidentes de seguridad.
Auditoría
El SOC debe permitir a la Universidad de Cundinamarca realizar auditorías sobre los procesos, tecnologías, logs y personas que operan en el SOC, en caso de ser requerido.
Protección física y lógica del SOC
El SOC debe estar protegido al menos con tres anillos de seguridad física. Indicar cuantos anillos de seguridad utilizan para la protección física, describa cada uno de ellos, y quien provee el servicio de protección (Propio, condominio, administración, etc).
El SOC debe tener protección física contra los siguientes posibles daños: Incendio, terremoto, manifestación social.
El acceso al área donde se encuentran los analistas de gestión de eventos e incidentes de seguridad del SOC debe contar con doble factor de autenticación.
El proponente deberá estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por falla en los servicios de suministro.
El proponente deberá estar protegido para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado.
Las instalaciones del SOC deben tener controles para los puntos de acceso por donde pueda ingresar personal no autorizado a las instalaciones del SOC
El proponente deberá garantizar controles de acceso a cualquier repositorio de información que se requiera para los Clientes Gestionados para evitar el acceso no autorizado
El proponente deberá contar con las herramientas necesarias para protección de Cualquier información para su visualización, procesamiento y/o almacenamiento.
El servicio deberá contemplar los siguientes entregables: • Incidentes documentados. • Reportes periódicos de incidentes y a demanda. • Mitigación de incidentes de seguridad.
Monitoreo
El monitoreo se realizará en horario 7x24 durante toda la duración del contrato.
El servicio debe detectar actividades, técnicas inusuales y recolectar evidencias necesarias para determinar si se trata de un evento o incidente de seguridad, de acuerdo con los niveles de servicio.
Las evidencias que sean recopiladas por el servicio de monitoreo SOC son propiedad de la Universidad y podrán ser solicitadas en cualquier momento para atención de requerimientos legales.
El servicio de monitoreo SOC deberá analizar las diferentes alertas detectadas para descartar falsos positivos, antes de crear el caso/ticket en la herramienta institucional dispuesta para ello.

Prestar el servicio desde un centro de monitoreo ubicado en la ciudad de Bogotá D.C. (Colombia). La conexión hacia la herramienta de correlación de la Universidad se realizará a través de una conexión segura utilizando internet.
El servicio de monitoreo SOC se debe poder realizar en forma remota y disponer un personal en sitio solo cuando sea necesario.
La herramienta SIEM que será adquirida por la Universidad, será administrada y operada por el contratista, con personal con experiencia en servicios de monitoreo de logs. La actividad de monitoreo y alertamiento se debe hacer en las instalaciones del contratista.
Las herramientas adicionales que deba utilizar el contratista, tales como hardware, software, firmware, utilitarios o appliances, deben cumplir con la regulación de derechos de autor y propiedad intelectual. Así mismo, deben contar con soporte, mantenimientos y actualizaciones del fabricante o proveedor.
Las herramientas adicionales que deba utilizar el contratista deben ser compatibles con la herramienta SIEM de la Universidad.
Se deben generar alertas de otras amenazas que puedan impactar la infraestructura de la Universidad, como las identificadas en los reportes de análisis de tendencia de centros SIRT/CERT o en las bases de datos de conocimiento del contratista.
El centro de operación del contratista debe garantizar condiciones de seguridad mínimas en aspectos de acceso al espacio físico y acceso a las herramientas de software.
El servicio de monitoreo SOC deberá mantener sincronizados todos los relojes de la herramienta SIEM con la hora legal colombiana, suministrada por el Instituto Nacional de Metrología de Colombia (https://inm.gov.co/web/servicios/hora-legal/).
El servicio de monitoreo SOC debe ejecutar actividades permanentes para garantizar el descubrimiento y monitoreo de nuevos dispositivos en la red.
El tiempo de custodia de los reportes, estadísticas, análisis de tendencia, métricas e indicadores será por la duración del contrato. Una vez terminado el vínculo contractual, el contratista deberá destruir toda la información a la que tuvo acceso de la Universidad.
Informes, métricas y tendencia.
El contratista debe informar al equipo de seguridad de la información de la Universidad de manera inmediata, sobre cualquier evento o incidente real que se presenten en la infraestructura tecnológica.
El contratista deberá presentar mensualmente o cada que sea requerido, los siguientes informes de: • Estado y resultados del servicio en el periodo de valoración, de tipo gerencial. • Eventos de actividad sospechosa atendidos durante el periodo. • Alertas, ataques, incidentes y tendencias. • Comportamientos más relevantes según la correlación realizada por el contratista. • Incidentes de seguridad presentados. • Estadísticas de la información procesada • Hallazgos realizados sobre la plataforma tecnológica • Análisis y recomendaciones sobre los resultados

