UNIVERSIDAD PEDAGOGICA NACIONAL

ANEXO NO. 2:

ESPECIFICACIONES TÉCNICAS

1. DEPENDENCIA SOLICITANTE

Subdirección de Gestión de Sistemas de Información

2. OBJETO A CONTRATAR

"RENOVACION LICENCIAMIENTO Y ACTUALIZACION DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL"

3. CLASIFICADOR DE BIENES Y SERVICIOS DE NACIONES UNIDAS (UNSPSC)

La obra, bien o servicio objeto del presente Proceso de Selección está codificada en el Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC), como se indica en la siguiente tabla:

CODIGOS UNSPSC	DESCRIPCIÓN
43233200	SOFTWARE DE SEGURIDAD Y PROTECCIÓN
43232900	SOFTWARE PARA TRABAJO EN REDES
43222600	EQUIPO DE SERVICIO DE RED
43222500	EQUIPO DE SEGURIDAD DE RED
81111800	SERVICIOS DE SISTEMAS Y ADMINISTRACIÓN DE COMPONENTES DE SISTEMAS
81111500	INGENIERIA DE SOFTWARE O HARDWARE

UNIVERSIDAD PEDAGOGICA NACIONAL

3.1 ESPECIFICACIONES TÉCNICAS

3.1.1 REQUERIMIENTOS RENOVACION LICENCIAMIENTO Y ACTUALIZACION DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL DE LA UNIVERSIDAD PEDAGÓGICA NACIONAL

CANTIDAD	REFERENCIA	DESCRIPCIÓN	SERVICIOS	CUMPLE (SI/NO)	¿CÓMO SE VERIFICA?
1	CPCES-COSTANDARD	CPAP-SG7000- NGTP SOPORTE, GARANTIA DE LOS UTM 7000 Next Generation Threat Prevention Appliances. Enterprise Based Protection - Next Generation Threat Prevention Package Including IPS, APCL, URLF, AV, ABOT and ASPM bladesABOT and ASPM bladesFor CK: 00:1C:7F:3D:7B:C9 STANDARD Collaborative Enterprise Support			
1	CPCES-CO-STANDARD-ADD	Standard Collaborative Enterprise Support			
1	CPEBP-NGTX	Security Services - Enterprise Based Protection - Next Generation Threat Prevention Package Including IPS, APCL, URLF, AV, ABOT and ASPM bladesABOT and ASPM bladesFor CK: 00:1C:7F:3D:7B:C9 Security Services - Enterprise Based Protection (Licenciamiento y grantia para los 2 Firewall)			
1	CPSB-EVS-COMP10-1Y	SmartEvent, SmartReporter and Compliance bldes for 10 gateways (Smart-1 & open server) year subscription)			
1	CP-CGAS-AGAS,CP-CGAS-10RD,CPCESCO-STANDARD	WAF CloudGuard Agent WAF Premium Baseline Package, CloudGuard Agent WASF Premium Bucket, Root Domains Package Monthly Price, Colaborative Enterprise Support Standard.			

1	**Servicios-Soporte**	**Servicio de Reinstalación, Transferencia de conocimientos, capacitación, visitas proactivas Mensuales, Soporte telefónico Web y en sitio cuando se solicite, Durante la vigencia del contrato, 7x24. Incluye, Seguimiento, monitoreo a los equipos objeto del contrato. Debe realizar un análisis de vulnerabilidades**	**Incluir servicios en las soluciones**		
	Servicios-Soporte	**El proponente deberá entregar un informe técnico mensual durante el tiempo de garantía y/o soporte sobre el desempeño de la plataforma mantenida, Se requiere servicio de análisis de log y generación de reportes de manera periódica**	**Incluir servicios en las soluciones**		
	Servicios-Soporte	**Dentro del Servicio de Seguridad debe realizar un análisis de vulnerabilidades que incluya lista de Vulnerabilidades encontradas con su respectivo plan de remedición, efectuando la presentación y socialización al personal técnico de la Subdirección de Gestión de Sistemas de Información.**	**Incluir servicios en las soluciones**		
		El oferente deberá realizar el correspondiente soporte técnico en sitio (7x24) cada vez que se realice el requerimiento por fallas de funcionamiento del producto durante el tiempo de vigencia de las licencias.	**Incluir servicios en las soluciones**		
1	**Servicios-Soporte**	**Durante la vigencia de las licencias, el proponente debe realizar dos (2) mantenimientos preventivos de la solución, para ello debe entregar un plan de trabajo que contenga al menos: Nombre de la actividad, tiempo estimado, fecha estimada, posibles afectaciones y responsables. Así mismo, al finalizar el mantenimiento preventivo debe entregar un informe con los resultados de este.**	**Incluir servicios en las soluciones**		

