	FABRICANTE Y REFERENCIA:			
	ÍTEM	**CARACTERÍSTICA**	**CUMPLE**	**OBSERVACIONES**
GENERALIDADES	1	El sistema de seguridad perimetral, en adelante llamado "el sistema" esta compuesto por todo el hardware, software y licenciamiento necesarios para su funcionamiento incluyendo alta disponibilidad HA		
	2	Cada una de las características debe ser confirmada mediante documentación oficial y pública del fabricante (guías de administración, manuales y/o guías técnicas) en medio físico y digital, en el cual se debe referenciar para cada característica un link a página WEB oficial donde se encuentre la documentación.		
	3	El sistema debe contar con máximo dos equipos con el fin de minimizar los puntos de falla, optimizar el espacio en el data center, optimizar el uso de las conexiones de red y facilitar la administración incluyendo el sistema de monitoreo y reportes. Estos deben trabajar de forma redundante entre sí en Alta disponibilidad (HA) soportando todos los servicios que presta el sistema de seguridad perimetral Firewall NG.		
	4	El hardware y software que ejecuten las funcionalidades del sistema deben ser de tipo appliance. No serán aceptados equipamientos servidores y sistema operativo de uso genérico		
	5	Los equipos ofrecidos deben ser adecuados para montaje en rack 19”. Cada equipo puede ocupar máximo 3 unidades de Rack.		
	6	El software del sistema deberá ser ofrecido en la última versión estable y recomendada por el fabricante.		
	7	El sistema debe poseer la capacidad de identificar al usuario de red con integración a Microsoft Active Directory, sin la necesidad de instalación de agente en el Controlador de dominio, ni en las estaciones de los usuarios.		
	8	Los equipos deben estar certificados para IPv6 en Firewall por USGv6 o IPv6 Ready		
	9	El sistema debe incluir actualización automática de firmas de prevención de intrusos (IPS), bloqueo de archivos maliciosos (Antivirus y Anti-Spyware), Filtrado WEB por categorías e identificación de aplicaciones		
	10	Motor de procesamiento en paralelo: el módulo de hardware del plano de control y el módulo de hardware del plano de datos deben estar separados y deben estar embebidos en cada equipo.		

	11	Los equipos ofertados NO deben estar en anuncio de fin de vida (end-of-life) y fin de venta (end-of-sale) por parte del fabricante		
	12	Control de políticas por identificación de País.		
	13	El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner GOLD (o equivalente a la marca) o superior de los productos adquiridos con el licenciamiento, teniendo en cuenta que en orden ascendente los niveles de certificación son: Silver, Gold, Platinum (o equivalente a la marca)		
ALTA DISPONIBILIDAD	14	Soporta configuración de alta disponibilidad en los modos Activo/Pasivo y Activo/Activo en modo transparente y en layer 3		
	15	El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.		
CAPACIDAD Y CANTIDADES	16	Throughput para cada equipo de mínimo 8 Gbps con la funcionalidad de control de aplicaciones habilitada y logs habilitados para todas las firmas (actualizaciones) que el fabricante posea		
	17	Throughput para cada equipo de mínimo 4 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas firmas (actualizaciones) que el sistema posea debidamente activadas y actuando con logs habilitados para: control de aplicaciones, IPS, Antivirus e Antispyware		
	18	Cada equipo tiene la Capacidad de procesar mínimo 3 millones de conexiones de red simultaneas (concurrentes)		
	19	Cada equipo tiene la Capacidad de procesar mínimo 135.000 nuevas conexiones en red por segundo.		
	20	Fuente 120V AC, redundante y hot-swappable		
	21	Cada equipo incluye Disco de Estado Solido (SSD) de mínimo 240 GB para almacenamiento del sistema y logs		
	22	Interfaz adicional y dedicada para administración 10/100/1000 para cada equipo		
	23	Mínimo 8 Interfaces Ethernet base-TX 10/100/1000 de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración)		
	24	Mínimo 4 Interfaces 10Gbps SFP/SFP+ de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración) incluyendo Mínimo 2 optical transceiver SFP+ 10-Gigabit multi-mode		
	25	Mínimo 1 Interfaz para alta disponibilidad a 1 Gbps (No deben estar incluidas en las interfaces para tráfico de Red, ni administración)		
	26	Mínimo 1 Interfaz adicional para alta disponibilidad a 10 Gbps SFP+ (No deben estar incluidas en las interfaces para tráfico de Red, ni administración)		
	27	1 interfaz de tipo consola		