La Universidad podrá solicitar los informes que considere pertinentes, en la medida en que se vayan integrando nuevas herramientas.
El contratista deberá generar reportes de eventos y de análisis de tendencias, para tomar las acciones preventivas, tales como: instalación de parches, actualización de versiones, modificación de políticas y configuraciones. Además, debe quedar registros de cuándo, dónde y cómo se presentan los incidentes, así como definir nuevos reportes acorde a las necesidades de la Universidad.
El contratista deberá entregar un informe preliminar de un incidente sucedido. Este debe ser remitido a la Universidad posterior a la declaración del evento o incidente y después de la investigación de la actividad sospechosa o incidentes de seguridad se entregará el informe final detallado del mismo.
Los servicios ofrecidos deberán poder ser visualizados a través de tableros de control que permitan ver métricas en línea de acuerdo con las necesidades de la Universidad, por ejemplo: • Alertas/Incidentes por tipo • Alertas/Incidentes nuevos y resuelto • Tiempo medio de creación de alertas/incidentes • Tiempo medio de solución • Tendencias y top de alertas/incidentes • Cumplimiento de acuerdos de servicio • Nivel de disponibilidad del servicio
Categorías de eventos de seguridad, mínimos para monitorear:
Cuentas Privilegiadas
Autenticación fallida
Autenticación exitosa
Usuario agregado a grupo especial local (cambio de privilegios)
Usuario eliminado de grupo especial local (cambio de privilegios)
Usuario agregado a grupo especial global (cambio de privilegios)
Usuario eliminado de grupo especial global (cambio de privilegios)
Cuenta bloqueada
Cuenta desbloqueada
Contraseña cambiada
Cambios de perfiles y permisos de cuentas privilegiadas
Actividades de administración de cuentas (creación, eliminación, cambio de perfiles)
Elevación de privilegios a usuarios
Bases de datos
Autenticación exitosa - cuenta ordinaria
Autenticación fallida - cuenta ordinaria
Autenticación exitosa - SA
Autenticación fallida - SA
Cuenta bloqueada
Cuenta desbloqueada

Usuario agregado al grupo de SA
Ejecución de instrucciones DML (Insert, Update y Delete) sobre tablas en producción por usuarios no autorizados
Ejecución de instrucciones DDL (Copia, (dump), Create, Drop, Alter) sobre tablas en producción por usuarios no autorizados
Acceso de desarrolladores
Actualización de cuentas
Cambios sobre plataformas - Windows
Software instalado en Servidor Windows
Software desinstalado en Servidor Windows
Archivo crítico modificado (control de integridad)
Cambio en políticas del Directorio Activo
Eliminación de logs de auditoría
Cambios sobre plataformas - Linux
Software instalado en Servidor Linux
Software desinstalado en Servidor Linux
Archivo crítico modificado (control de integridad)
Eliminación de logs de auditoría
Conexiones
Acceso remoto
Cantidad inusual de conexión a los dispositivos, equipos, servidores y base de datos.
Comportamiento sospechoso
Ataques de fuerza bruta.
Instalación o descarga de software no autorizado.
Acceso no autorizado a carpetas restringidas.
Patrones de vírus informáticos o códigos maliciosos.
Ejecución de secuencia de operaciones y/o transacciones sobre los sistemas de información que pueden implicar fraudes
Auditoría
Cambios de parámetros de seguridad
Archivos críticos del sistema operativo modificados
Cambios de políticas en Directorios Activos
Eliminación de logs de auditoría
Modificación de winlogon.exe
7. Acuerdos de Nivel de Servicio
El monitoreo se realizará en horario 7x24 durante toda la duración del contrato.
La configuración de cambios o requerimientos solicitados sobre la plataforma SIEM y/o otras deberán ser gestionados en máximo 24 horas, previa aceptación de la ventana. Para casos de alta complejidad se definirán los tiempos específicos para estas configuraciones.