	Servicios-Soporte	**El proponente deberá entregar Documentación con un análisis de buenas prácticas en: Seguridad informática para Windows Data Center 2019 y Seguridad informática para SQL/Server, Última Versión**	**Incluir servicios en las soluciones**		
1	**Servicios-Soporte**	**El proponente deberá realizar capacitación básica de 20 horas para dos (2) personas en ISO 27001 y Ciberseguridad**	**Incluir servicios en las soluciones**		

3.1.2 REQUERIMIENTOS DEL WEB APPLICATION FIREWALL - WAF

ESPECIFICACIONES WAF	**CUMPLE (SI/NO)**	**¿CÓMO SE VERIFICA?**
La Universidad Pedagógica requiere una solución para la protección automatizada de aplicaciones WEB y API, la misma debe cumplir con las siguientes características o especificaciones, las cuales deben ser confirmadas punto a punto con la correspondiente evidencia mediante documentación oficial acceso público (guías de administración, manuales y/o guías técnicas). No se aceptarán documentos generados o certificados expresamente para este proceso.		
La solución deberá ser una solución de seguridad de Aplicaciones Web y API completamente automatizada, impulsada por un motor de aprendizaje automático patentado. Este motor analizará continuamente las solicitudes HTTP/S de los usuarios al visitar el sitio web o la API, incluyendo la estructura de la aplicación y la interacción de los usuarios con el contenido para identificar patrones, detener y bloquear automáticamente solicitudes maliciosas y actores no deseados.		
Deberá incorporar las siguientes tecnologías de protección principales: o Web Application Protection o API Security o Bot Prevention o File Security o Intrusion Prevention (IPS) o HTTPS Traffic Inspection o Rate Limit		
De acuerdo con Cybersecurity Mesh de Gartner sobre tecnologías unificadas, la solución WAF debe ser del mismo fabricante que la solución perimetral actualmente implementada en la Universidad Pedagógica, asegurando compatibilidad nativa y simplificación en la administración		

Protección de Día Cero Avanzada:		
La solución deberá ser capaz de proteger contra ataques de día cero en la aplicación protegida sin necesidad de firmas de IPS relacionadas.		
Esta protección deberá realizarse a través del aprendizaje continuo de la aplicación y su comportamiento, analizando la estructura de la aplicación y como los usuarios interactúan con el contenido para identificar patrones, detener y bloquear automáticamente solicitudes maliciosas y actores no deseados, evitando ataques a través de encabezados o formularios web.		
Escalabilidad y posibilidades de despliegue		
La solución deberá de permitir una cantidad ilimitada de aplicaciones y de ancho de banda, ya que la solución brindara protección a diferentes ambientes WEB y API, la cantidad de estas aplicaciones es muy dinámica al igual que la cantidad de ancho de banda y su ubicación (nube/on-premise)		
La solución deberá brindar en conjunto una protección de al menos 5.880 millones de solicitudes web por año.		
La solución deberá de ser administrada desde un portal en la nube.		
La solución debe poder proteger las aplicaciones en diferentes entornos construidos en cualquier arquitectura (on-premise, nube, containers) administrado desde un único portal centralizado.		
La solución debe poder ser instalada en diferentes ambientes, algunos actualmente implementados en la institución y otros que se implementaran en el futuro, al menos debe poder ser instalada en: o Nube: Amazon Web Services (AWS), Microsoft Azure, VMware o Contenedores: Docker, Kubernetes, Kubernetes Ingress o Un agente que funcione sobre NGINX Web Server o un proxy reverso de NGINX		
Los recursos instalados, como máquinas virtuales, contenedores o agentes, deben comunicarse con la Nube de forma segura vía HTTPS/TLS, encriptando el tráfico.		
Los recursos implementados deben funcionar como proxy reverso		
La solución no debe limitar a un mínimo la cantidad de despliegues		
Prevención de Ciberataques:		
La solución debe poder prevenir ciberataques conocidos y desconocidos, esto incluye la detención de ataques de día cero de forma preventiva (sin actualizaciones de software) y protecciones para más de 2,800 CVEs específicas de la web.		
La solución debe poder analizar cada solicitud entrante y se debe analizar en contexto esta solicitud.		