	28	Capacidad de mínimo 60 zonas de seguridad		
SERVICIOS Y PROTOCOLOS DE RED	29	Soporte de mínimo 1024 VLAN Tags 802.1q		
	30	Soporte de Agregación de links 802.3ad		
	31	Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2) Para IPv4		
	32	Debe soportar enrutamiento estático y dinámico (OSPFv3) Para IPv6		
	33	Capacidad de balancear varios enlaces de internet sin el uso de políticas especificas		
	34	Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QoS y SSL Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no hay contrato de licenciamiento con el fabricante.		
CONTROL POR POLÍTICA DE FIREWALL	35	Soportar controles por zona de seguridad		
	36	Controles de políticas por puerto y protocolo.		
	37	Control de políticas por aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.		
	38	Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.		
	39	Soportar objetos y Reglas multicast.		
	40	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.		
CONTROL DE APLICACIONES	41	El sistema deberá tener la capacidad de reconocer aplicaciones, independiente del puerto y protocolo		
	42	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.		
	43	Detectar y limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD		
	44	Para mantener la seguridad de la red, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas		
IENAZAS	45	Para seguridad del ambiente contra ataques informáticos, el sistema de seguridad debe poseer módulo de IPS, Antivirus y Anti-Spyware integrados en los equipos que componen el sistema		
	46	El sistema debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.		
	47	Debe incluir seguridad contra ataques de negación de servicios.		

PREVENCIÓN DE AM	48	Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3		
	49	Soportar bloqueo de archivos por tipo		
	50	Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall donde cada política pueda incluir como mínimo Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad		
	51	El sistema debe poseer funcionalidades para análisis de Malwares no conocidos incluidas en la propia herramienta.		
	52	El sistema debe ser capaz de enviar archivos sospechosos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado.		
FILTRO URL	53	Debe ser posible crear políticas por usuario, grupo de usuario, IPs, redes y zonas de seguridad		
	54	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quien esta utilizando URLs a través de la integración con servicios de directorio, autenticación via LDAP, Active Directory, E-Directory y base de datos local		
	55	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL		
	56	Debe poseer al menos 60 categorías de URLs		
	57	Debe soportar la creación de categorías URL custom		
	58	Debe soportar la exclusión de URLs del bloqueo por categoría		
IDENTIFICACIÓN DE USUARIOS	59	Debe poseer integración con Radius, ldap, Active Directory, E-directory y base de datos local, para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.		
	60	Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC via syslog, para la identificación de direcciones IP y usuarios		
	61	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tienen estos servicios		
	62	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.		
CIO	63	Como la finalidad de controlar aplicaciones y trafico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc.) y tener un alto consumo de ancho de banda, el sistema debe controlarlas por políticas de máximo ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.		