Diseño, integración y configuración del servicio
8 semanas
Reportes y monitorización
Tiempos de alertamiento y escalamiento al equipo de respuesta a incidentes de seguridad de la Universidad: • De impacto crítico: alertamiento dentro de los primeros 30 minutos y escalamiento en máximo 1 hora. • De impacto alto: alertamiento dentro de los primeros 60 minutos y escalamiento en máximo 2 horas • De impacto moderado: alertamiento dentro de las primeras 2 horas y escalamiento en máximo 12 horas • De impacto bajo: alertamiento dentro de las primeras 12 horas y escalamiento en máximo 24 horas.
Generación y envío de informes de servicio
5 primeros días hábiles del mes. Los documentos entregables e informes que el contratista presente, deben contar con un formato de presentación estándar, redacción clara, buena ortografía y en idioma español.
Mejores prácticas
El servicio deberá estar enmarcado en el cumplimiento de la norma ISO 27001 del 2022 (SGSI) en: • Responsabilidades y procedimientos • Reporte de eventos de seguridad de la información • Reporte de debilidades de seguridad de la información • Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
Los incidentes deben ser gestionados de acuerdo con: 1. Planificar y preparar: establecer una política de gestión de incidentes de seguridad de la información y formar un Incident Respuesta Team (Grupo de respuesta de incidentes). 2. Detección e informes: El contratista deberá detectar e informar "eventos" que pueden ser o convertirse en incidentes. 3. Evaluación y decisión: El contratista deberá evaluar la situación para determinar si de hecho se trata de un incidente. 4. Respuestas: El contratista deberá reportar de manera oportuna al equipo de seguridad de la Universidad para que pueda contener, erradicar y remediar. 5. Lecciones aprendidas: El contratista deberá documentar la gestión de los riesgos de la información como consecuencia de las incidencias experimentadas.
Certificaciones Exigidas al Proceso de SOC del Oferente
ISO27001: El oferente debe presentar junto con su propuesta el certificado ISO 27001 del 2022 o superior (SGSI) para su proceso de SOC y este debe de tener al menos un (1) año de vigencia.
FIRST: El oferente debe presentar junto con su propuesta el certificado de membresía de FIRST para su proceso de SOC, con una vigencia mínima de un (1) año de expedición del certificado, la cual será tenida en cuenta como requisito adicional para asignación de puntaje dentro del presente proceso contractual.

Certificado de Fabrica: El oferente deberá presentar junto con su propuesta una certificación del fabricante de la solución SIEM adquirida por la Entidad, donde se evidencia que el oferente cuenta con la categoría de partner a nivel de canales.
Visita técnica por parte del cliente
La Universidad podrá realizar una visita presencial a las instalaciones del SOC, donde el oferente deberá cumplir con las garantías de las normativas en ISO 27001. Esta visita deberá ser coordinada con el gerente del proyecto.

Nota Técnica 5: El oferente debe allegar junto con la propuesta económica todos los soportes correspondientes a los perfiles solicitados como requisito habilitante del presente proceso remitirse al **numeral 10. PERFILES REQUERIDOS** del presente anexo. La NO presentación de estos soportes ocasionará que la propuesta técnica presentada sea inhabilitada para su evaluación. La Universidad no aceptará que una persona ocupe más de uno de los roles solicitados.

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.

Es importante tener en cuenta esta clasificación interna de la criticidad de los incidentes en seguridad perimetral *(**Tabla 11. Niveles de Criticidad de Incidentes**)* para la asignación de recursos, personal y la toma de medidas adecuadas de acuerdo con la gravedad del incidente por parte del proveedor al que sea adjudicado el presente proyecto lo cual garantiza a la Universidad que se aborden los incidentes de manera oportuna y eficaz, minimizando el impacto en la seguridad y en el funcionamiento de las actividades administrativas y propias de la academia.

Tabla 11. Niveles de Criticidad de Incidentes - Fuente: Elaboración Propia.