El motor de inteligencia artificial de la solución debe poder llevar a cabo un análisis de riesgos mediante el examen de parámetros como: o El perfil del usuario o Los patrones observados en la sesión del usuario o La forma en que otros usuarios interactúan típicamente con la aplicación		
A cada solicitud se le debe asignar una puntuación que determine la probabilidad de que sea maliciosa.		
El motor se debe poder adaptar automáticamente a los cambios de la aplicación al perfilar continuamente el usuario, la aplicación y el contenido.		
El motor deberá contar con un aprendizaje asistido donde el operador con una simple decisión pueda asegurar el tráfico.		
La solución debe poder detener los ataques contra aplicaciones que incluyen: o Cross Site Request Forgery o XML External Entity o Remote Code Execution o Evasion Techniques o LDAP Injection o Path Traversal o Vulnerability Scanning o SQL Injection o Métodos HTTP ilegales Entrada no válida para formularios y APIs Bot Scraping Brute Force Attacks o Al menos 2800 Web Specific CVEs		
La solución deberá poder limitar los siguientes parámetros o Los Bytes en el tamaño de URL o La profundidad de los objetos de HTTP o El tamaño del body de una petición o El tamaño del encabezado en una petición o Deberá contar con una protección de CSRF		
La solución deberá ser capaz de configurar excepciones tales como: o Expresión regular que determina el uri que debe coincidir. Por ejemplo: /login/.* o Expresión regular y CIDR que determina el identificador de fuente que debe coincidir. Por ejemplo: 192.168.24.0/24 o. *@Acme.com) o CIDR que determina la IP de origen físico que debe coincidir. Por ejemplo: 192.168.24.0/16 o Expresión regular que determina el nombre del parámetro que debe coincidir. Por ejemplo: * Contraseña. * o Expresión regular que determina el nombre del parámetro que debe coincidir. Por ejemplo: ^ 4 [0-9] {12} (?: [0-9] {3})? $) o El indicador que debe coincidir. Si es necesario, usa una lista		

separada por comas.		
La solución deberá ser capaz de configurar excepciones y modificar la acción que toma la herramienta de forma predeterminada, la solución deberá permitir aceptar o bloquear el tráfico cuando el mismo haga match a algunas de las condiciones mencionadas en el punto anterior.		
La solución deberá permitir subir certificados digitales para poder proteger sitios https de la institución.		
La solución deberá incluir un motor de aprendizaje que ayude a disminuir la cantidad de eventos críticos y altos a lo largo del tiempo a medida que aprende el tráfico del sitio y comprende el comportamiento del usuario.		
El aprendizaje de la solución debe de funcionar de manera continua y no solo tener un “modo aprendizaje”		
La solución deberá clasificar cada solicitud y decidir sus posibilidades de ataque a través de un motor de inteligencia artificial inteligente		
Funcionalidades para la seguridad WEB:		
La solución deberá permitir aplicar políticas para definir los límites en los mensajes del protocolo HTTP. Incluir al menos los siguientes parámetros: o Tamaño del cuerpo (Body Size): tamaño máximo del cuerpo del mensaje HTTP o Tamaño de URL (URL Size): tamaño máximo de la URL, esto incluye todos los campos de consulta. o Tamaño del encabezado (Header Size): tamaño máximo del encabezado HTTP o Profundidad máxima del objeto (Object Depth): tamaño de profundidad máxima del objeto JSON / XML, esto incluye XML incrustado en JSON y lo contrario. o Métodos validos HTTP (RFP): Aceptar o bloquear métodos https no standard		
La solución deberá soportar métodos para poder distinguir a los usuarios entre sí. Deberá soportar al menos los siguientes mecanismos: o X-Forwarded-For o IP Origen o JWT Key o Cookie o Header Key		
La solución debe permitir agregar usuarios confiables como fuente del proceso de aprendizaje, con el fin de mejorar la capacidad de aprendizaje		
File Security		
La solución deberá proporcionar seguridad de archivos, con el objetivo de prevenir que archivos maliciosos sean cargados a los servidores de la organización vía HTTP Post.		

o El motor de seguridad de archivos debe escanear el tráfico HTTP entrante, analizará cualquier archivo cargado o Configurar el umbral de severidad a partir del cual el motor tomará una acción. o Cambiar el comportamiento exacto (Prevenir/Detectar/Inactivo) ante la detección de una firma según su nivel de confianza. o Seleccionar si se deben extraer archivos comprimidos para su análisis y configurar límites de escaneo y comportamiento ante archivos anidados o fallos en la extracción de contenido. o Escaneo de tipos de archivo conocidos (Word, Excel, PowerPoint, PDF y ejecutables) mediante el motor de Emulación de Amenazas.		
Los archivos inspeccionados deberán emularse en la nube del fabricante proveedor del servicio		
Funcionalidades para la seguridad de API:		
La solución debe proporcionando seguridad a través de la visibilidad, ofreciendo un esquema aprendido por el motor de descubrimiento de API y un análisis del uso de la API.		
Debe descubrir como mínimo soportado REST API y GraphQL. o La detección de API debe ser hecha mediante un motor de IA de aprendizaje automático iterativo que detecta el uso de API (combinando el método y el endpoint utilizado en la solicitud).		
La solución debe ofrecer protección preventiva para posibles vulnerabilidades de API a través de un procedimiento de validación de esquema (schema) o La solución debe proporcionar el schama en el formaton OpenAPI, de acuerdo con el proceso de descubrimiento para la mejora en la capacidad de detección y prevenir solicitudes ilegales. o La solución debe generar el schema basado en los parámetros de consulta y el cuerpo de la solicitud para crearlo de forma exacta para cada API basándose en múltiples solicitudes. o La solución también debe permitir subir schemas personalizados para proteger las API utilizando técnicas como la validación automatizada mediante archivos de esquema Open API.		
La solución debe ofrecer un mecanismo de aprendizaje para que sea posible acompañar el proceso de aprendizaje y caso necesario puede requerir que el usuario decida entre varias opciones cuando el resultado del aprendizaje no es lo suficientemente concluyente.		
La solución debe brindar los datos de cada endpoint: o Estado del cambio en comparación con la versión del		