CALIDAD DE SERVIC	64	Soportar la creación de políticas de QoS por: - Direccion de origen - Direccion de destino - Por usuario y grupo de LDAP/AD - Por aplicaciones - Por puerto		
	65	El QoS debe permitir la definición de clases por: - Ancho de Banda garantizado - Ancho de Banda Máximo - Cola de prioridad.		
	66	Soportar priorización RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.		
	67	Soportar marcación de paquetes Diffserv		
FILTRO DE DATOS	68	Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, mas no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos via expresión regular		
	69	Permitir la detección de portales de phishing estableciendo políticas que eviten el envío de credenciales válidas de usuarios a sitios no autorizados		
VPN	70	Soportar VPN IPSec Nativa Client-To-Site y Site-to-Site (Incluyendo conexión Site-to-Site con infraestructuras en la nube mínimo con: Amazon, Microsoft Azure)		
	71	La VPN IPSEc debe soportar mínimo: - 3DES; - Autenticación MD5 e SHA-1; - Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; - Algoritmo Internet Key Exchange (IKEv1 & IKEv2); - AES 128 y AES 256 (Advanced Encryption Standard) - Autenticación via certificado IKE PKI.		
	72	Debe poseer interoperabilidad VPN IPSec mínimo con los siguientes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, Sonic Wall		
	73	Permitir que el usuário realice la conexión por medio de cliente instalado en el sistema operativo del equipo cliente o por medio de interfaz WEB		
	74	Soportar autenticación via AD/LDAP, Secure id, certificado y base de usuarios local		
	75	Permite establecer un túnel VPN client-to-site del cliente al sistema de seguridad, proveyendo una solucion de single-sign-on a los usuarios, integrandose como las herramientas de Windows-logon		
	76	Debe permitir que las conexiones VPN SSL o VPN IPSec sean establecidas de las siguientes formas: - Antes o durante la autenticación del usuario en la estación - Después de la autenticación del usuario en la estación - Manualmente por el usuario		
	77	El cliente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10		

	78	Capacidad de soportar mínimo 2000 clientes de VPN SSL simultáneos sin uso de licenciamiento o licenciado a perpetuidad		
	79	Capacidad de soportar mínimo 1000 túneles de VPN IPSEC simultáneos sin uso de licenciamiento o licenciado a perpetuidad		
CONSOLA DE ADMINISTRACIÓN y MONITOREO	80	El sistema debe incluir consola de administración y monitoreo, incluyendo el licenciamiento de software necesario para las dos funcionalidades, como también el hardware dedicado para el funcionamiento de las mismas		
	81	La consola de administración y monitoreo puede residir en el mismo appliance de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función.		
	82	La administración del sistema debe soportar acceso via SSH, cliente WEB (HTTPS) y API abierta		
	83	La administración en la consola debe permitir/hacer: - Creación y administración de políticas de firewall y control de aplicaciones - Creación y administración de políticas de IPS y Anti-Spyware - Creación y administración de políticas de filtro de URL - Monitoreo de logs - Herramientas de investigación de logs - Debugging - Captura de paquetes		
	84	Debe permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing)		
	85	Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones mas antiguas		
	86	Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo y el horario del cambio		
	87	Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del trafico generado en la Universidad		
	88	Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Antispyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes		
	89	Debe ser posible acceder remotamente al sistema a aplicar configuraciones durante momentos donde el trafico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.		

	90	Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto): - Debe mostrar la situación del dispositivo y del clúster - Debe poder mostrar las principales aplicaciones - Debe poder mostrar las principales aplicaciones por riesgo - Debe poder mostrar los administradores autenticados en la plataforma de seguridad - Debe poder mostrar el número de sesiones simultaneas - Debe poder mostrar el estado de las interfaces - Debe poder mostrar el uso de CPU		
SERVICIOS	91	Soporte y cambio de partes 7x24 durante 3 años: El proveedor debe otorgar el Soporte técnico de todos los componentes del sistema durante los 3 años contratados, asegurando que este servicio se preste en sitio, remoto, telefónico o correo electrónico, con personal certificados en la marca. Cuando el diagnóstico sobre los equipos o partes determine falla total o parcial, el contratista deberá realizar el proceso de RMA. El equipo entregado o partes por RMA debe contar con iguales o superiores características y capacidades tanto en hardware como en software que el equipo o parte remplazada. La atención de soporte será en esquema 7x24xNBD: 7 días de la semana de 8:00 am a 5:00 pm, con remplazo de hardware al siguiente día hábil, sin generar costo adicional para la Universidad.		
	92	Instalación, configuración, migración, puesta en funcionamiento y optimización del sistema: hardware, software, licenciamiento y todas las funcionalidades adquiridas, incluyendo todos los cables, accesorios, soportes y demás elementos necesarios.		
	93	Licenciamiento en HA durante 3 años incluyendo todas las funcionalidades descritas en este documento		
	94	2 cursos con certificación		