NIVEL	GRAVEDAD	TIEMPO DE RESPUESTA
Nivel 1 Bajo	Incidentes menores que no tienen un impacto significativo en la seguridad o la disponibilidad de los sistemas perimetrales. Pueden ser eventos de seguridad de baja importancia, como escaneos de puertos no autorizados, intentos de acceso no autorizado que son bloqueados por medidas de seguridad adecuadas o tráfico anómalo sin consecuencias graves.	Dentro de las 24 horas Siguientes
Nivel 2 Moderado	Incidentes que indican una posible amenaza o compromiso en curso, pero que aún no han causado un impacto significativo en la red perimetral. Esto podría incluir intrusiones menores en sistemas perimetrales no críticos, detección de malware en el tráfico de red o intentos de acceso no autorizado que resultan en acceso limitado.	Dentro de las 12 horas Siguientes
Nivel 3 Significativo	Incidentes que tienen un impacto moderado en la seguridad o la disponibilidad de los sistemas perimetrales y que requieren una atención inmediata. Esto podría incluir intrusiones exitosas en sistemas perimetrales críticos, compromiso de credenciales de usuario privilegiadas, exfiltración de datos sensibles o ataques de denegación de servicio que afectan parcialmente a los servicios perimetrales.	Dentro de las 6 horas Siguientes
Nivel 4 Alto	Incidentes que tienen un impacto grave en la seguridad o la disponibilidad de los sistemas perimetrales y que requieren una respuesta urgente y coordinada. Esto podría incluir fallos críticos de seguridad que exponen datos altamente sensibles, ataques de ransomware que cifran datos críticos para el negocio o interrupciones importantes en los servicios perimetrales que afectan a la operación de la Universidad.	Dentro de las 3 horas Siguientes
Nivel 5 Crítico	Incidentes que representan una amenaza inmediata para la integridad, la confidencialidad o la disponibilidad de los sistemas perimetrales y que requieren una acción inmediata a nivel ejecutivo. Esto podría incluir intrusiones altamente sofisticadas que comprometen toda la infraestructura perimetral, violaciones de datos masivas que afectan a clientes o usuarios finales, o ataques que tienen un impacto significativo en la infraestructura crítica de la Universidad.	Inmediato (dentro de minutos)

- La solución deberá notificar los incidentes como mínimo en dos medios diferentes de comunicación (SMS, Correo electrónico, aplicaciones de mensajería instantánea tales como Microsoft Teams 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, y el respectivo tratamiento que se les allá dado a dichas incidencias.
- 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 TRANSFERENCIA DE CONOCIMIENTO

- 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, 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. PERFILES REQUERIDOS

RECURSO	FORMACION	POSTGRADO	CERTIFICACIONES	EXPERIENCIA	DEDICACION	FUNCIONES
Un (01) Ingeniero Gerente de Proyecto	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicación o carreras afines. Tarjeta Profesional con expedición mínimo de cinco (5) años	Posgrado en Gerencia de Proyectos y/o Certificación PMP.	Certificación Itil Foundation v3 o superior	Experiencia general de cinco (5) años en gerencia de proyectos deTI, de los cuales mínimo tres (3) años de experiencia especifica gerenciando y/o coordinando proyectos de seguridad informática. La experiencia se cuenta a partir de la expedición de la tarjeta profesional	100 % al proyecto, de requerirse de manera presencial o virtual en las instalaciones de la entidad	Definir los objetivos y los alcances del proyecto. Desarrollar un plan de trabajo detallado, estableciendo metas, cronograma, recursos. Identificar riesgos y establecer un plan de mitigación
Un (01) Ingeniero Líder Técnico	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carrerasafines.	Especialización o maestría en Seguridad de la Información o informática.	Certificación vigente en SCRUM Foundations Professional (SFPC) Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018 Certificación vigente en Especialista en Soluciones de Seguridad de Operaciones. Emitida por el fabricante con el que se este presentado el proponente. .	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de tres (3) años como líder o coordinador o gerentede servicio de TI. Certificaciones de Experiencia especifica de mínimo años (4) años en implementación o administración en plataformas de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.	100 % al proyecto, de requerirse de manera presencial o virtual en las instalaciones de la entidad	Guiar al equipo en las mejores prácticas, estándares de codificación y metodologías de trabajo. Asegurarse de que todos los miembros del equipo comprendan la dirección técnica del proyecto y su papel en él. Ser el punto de referencia para resolver problemas técnicos complejos que el equipo pueda enfrentar. Asegurarse de que el equipo esté al tanto de las últimas tendencias tecnológicas y las mejores

						prácticas del sector.
Implementador y soporte Un (01) Ingeniero	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carrerasafines.	N/A	Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018 Certificación vigente en Profesional de Seguridad de Redes Certificación vigente en Especialista de Soluciones en Seguridad de Nube Pública. Emitida por el fabricante con el que se esté presentado el proponente. .	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de cuatro (4) año en implementación, soporte y monitoreo de soluciones de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.	100 % al proyecto, de requerirse de manera presencial o virtual en las instalaciones de la entidad	Instalación y configuración de dispositivos. Integración con la red existente. Generar la respectiva documentación técnica.

ANA LUCIA HURTADO MESA
Directora Sistemas y Tecnología
Universidad de Cundinamarca

JENIFFER CASTILLO FERNÁNDEZ
Profesional Director de Área I
Dirección de Sistemas y Tecnología
Universidad de Cundinamarca

Proyecto: Ing. Jeniffer Castillo
Ing. Ingrid Sánchez
Área Servicios Tecnológicos