esquema previamente aprendida. o Uso de datos confidenciales en las solicitudes a este endpoint. o Recuento de solicitudes y orígenes únicos que utilizan este endpoint. o Indicación de la API pública (si se accedió desde otras direcciones públicas). o Fechas de primera y última visita (estos datos se guardan después de 7 días).		
Los tipos de datos confidenciales cuyo uso se detecta mediante el descubrimiento de API incluyen: o UUIDs. o Emails. o Números de tarjetas de crédito. o IP y MAC addresses. o Social Security Numbers. o Números de teléfono. o IBAN. o SSH Keys. o Certificates. o Números de identificación del vehículo. A solución deberá también utilizar las funciones de WAF para detectar y bloquear automáticamente los payloads maliciosos en la API.		
Funcionalidades para la protección anti-bot:		
La solución deberá poder inyectar scripts en páginas de aplicaciones web, como páginas de inicio de sesión o utilizar algún otro mecanismo para recopilar datos sobre patrones de entrada y canalice secuencias de pulsaciones de teclas, movimientos del ratón y toques con los dedos. Esto con el fin de poder diferenciar a un humano de un bot		
La solución deberá poder identificar estos patrones en caso de que un bot los utilice.		
La solución deberá poder tomar una decisión si la entrada es ingresada por un humano o por un script automático (como un bot), y bloquear esta actividad.		
La solución debe poder detener el relleno de credenciales (credential stuffing), los ataques de fuerza bruta y el site scraping con la protección avanzada de bots.		
Rate Limit:		
• La solución deberá tener la capacidad de limitar la cantidad de solicitudes a una URI coincidente dentro de un período de tiempo configurado, de acuerdo con el identificador de origen.		
• El mecanismo debe soportar las siguientes condiciones: o URI		

▪ "/" para que todas las solicitudes coincidan con los dominios del recurso. o Expresión regular de coincida con el campo URI o Identificador de origen ▪ IP de origen ▪ CIDR ▪ Header ▪ Cookie o Limites el número máximo de solicitudes en un período de tiempo específico. o Unidad de tiempo: el ámbito de tiempo en el que se aplica el límite		
La configuración debe soportar ser aplicadas en el modo (Prevenir/Detectar/Inactivo)		

3.1.3 CONDICIONES DE VISITAS DE SOPORTE, MANTENIMIENTO, CAPACITACIÓN Y GARANTIA

CONDICIONES DE VISITAS DE SOPORTE, MANTENIMIENTO, CAPACITACIÓN Y GARANTIA	**CUMPLE (SI/NO)**	**¿CÓMO SE VERIFICA?**
Realizar un afinamiento, configuración, pruebas y puesta en funcionamiento, cuando aplique, de la Actualización a realizar sobre los equipos tipo APPLIANCE (hardware y software) que actualmente cuenta la universidad.		
Realizar las nuevas configuraciones. Después de realizar el proceso de actualización, se acordará el proceso de administración de cambios para la creación de nuevas reglas o configuraciones, previa aprobación de la UNIVERSIDAD PEDAGOGICA NACIONAL		
Realizar la Actualización de nuevas versiones de software y parches, previa autorización de la UNIVERSIDAD PEDAGOGICA NACIONAL y por medio del proceso de control de cambios.		
Realizar Backup de las configuraciones antes y después de cada cambio, con el fin de garantizar una respuesta oportuna en caso de alguna eventualidad que requiera la reconfiguración de los equipos utilizados en la solución.		
Aplicar las mejores prácticas y aseguramiento de los servicios		
El proponente deberá entregar la documentación técnica detallada de toda la actualización realizada		

El proponente deberá entregar un informe técnico mensual durante el tiempo de garantía y/o soporte sobre el desempeño de la plataforma mantenida		
Deberá realizar análisis previo de la plataforma tecnológica actual: hardware, software, red de comunicaciones, condiciones ambientales y sistemas de información.		
Deberá efectuar Transferencia de conocimientos en los productos ofrecidos. El proponente debe brindar capacitación y transmisión de conocimientos de la renovación sobre la solución instalada.		
Realizar las Pruebas necesarias para garantizar el buen funcionamiento de la solución		
Efectuar Administración, Seguimiento, monitoreo a los equipos objeto del contrato.		
Para la prestación del servicio se requiere que el proponente cuente con un esquema de mesa de Ayuda, donde se puedan generar los reportes de incidentes frente a la prestación del servicio. Adjuntar Metodología y mencionar el software con el cual realiza esta función.		
Detectar y reaccionar oportunamente ante incidentes de seguridad de la información, de acuerdo a los niveles de servicio (SLAs).		
Brindar constantemente recomendaciones que permitan obtener un mejor nivel de mitigación de riesgos derivados del uso de la tecnología.		

Se debe brindar un componente de alarma para la detección automática de eventos de seguridad, que faciliten la gestión de los mismos sobre la infraestructura tecnológica		
En caso de no ser posible la solución remota o telefónica, se requiere prestación del servicio en sitio, de acuerdo a los niveles de servicio pactados		
Se requiere servicio de análisis de log y generación de reportes de manera periódica.		
El contratista deberá brindar soporte remoto y/o en sitio dependiendo el nivel de criticidad de la solicitud realizada para fallas e implementaciones.		

Dentro del Servicio de Seguridad debe realizar un análisis de vulnerabilidades que incluya lista de Vulnerabilidades encontradas con su respectivo plan de remedición, efectuando la presentación y socialización al personal técnico de la Subdirección de Gestión de Sistemas de Información.		
El proponente deberá adjuntar a la propuesta mínimo una certificación de haber realizado un análisis de vulnerabilidad de este tipo en una entidad superior a 500 usuarios y otra certificación adicional en una entidad de 3000 usuarios. El ingeniero que realizará el análisis de Vulnerabilidad debe ser un ingeniero con especialización en seguridad informática, certificado por el Fabricante de los equipos Firewall en HA a renovar y certificación ISO/IEC 27001:2022 con mínimo 2 certificaciones de experiencia en mínimo 2 entidades en donde haya realizado, soportado consecutivamente durante 5 años esta labor de análisis de vulnerabilidades.		
El proponente debe ser distribuidor autorizado del fabricante de los equipos a renovar, lo cual debe acreditar, mediante presentación de certificación vigente, expedida por el Fabricante, no mayor a 15 días anteriores a la fecha del cierre de la presente Convocatoria Pública y dirigida a la UNIVERSIDAD PEDAGOGICA NACIONAL, donde se especifique que se encuentra autorizado para licenciar, vender y soportar técnicamente las soluciones de seguridad en Colombia. La certificación debe indicar que el proponente cuenta con certificación CCSP (Certified Collaborative Support Provider), que tiene nivel mínimo de **Professional Partner o superior.**		
El oferente deberá realizar el correspondiente soporte técnico en sitio (7x24) cada vez que se realice el requerimiento por fallas de funcionamiento del producto durante el tiempo de vigencia de las licencias.		
El soporte deberá incluir la puesta en marcha de RELEASE y PATCHES necesarios para corregir problemas y efectuar mejoras sobre la solución y mantenerla actualizada en su última versión disponible en el mercado.		

El oferente debe ofrecer soporte técnico vía telefónica e Internet, como primer nivel de atención.		
El proponente debe especificar claramente en su propuesta los datos mediante los cuales La UNIVERSIDAD PEDAGOGICA podrá solicitar los servicios de soporte y que deberán ser como mínimo: Una dirección de correo electrónico, un sistema de tickets vía web, un teléfono fijo y por lo menos una línea de celular, ésta última disponible 7 días x 24 horas a la semana. Durante la vigencia de las licencias, el proponente debe realizar dos (2) mantenimientos preventivos de la solución, para ello debe entregar un plan de trabajo que contenga al menos: Nombre de la actividad, tiempo estimado, fecha estimada, posibles afectaciones y responsables. Así mismo, al finalizar el mantenimiento preventivo debe entregar un informe con los resultados de este.		
La garantía ofrecida por el fabricante debe cubrir todos los incidentes por fallas de Software. Si la falla no puede ser resuelta por el fabricante dentro de las 12 horas siguientes al reporte del incidente (Interrupción del servicio altamente critica para La		
Universidad Pedagógica), el proponente se debe comprometer a gestionar con el fabricante y a restablecer el servicio en un periodo adicional de máximo de 24 horas.		
El proponente deberá demostrar que cuenta con equipos Firewall Appliances del mismo Fabricante de los equipos que tiene la Universidad, que permitan reemplazar estos en caso de alguna falla o indisponibilidad de los mismos. (adjuntar documentación).		
De acuerdo con lo establecido en el Artículo 5 de la resolución 2710 de 2017 del Ministerio de las Tecnologías de Información y Comunicaciones, el proponente deberá entregar certificación del fabricante en donde se evidencie que la solución ofertada soporta IPV6 nativo en coexistencia con IPV4, de la solución o servicios listados en las Especificaciones técnicas mínimas, expedida por el fabricante		
Los proponentes deben adjuntar certificaciones vigentes del fabricante dirigidas a la Universidad que incluya los siguientes aspectos: Carta expedida por el fabricante con autorización al distribuidor para vender lo requerido, dirigida a la Universidad Pedagógica Nacional, con fecha de expedición no mayor a quince (15) días antes del cierre de la presente convocatoria, indicando que son aptos para el diseño en implementación de la tecnología con base en la renovación ofrecida.		
El proponente debe entregar en físico y en digital la documentación de la configuración del estado inicial de la solución Perimetral y su licenciamiento.		

El proponente deberá realizar un monitoreo, de manera proactiva, de la solución ofertada con el fin de alertar los problemas y proponer una solución más rápida y verificación de un correcto funcionamiento de todos los servicios mediante un SOC (Adjuntar un documento explicativo del proceso de monitoreo que prestará a la Universidad y las herramientas y soluciones utilizadas que garanticen este servicio). De este servicio se deberá entregar un informe mensual.		
El proponente deberá entregar Documentación con un análisis de buenas prácticas en: Seguridad informática para Windows Data Center 2019 y Seguridad informática para SQL/Server, Última Versión		
El proponente deberá realizar capacitación básica de 20 horas a dos (2) personas en ISO 27001, y en Ciberseguridad el cual debe ser dictado por un profesional en ingeniería, certificado ISO 27001 y Ethical Hacking. Deberá aportar certificación respectiva y haber dirigido al menos un equipo de auditores como auditor líder en ISO27001.		

4. OBLIGACIONES DEL CONTRATISTA

4.1 OBLIGACIONES DEL CONTRATISTA

1. El futuro contratista acepta con el perfeccionamiento del contrato, el envío de citaciones, comunicaciones y requerimientos a través la plataforma transaccional del SECOP II y se responsabiliza por su diaria verificación. De igual forma autoriza con el perfeccionamiento del contrato, a recibir citaciones, comunicaciones y notificaciones al correo electrónico registrado en el SECOP II y/o al diligenciado en la carta de presentación de la propuesta.
   PARAGRAFO: Podrá en todo caso, el supervisor, interventor u ordenador del gasto, enviar citaciones, comunicaciones o requerimientos a través de otros medios digitales o físicos, siempre y cuando se permita la trazabilidad de la actuación, a la luz de la normatividad vigente.
2. Publicar en el SECOP II los documentos de ejecución contractual, incluida la Garantía Única de Cumplimiento dentro de los 3 a 5 días hábiles siguientes del perfeccionamiento del contrato y los demás de competencia del contratista de acuerdo a las instrucciones impartidas por el supervisor del contrato.
3. Responder por el manejo de documentos de manera eficiente y oportuna haciendo la devolución con los expedientes a cargo con la documentación foliada, legajada, organizada, rotulada y almacenada, cumplimento los estándares y directrices de gestión documental y Tablas de Retención Documental (TRD) vigentes. (si aplica)
4. Mantener estricta reserva y confidencialidad sobre la información que conozca con ocasión del contrato.
5. Realizar la consignación o transferencia del impuesto de timbre
6. Suscribir el acta de inicio una vez se han cumplido los requisitos de perfeccionamiento y ejecución del contrato.
7. Atender las instrucciones relacionadas con el objeto y obligaciones, que realice el supervisor del contrato.
8. Entregar para cada pago, la certificación suscrita por el representante legal o revisor fiscal, que acredite el cumplimiento del pago de aportes al sistema de seguridad social integral,

parafiscales, ICBF, SENA y cajas de compensación familiar de los últimos seis (6) meses, de conformidad con el artículo 50 de la Ley 789 de 2002 o aquella que la modifique, adicione o complemente. (Aplica para personas jurídicas contratistas).

9. Mantener la vinculación laboral o la relación contractual durante el plazo de ejecución del contrato con personas vulnerables, marginadas y/o excluidas de la dinámica productiva de la ciudad, de acuerdo con lo expuesto en la Directiva 001 del 31 de enero de 2011, establecidas en la propuesta.

(Si aplica)

10. Realizar las solicitudes de modificación al contrato, en caso de requerirse, como mínimo dentro de los diez (10) días hábiles anteriores a la fecha en que se pretende su efectividad.

PARÁGRAFO: La UPN se reserva la posibilidad de aceptar o negar la solicitud, de acuerdo con su estudio, justificación y las necesidades de la contratación.

4.2 OBLIGACIONES ESPECÍFICAS

El contratista deberá responder y entregar lo siguiente:

1 Firmar el acta de inicio una vez se haya perfeccionado y reunido los requisitos para la ejecución del contrato de Prestación de Servicios.

2 Entregar la consignación o transferencia del impuesto de timbre

3 Ejecutar el objeto del contrato en coordinación con el personal técnico de la DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.

4 Entregar la totalidad de los productos y servicios ofrecidos como valores agregados.

5 Cumplir y entregar todo lo relacionado en el Anexo No. 2 ESPECIFICACIONES TÉCNICAS.

6 Acordar de manera mancomunada con el supervisor del contrato, dentro de los cinco (5) días siguientes a la firma del acta de inicio, un cronograma de entrega y prestación de servicios de las licencias renovadas.

7 Suministrar información suficiente y necesaria para acceder a los servicios de garantía y soporte ofrecidos por el fabricante cuando se llegase a requerir, durante el tiempo de la misma.

8 Entregar la certificación de la activación de los Códigos Identificadores de Soporte (CIS).

9 Entregar la certificación, a manera de paz y salvo, expedida por el fabricante, en donde se constate que la Universidad utiliza legalmente las licencias de las soluciones perimetrales adquiridas.

10 Prestar asistencia técnica y servicio de soporte con los requerimientos de servicios 8 horas al día, 5 días a la semana y realizar 3 visitas en sitio durante la vigencia de las licencias y Servicio no-técnico al cliente durante horas normales de oficina.

11 Atender las observaciones que le haga LA UNIVERSIDAD a través del Supervisor del contrato, siempre que se ajusten a las exigencias propias del objeto contractual e implementar las medidas correctivas a que haya lugar.

12 Sincronizar los tiempos de Licenciamiento ante el fabricante, después de legalizado el contrato.

13 Realizar un afinamiento en todos los componentes de la solución perimetral propuesta.

14 El proveedor deberá realizar la configuración de la consola y sistema perimetral siguiendo las buenas prácticas de implementación dadas por el fabricante para el sector educación.

15 El proveedor debe diseñar e instalar un sistema de repositorios remotos, para que de esta manera estos equipos realicen las descargas de actualizaciones y firmas de la consola principal en horarios no hábiles, y así no afectar el ancho de banda de los canales de comunicaciones de la Universidad.

16 El sistema solución perimetral se debe instalar sobre equipos Windows (7, 8, 8.1,10 y 11), MAC,

Linux y en versiones posteriores que haya a lugar.

17 Se debe garantizar que el sistema solución perimetral sea un agente liviano que no llegue a consumir más del 60% de los recursos de los PCs de la universidad, aparte de las tareas que se ejecutan en estos equipos normalmente.

18 El sistema solución perimetral debe realizar escaneos locales sobre los equipos de cómputo en diferentes periodos de tiempo durante el transcurso del día sin llegar a afectar el rendimiento de los PCs.

19 Se debe garantizar que el sistema solución perimetral realice un escaneo completo de dispositivos periféricos y eliminación de archivos maliciosos antes de que el usuario pueda ejecutar y/o abrir este tipo de archivos.

20 El proveedor deberá realizar la programación de reportes mensuales, para de esta manera conocer el estado de la solución en general (Ej. equipos con solución perimetral instalado, archivos infectados, archivos en cuarentena, estado de actualizaciones, top de equipos infectados, top de virus y malware, entre otros).

21 El proveedor deberá entregar un documento final, el cual incluya licenciamiento, políticas, parámetros de configuración, descripciones de parámetros de configuración, procedimientos de backups, procedimientos de mantenimiento, procedimientos de administración, entre otros.

22 Atender las observaciones que le haga LA UNIVERSIDAD a través del supervisor del contrato, siempre que se ajusten a las exigencias propias del objeto contractual e implementar las medidas correctivas a que haya lugar.

23 Disponer del equipo humano y técnico necesario propuesto para la ejecución del objeto del contrato.

24 Cumplir a cabalidad con las condiciones técnicas y económicas ofertadas.

25 Obrar con lealtad y buena fe, evitando dilataciones y trabas.

26 Ejecución de pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de la plataforma de la seguridad perimetral renovada.

27 Entregar informe de ejecución de entrega que se realice en donde se incluya un resumen de las actividades realizadas (instalación y configuración y sitio), problemas presentados, soluciones utilizadas y recomendaciones.

28 Informar al supervisor de las novedades que se presentan relacionadas con el cumplimiento de las actividades del objeto contractual.

Parágrafo: La propuesta presentada por el Contratista hará parte integral de este contrato.

4.3 OBLIGACIONES DE LA UPN

1. Designar el supervisor para la vigilancia y control de la ejecución del objeto contratado.
2. Pagar el valor del futuro contrato en las condiciones pactadas.
3. Verificar que el futuro contratista realice el pago de aportes al sistema de seguridad social integral, parafiscales, ICBF, SENA y cajas de compensación familiar (cuando a ello haya lugar), en las condiciones establecidas por la normatividad vigente.
4. Verificar que el futuro contratista realice el la consignación o transferencia de recursos por concepto del impuesto de timbre para el perfeccionamiento del futuro contrato.
5. Ordenar en cualquier momento, a través del supervisor del contrato, que se suspenda el servicio si por parte del Contratista existe un incumplimiento sistemático de los requisitos generales de seguridad o de las instrucciones del supervisor a este respecto, sin que el Contratista tenga derecho a reclamo o a la ampliación del plazo de ejecución.

5. FORMA DE PAGO

La Universidad pagará el valor del contrato que resulte del presente proceso de selección, de la forma que a continuación se dispone, previo cumplimiento de los trámites administrativos y financieros a que haya lugar y de los siguientes requisitos, y disponibilidad PAC -Programa Anual Mensualizado de Caja.

Se realizará el pago del 100% dentro de los treinta (30) días hábiles siguientes a la presentación de la factura electrónica de venta, conforme a la disponibilidad del PAC, previa certificación de cumplimiento por parte del supervisor y la acreditación de los pagos por parte del contratista de los aportes al Sistema Integral de Seguridad Social y Parafiscales, conforme a lo señalado en el artículo 23 de la Ley 1150 de 2007, y demás normas que regulan la materia.

Cobro del IVA: El impuesto al valor agregado IVA debe ser calculado conforme al Estatuto Tributario vigente de acuerdo a la naturaleza de los productos a suministrar en desarrollo de este contrato, para este proceso.

Para la procedencia del respectivo pago, el contratista deberá cumplir los siguientes requisitos:

1. Formato de abono a cuenta debidamente diligenciado.
2. Certificación Bancaria, con fecha de expedición no mayor a treinta (30) días, que contenga los siguientes datos:

    - Nombre o Razón Social
    - Numero de NIT.
    - Entidad Financiera
    - Número de cuenta
    - Tipo de cuenta (Ahorros o corriente)

3. Factura Electrónica de Venta. Este último con el cumplimiento de los requisitos señalados en los Artículos 621 y 774 del Código de Comercio, Artículo 617 del Estatuto Tributario Nacional, la Resolución DIAN 000165 de 2023 y Resolución 00119 de julio 2024.y demás normas específicas que rijan la materia.
4. Certificación de paz y salvo del pago de seguridad social integral y parafiscales y obligaciones laborales. Si es U.T o Consorcio se deben anexar igualmente por cada miembro. Tratándose de personas jurídicas, se deberá acreditar el pago de los aportes de sus empleados, a los sistemas mencionados mediante certificación expedida por el revisor fiscal, cuando este exista de acuerdo con los requerimientos de ley, o en su defecto por el representante legal.
5. Si es persona natural, aportar planilla de pago seguridad social y parafiscales; por parte del contratista de las obligaciones frente al sistema de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, cuando a ello haya lugar.

NOTA No. 1. La Universidad no se hace responsable por las demoras presentadas en el trámite para el pago al Contratista cuando ellas fueren ocasionadas por encontrarse incompleta la documentación de soporte o no ajustarse a cualquiera de las condiciones establecidas en el presente Contrato. En atención a lo anterior, la Universidad no pagará intereses moratorios bajo ninguna circunstancia.

NOTA No. 2. La Universidad hará las retenciones a que haya lugar sobre cada pago, de acuerdo con las disposiciones legales vigentes sobre la materia.

NOTA No. 3. El futuro contratista para la acreditación del pago de seguridad social integral y parafiscales, deberá atender lo dispuesto por la Resolución No. 209 del 12 febrero de 2020, expedida por la Unidad Administrativa de Gestión Pensional y Contribuciones Parafiscales de la Protección Social – UGPP. *Por la cual se adopta el esquema de presunción de costos para los trabajadores independientes con contratos diferentes a prestación de servicios personales, conforme a su actividad económica.*

CÉSAR MAURICIO BELTRÁN LÓPEZ
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN