Fecha:	24/10/2024

ASPECTOS TÉCNICOS

Área Solicitante:	Dirección de Planeación y Desarrollo - Subdirección de Sistemas y Tecnologías de la Información y Comunicación
Responsable del área solicitante:	Lina Manchego Almanza
Correo Electrónico Institucional:	sistemasytelematica@correo.unicordoba.edu.co

1. CONCORDANCIA CON EL PLAN DE DESARROLLO

El Plan de Desarrollo de la Universidad de Córdoba establece como en sus perspectivas de calidad, pertinencia e innovación, en el que se define el lineamiento de integración y fortalecimiento TIC y acciones estratégicas de Gestionar recursos para fortalecer la infraestructura académica que soportan los laboratorios que prestan servicio a la docencia. Y la perspectiva Equidad, Inclusión y Bienestar, en su lineamiento de Infraestructura y equipamiento soporte para la comunidad educativa y acciones estratégicas de "Potenciar el ecosistema digital universitario a través del fortalecimiento de la infraestructura tecnológica (internet de alto rendimiento, salas de cómputo, entre otros)"

Así mismo, las actividades misionales de docencia, investigación y extensión y procesos de apoyo y control requieren de gestión sobre la infraestructura de tecnológica de los servidores virtuales; capaz de soportar los requerimientos de las diferentes facultades y departamentos académicos, y las exigencias del entorno digital, y el WAF, Firewall, los switch core y soporte de la red misma ayuda a dar seguridad a esta gestión

2. JUSTIFICACION Y DESCIPCIÓN DE LA NECESIDAD

2.1 JUSTIFICACIÓN:

La Universidad de Córdoba busca, mediante la formulación del Plan de Fomento, mejorar las condiciones de calidad de sus procesos misionales, a través del fortalecimiento de infraestructura tecnológica, acciones en pro de la permanencia estudiantil y la investigación, con el propósito de mantener la acreditación institucional y por ende la acreditación de alta calidad de sus programas académicos y crecimiento de los servicios tecnológicos, que apoyan los programas en los lugares de desarrollo de Lorica, Berástegui, Sahagún, Montelíbano la sede de Montería y CUZ de Planeta Rica, y lugares donde opera La Universidad de Córdoba.

La Universidad cuenta actualmente con una infraestructura servidores físicos y virtuales institucionales; sobre los que se encuentra instalados los sistemas de información y servicios tecnológicos institucionales; los cuales deben ser protegidos antes las amenazas de ciberseguridad y garantizar su comunicación con la modernización de los equipos de red centrales del datacenter, los cuales soportan la comunicación de los servicios institucionales.

En Colombia hay partners especializados en el tema que brindan la implementación de una solución WAF, Firewall y los switches core y soporte de la red. que aumente la seguridad de los sistemas de información institucionales.

2.2 DESCRIPCIÓN DE LA NECESIDAD

La implementación de una solución WAF (Web application Firewall) es esencial para aumentar la protección de las aplicaciones WEB institucionales frente amenazas externas e internar sobre en la gestión de la infraestructura de servidores virtuales.

WAF es una solución que nos aumentan la protección de los aplicaciones y sitio web institucionales frente a las amenazas de:

1. Protección Integral del Ecosistema Digital
La universidad maneja una gran cantidad de datos sensibles, incluyendo información académica, financiera y personal de estudiantes, profesores y empleados. La solución basada en Firewalls, swich cord y WAF ofrece:

•Protección Avanzada contra Amenazas: Los firewalls, proporcionan una capa de defensa robusta contra malware, ransomware y ataques DDoS, asegurando la continuidad operativa de la universidad.

•Control del Tráfico en Tiempo Real: La capacidad de inspección profunda de paquetes (DPI) y la protección contra amenazas basadas en inteligencia artificial permiten detectar y mitigar ataques en tiempo real, minimizando el riesgo de brechas de seguridad.

2. Escalabilidad para Crecimiento Futuro
La infraestructura de la Universidad está en constante crecimiento, con la adopción de nuevas tecnologías como IoT, aprendizaje en línea y sistemas de gestión basados en la nube. La familia de firewalls seleccionada, permite:

•Soportar el Crecimiento de la Red: La arquitectura de alto rendimiento y capacidad de procesamiento de los modelos de la marat garantiza que la infraestructura pueda manejar un aumento en el tráfico y usuarios sin comprometer la seguridad.
•Seguridad en Ambientes Multicloud: la marca facilita la integración con plataformas en la nube y brinda protección para aplicaciones y datos distribuidos, asegurando una transición fluida hacia soluciones tecnológicas más avanzadas.

3. Optimización de la Gestión y Reducción de Costos Operativos
Uno de los retos de gestionar la ciberseguridad en una institución educativa es la complejidad y los costos asociados a mantener sistemas heterogéneot, la universidad puede:

•Consolidación de la Gestión: La plataforma permite una gestión centralizada de todos los dispositivos, lo que facilita la administración de políticas de seguridad de manera eficiente y con menos recursos humanos.

•Reducción de los Tiempos de Inactividad: Al contar con una protección proactiva y automatizada, se reducen significativamente los tiempos de respuesta a incidentes y las posibles interrupciones en los servicios, lo que a su vez disminuye los costos derivados de la inactividad.

4. Cumplimiento Normativo y Protección de Datos
Las universidades están obligadas a cumplir con regulaciones locales e internacionales en cuanto a la protección de datos y privacidad. Con la solución , la Universidad de Córdoba:

•Cumplimiento de Normativas: Los equipos solicitados están diseñados para cumplir con las principales regulaciones de seguridad de datos, como el GDPR, asegurando que la universidad esté alineada con las mejores prácticas globales.

•Protección de Aplicaciones Críticas con el WAF: El WAF (Web Application Firewall) es fundamental para proteger aplicaciones web críticas, como plataformas de gestión académica y financiera, contra vulnerabilidades como inyecciones SQL, cross-site scripting (XSS) y ataques de día cero.

5. Beneficios en el Rendimiento General de la Red
Además de proteger la red, los equipos están diseñados para mejorar la eficiencia del tráfico:

•Mejoras en el Ancho de Banda: Con el procesamiento de seguridad acelerado y el uso eficiente del ancho de banda, la universidad experimentará mejoras en el rendimiento general de la red, garantizando que los usuarios disfruten de una experiencia rápida y segura.

•Reducción de la Latencia: Al integrar soluciones avanzadas de caching y optimización del tráfico, los Firewalls y el WAF mejoran el tiempo de respuesta de aplicaciones y servicios clave.
La implementación de una solución integral de ciberseguridad basada en equipos Firewall y WAF no solo fortalece la seguridad de la Universidad de Córdoba, sino que también aporta beneficios significativos en términos de escalabilidad, reducción de costos, cumplimiento normativo y optimización del rendimiento de la red. Esta inversión es estratégica para proteger la infraestructura digital de la universidad, garantizando un entorno seguro para la enseñanza, investigación y gestión administrativa.

6. Inyección
Los ataques de inyección ocurren cuando se envían datos que no son de confianza a un intérprete de código a través de la entrada de un formulario o algún otro envío de datos a una aplicación web. Por ejemplo, un atacante podría introducir código de base de datos SQL en un formulario que espera un nombre de usuario en texto plano. Si la entrada del formulario no está asegurada de forma adecuada, se acabaría ejecutando el código SQL. Esto se conoce como un ataque de inyección de código SQL.

Los ataques de inyección pueden evitarse al validar o sanear los datos enviados por el usuario. (La validación significa rechazar los datos que tienen un aspecto sospechoso, mientras que la sanitización hace referencia a la limpieza de las partes de aspecto sospechoso de los datos). Además, el administrador de la base de datos puede establecer controles para minimizar la cantidad de información que puede sacar a la luz un ataque de inyección.

Más información sobre cómo evitar la inyección de código SQL.

7. Autenticación rota
Las vulnerabilidades en los sistemas de autenticación (login) pueden dar a los atacantes acceso a las cuentas de los usuarios e incluso la capacidad de poner en riesgo todo un sistema mediante el uso de una cuenta de administrador. Por ejemplo, un atacante puede coger una lista con miles de combinaciones conocidas de nombres de usuarios y contraseñas conseguidas durante una fuga de datos, y utilizar un script para probar todas esas combinaciones en un sistema de inicio de sesión para ver si funciona alguna.

Algunas estrategias para mitigar las vulnerabilidades de autenticación son pedir la autenticación en dos fases (2FA), así como limitar o retrasar los intentos repetidos de inicio de sesión mediante el uso de la limitación de velocidad.

8. Exposición de datos confidenciales
Si las aplicaciones web no protegen los datos confidenciales, como la información financiera y las contraseñas, los atacantes pueden acceder a esos datos y venderlos o utilizarlos con fines maliciosos. Un método popular para robar información confidencial es el uso de un ataque en ruta.

El riesgo de exposición de datos puede minimizarse al encriptar todos los datos confidenciales, y al desactivar el almacenamiento en caché* de cualquier información confidencial. Además, los desarrolladores de aplicaciones web deben asegurarse de que no están almacenando innecesariamente ningún dato confidencial.

*El almacenamiento en caché es la práctica de almacenar temporalmente los datos para reutilizarlos. Por ejemplo, los navegadores web suelen almacenar en caché las páginas web para que, si un usuario vuelve a visitarlas en un periodo de tiempo determinado, el navegador no tenga que recuperarlas de la web.

9. Entidades XML externas (XXE)
Este es un ataque contra una aplicación web que analiza la entrada XML*. Esta entrada puede hacer referencia a una entidad externa, que intenta aprovecharse de una vulnerabilidad en el analizador. En este contexto, una "entidad externa" hace referencia a una unidad de almacenamiento, como un disco duro. A un analizador XML se le puede engañar para que envíe datos a una entidad externa no autorizada, que a su vez puede pasar datos confidenciales directamente a un atacante.

La mejor manera de prevenir los ataques XEE es hacer que las aplicaciones web acepten un tipo de dato menos complejo, como JSON**, o al menos parchear los analizadores XML y desactivar el uso de entidades externas en una aplicación XML.

*XML, o Lenguaje de marcado extensible, es un lenguaje de marcado destinado a ser legible tanto por humanos como por máquinas. Debido a su complejidad y las vulnerabilidades de seguridad, se está dejando de utilizar en muchas aplicaciones web.

**La Notación de objetos de JavaScript (JSON) es un tipo de notación simple y legible para seres humanos que se suele utilizar para transmitir datos a través de Internet. Aunque fue creado originalmente para JavaScript, JSON es independiente del lenguaje y puede ser interpretado por diferentes lenguajes de programación.

10. Pérdida de control de acceso

El Control de acceso hace referencia a un sistema que controla el acceso a la información o a la funcionalidad. Los controles de acceso que no funcionan permiten a los atacantes saltarse la autorización y realizar tareas como si fueran usuarios privilegiados, como los administradores. Por ejemplo, una aplicación web podría permitir que un usuario cambiará la cuenta con la que ha iniciado sesión con solo cambiar parte de una url, sin ninguna otra verificación.

Los controles de acceso pueden asegurarse al asegurar que una aplicación web utilice tokens de autorización* y establezca controles estrictos sobre los mismos.

*Muchos servicios emiten tokens de autorización cuando inician sesión los usuarios. Cada solicitud privilegiada que haga un usuario requerirá que haya un token de autorización. Esta es una forma segura de garantizar que el usuario es quien dice ser, sin tener que introducir constantemente sus credenciales de acceso.

11. Mala configuración de la seguridad

La desconfiguración de la seguridad es la vulnerabilidad más común de la lista, y suele ser el resultado de usar configuraciones por defecto o de mostrar errores excesivamente detallados. Por ejemplo, una aplicación podría mostrar al usuario errores demasiado descriptivos que mostraran vulnerabilidades en la aplicación. Esto se puede mitigar mediante la eliminación cualquier función no utilizada en el código y al asegurarse de que los mensajes de error sean más generales.

12. Scripting entre sitios

Las vulnerabilidades de scripting entre sitios se producen cuando las aplicaciones web permiten que los usuarios añadan código personalizado en una url o en un sitio web que será visto por otros usuarios. Esta vulnerabilidad puede ser explotada para ejecutar código JavaScript malicioso en el navegador de la víctima. Por ejemplo, un atacante podría enviar un correo electrónico a una víctima que parece que viene de un banco de confianza, con un enlace al sitio web de dicho banco. Este enlace podría tener algún código JavaScript malicioso etiquetado al final de la url. Si el sitio del banco no está debidamente protegido contra el scripting entre sitios, ese código malicioso se ejecutará en el navegador de la víctima cuando se haga clic en el enlace.

Las estrategias de mitigación para el scripting entre sitios incluyen evitar las solicitudes HTTP que no sean de confianza, así como validar o sanear el contenido generado por el usuario. El uso de marcos de desarrollo web modernos, como ReactJS y Ruby on Rails, también ofrece cierta protección integrada contra el scripting entre sitios.

13. Deserialización no segura

Esta amenaza se dirige a las numerosas aplicaciones web que serializan y deserializan datos con frecuencia. La serialización implica tomar objetos del código de la aplicación y convertirlos en un formato que pueda ser utilizado con otro objetivo, como almacenar los datos en el disco o transmitirlos. La deserialización es justo lo contrario: convertir los datos serializados de nuevo en objetos que la aplicación pueda utilizar. La serialización es como meter los muebles en cajas antes de una mudanza, y la deserialización es como sacarlos de las cajas y volver a montarlos después de la mudanza. Un ataque de deserialización inseguro es como si la empresa de mudanzas manipulara el contenido de las cajas antes de desembalarlas.

Una explotación de deserialización insegura es el resultado de la deserialización de datos desde fuentes no confiables, y puede tener graves consecuencias, como los ataques DDoS y los ataques de ejecución remota de código. Aunque se pueden tomar medidas para intentar atrapar a los atacantes, como la supervisión de la deserialización y la implementación de comprobaciones de tipo, la única forma segura de protegerse antes los ataques de deserialización insegura es prohibir la deserialización de datos desde fuentes no fiables.

14. Uso de componentes con vulnerabilidades conocidas
Muchos desarrolladores web modernos utilizan componentes como bibliotecas y marcos en sus aplicaciones web. Estos componentes son piezas de software que ayudan a los desarrolladores a evitar el trabajo redundante y a ofrecer la funcionalidad necesaria; un ejemplo común son los marcos frontales como React y las bibliotecas más pequeñas que se utilizan para añadir iconos compartidos o pruebas a/b. Algunos atacantes buscan vulnerabilidades en estos componentes que luego pueden utilizar para orquestar ataques. Algunos de los componentes más famosos se utilizan en cientos de miles de sitios web; un atacante que encuentre un agujero de seguridad en uno de estos componentes podría dejar cientos de miles de sitios vulnerables.

Los desarrolladores de componentes suelen ofrecer parches de seguridad y actualizaciones para tapar las vulnerabilidades conocidas, pero los desarrolladores de aplicaciones web no siempre tienen las versiones parcheadas o más recientes de los componentes que se ejecutan en sus aplicaciones. Para minimizar el riesgo de ejecutar componentes con vulnerabilidades conocidas, los desarrolladores deben eliminar de sus proyectos los componentes que no utilicen, así como asegurarse de que reciben componentes de una fuente de confianza y de que estos estén actualizados.

15. Registro y supervisión insuficientes
Muchas aplicaciones web no toman suficientes medidas para detectar las fugas de datos. Se suele tardar unos 200 días de media en detectar una fuga después de que esta se haya producido. Esto da a los atacantes mucho tiempo para causar daños antes de que haya una respuesta. OWASP recomienda que los desarrolladores web implementen planes de registro y supervisión, así como de respuesta a incidentes, para asegurarse de que están al tanto de los ataques a sus aplicaciones.

FIREWALL

El firewall debe combinar seguridad impulsada por IA y aprendizaje automático para brindar protección contra amenazas a cualquier escala. Obtenga una visibilidad profunda de su red y vea aplicaciones, usuarios y dispositivos antes de que se conviertan en amenazas.

Se requiere capacidades de seguridad AI/ML que se extienden a una plataforma de estructura de seguridad integrada que ofrezcan redes seguras que son amplias, profundas y automatizadas. Se requiere protejer la red de extremo a extremo con protección perimetral avanzada que incluya seguridad web, de contenido y de dispositivos, mientras que la segmentación de la red y la SD-WAN segura reduzcan complejidad y el riesgo en las redes de TI híbridas.

Se requiere controlar, verificar y facilitar automáticamente el acceso de los usuarios a las aplicaciones, reduciendo las amenazas laterales al proporcionar acceso solo a los usuarios validados. La protección contra amenazas ultrarrápida y la inspección SSL debe brindar seguridad en el borde que puede ver sin afectar el rendimiento.

Características requeridas:

Parte de cada cortafuegos firewall debe tener, entre otras cosas, el uso gratuito de IPSec y SSL VPN. Se requiere que, la VPN que sea gratuita puede utilizarse como cliente VPN.

Se requiere la opción de operar el cortafuegos con capacidad multicliente, de manera que se pueda operar los cortafuegos para diferentes departamentos de manera granular.

El soporte debe tener la opción de ponerse en contacto directamente con el fabricante en caso de problemas o preguntas.

LOS SWITCHES requieren alto rendimiento, seguridad y resiliencia, como elección óptima para redes de campus y centros de datos. Con 48 puertos de 25G, 8 puertos de 100G y 2 puertos de 10G.

Características Principales:

Contar con posición importante en Gartner Magic Quadrantpara cortafuegos de red e infraestructura WAN Edge

Redes orientadas a la seguridad:Redes convergentes y seguridad

Seguridad para empresas con servicios consolidados basados en IA / ML

Conocimiento profundo de las aplicaciones, usuarios, y dispositivos más allá de las técnicas tradicionales de firewall

Alto rendimiento con baja latencia

Opciones de implementación independiente o integrada

Implementación sin intervención

Gestión en la nube y en las instalaciones

Interfaz intuitiva de gestión

Cumple con los estándares de acceso y aplicación de políticas

Escalable y flexible con fuentes de alimentación duales intercambiables en caliente

Segmentación y Cumplimiento de Políticas: El Switche debe facilitar la implementación de políticas de seguridad en el nivel de acceso, permitiendo la segmentación eficiente del tráfico y limitando la exposición a amenazas. Las políticas de próxima generación deben garantizar una seguridad efectiva en el núcleo de la red.

SASE y Acceso Seguro: Esta arquitectura empresarial proporciona una base incorporada para el acceso de red de confianza cero (ZTNA) y la infraestructura de acceso seguro a servicios (SASE), ofreciéndote flexibilidad para desplegar el nivel de seguridad necesario en el borde de tu red.

Núcleo y Centro de Datos Escalables y Flexibles: Escalando sin esfuerzo para satisfacer las demandas de los núcleos de campus y centros de datos de próxima generación, FortiSwitch ocupa un espacio mínimo en el rack mientras ofrece rendimiento y escalabilidad. Soporta hasta 48 puertos en un factor de forma compacto de 1 RU, con opciones de medios variados para adaptarse a tu entorno.

SWICH CORD DE COBRE

Experimenta un rendimiento excepcional con el swich de cord, un conmutador diseñado para satisfacer las demandas de los centros de datos intensivos en ancho de banda. Con capacidad para 10 GE, este conmutador garantiza un rendimiento óptimo para aplicaciones críticas.
Características Destacadas:

Capacidad elevada para despliegues en Top of Rack o redes empresariales.
Máxima disponibilidad gracias a las fuentes de alimentación duales intercambiables en caliente.
Gestión sencilla a través de interfaz web o de línea de comandos.
Funciones de seguridad del conmutador protegen la infraestructura sin agregar latencia.
Puertos de acceso 1 GE o 10 GE, en un factor de forma compacto de 1 RU.
Capacidad de 40 GE.

Beneficios Clave:
Capacidad futura con 10 GE para satisfacer las exigencias de centros de datos y redes centrales.
Máxima disponibilidad de red al eliminar el tiempo de inactividad con fuentes de alimentación duales.
Gestión simple a través de interfaz web o CLI para una configuración y visibilidad sin complicaciones.

3. DESCRIPCION DEL OBJETO, PLAZO Y LUGAR DE EJECUCIÓN

3.1 DESCRIPCIÓN DEL OBJETO:

SUMINISTRO E INSTALACION DE LOS EQUIPOS WAF, FIREWALL Y SWICH CORD PARA LA CIBERSEGURIDAD DE LAS APLICACIONES INSTITUCIONALES ALOJADAS EN LOS SERVIDORES INSTITUCIONALES DEBIDO A LA DEMANDA Y CRECIMIENTO DE LOS SERVICIOS TECNOLÓGICOS, QUE APOYAN LOS PROGRAMAS EN LOS LUGARES DE DESARROLLO DE LORICA, BERÁSTEGUI, SAHAGÚN Y MONTERÍA, CUZ DE PLANETA RICA, MONTELÍBANO Y LUGARES DONDE OPERA LA UNIVERSIDAD DE CÓRDOBA.

Descripción	Cantidad
firewall Hardware plus 1 Year Premium and Unified Threat Protection (UTP), con Inspección de tráfico en tiempo real, Detección y prevención de intrusiones	1

(IPS), Protección contra malware y virus, Control de aplicaciones y visibilidad, Autenticación y autorización de usuarios, Cifrado de tráfico (IPSec, SSL/TLS), Protección contra ataques DDoS, Velocidad de hasta 100 Gbps de tráfico firewall, Conectividad de alta velocidad (10GbE, 40GbE, 100GbE), Soporte para IPv4 y IPv6, Capacidad para manejar hasta 10.000 usuarios simultáneos, Compatible con protocolos de enrutamiento (OSPF, BGP, RIP)	
Hardware plus 1 Year Enterprise Bundle WAF para aplicaciones, Protección contra ataques web (OWASP Top 10), Detección y prevención de intrusiones (IPS, Protección contra malware y virus, Control de acceso y autenticación de usuarios, Cifrado de tráfico (SSL/TLS), Protección contra ataques DDoS, Velocidad de hasta 2 Gbps de tráfico web, Procesamiento de hasta 10.000 solicitudes por segundo, Soporte para IPv4 y IPv6, Compatible con protocolos de enrutamiento (OSPF, BGP, RIP)	1
Swich cord de 48 puertos de fibra Layer 2/3 FortiGate switch controller compatible switch with 48x25G(SFP28) +8x100G (QSFP28)+2x10G(SFP+). Dual AC power supplies	1
Switch-48 puertos de cobre Layer 2/3 FortiGate switch controller compatible switch with 48 x GE/10GE SFP/SFP+ slots and 6 x 40GE QSFP+ or 4 x 100GE QSFP28. Dual AC power supplies	1
25 GE SFP28 passive direct attach Cable 25 GE SFP28 passive direct attach cable 3m for systems with SFP28 slots.	4
100GE QSFP28 Passive Direct Attach Cable, 3m 100GE QSFP28 Passive Direct Attach Cable, 3 m for Systems with QSFP28 slots	6
10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	22
10GE copper SFP+ RJ45 Transceiver (30m range) 10GE copper SFP+ RJ45 transceiver module (30m range) for systems with SFP+ slots	14
soporte 1 Year FortiCare Premium Support para swich cord fibra	1
soporte 1 Year FortiCare Premium Support para swich cord de cobre	1
Servicios de instalación, puesta en servicio del firewall, solución Waff y switche Core	1
"Bolsa para elementos de red Jack, Faceplate, conectores, Patchcord Fibra óptica, Patchcord, Cable UTP, canaletas, tuberías... y tendido, fusión y conectorización de fibra óptica"	1

. Alcance de la contratación:

- Protección de las aplicaciones web institucionales definidas.
- Configuración de Dominios
- Configuración certificado digital.
- Configuración de machine learning para las aplicaciones
- Configuración de detección de bots para aplicaciones.

- ventana de puesta en producción del equipo.
- Afinamiento de protección Web durante la duración del proyecto.
- Implementación de Core fortinet
- Implementación de Switch fortinet
- Soporte y actualizaciones liberadas sobre el Licenciamiento por un año, lo cual incluye:
  - Incluye atención a incidentes y requerimientos de soporte nivel 2 durante el
  - periodo de validez del contrato.
  - El servicio de soporte tendrá un cubrimiento de 7x24 durante el periodo del
  - Contrato.
  - El cubrimiento aplica únicamente sobre los equipos Fortinet a los que hace
  - referencia este pliego.
  - El servicio de soporte incluye 1 sesión de mantenimiento preventivo al año. El
  - mantenimiento cubre temas lógicos únicamente, como revisión de
  - configuraciones, depuración de políticas de FWB, informe, etc.

PRORIDAD	DESCRIPCION	TIEMPO DE RESPUESTA
Consulta	Este tipo de solicitud no requiere intervención técnica inmediata. Ejemplos: Revisión de cantidad de VPNs, políticas de FW, traffic shapers o nuevas configuraciones.	24 horas
Evento	Afectación puntual de un servicio en 1% - 30% prioridad 3. Ejemplos: Un servicio DHCP dependiente del NGFW que no esté funcionando / Un usuario con falla de VPN	3 horas
Incidente	Afectación del servicio en 30% - 80% prioridad 2. Ejemplos: varios usuarios o grupos de usuarios con falla de VPN / Publicaciones en el NGFW sin funcionamiento / Un área de la compañía sin servicio de navegación.	2 horas.
Incidente grave	Afectación del servicio en 81%-100% prioridad 1. Ejemplos: Falla de navegación masiva / Caída de todas las publicaciones / Caída masiva de la(s) VPN(s) de usuarios / Pérdida de comunicación con los servicios Core del negocio	1 hora

3.2 PLAZO DE EJECUCIÓN:

El Plazo de ejecución del contrato será hasta el 31 de Diciembre de 2024, contados a partir del acta de inicio

3.3 LUGAR DE EJECUCIÓN:

El lugar de ejecución del contrato será Montería Córdoba en el Lugar de Desarrollo Central Cra. 6ª Nro. 77 305 en la subdirección de Almacén, y las instalaciones y configuraciones se realizarán en las oficinas de la Subdirección de Sistemas y Tecnologías de La Información y Comunicación, ubicada en el Edificio de Biblioteca, de forma remota.

4. ANÁLISIS DEL VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO OFICIAL

El presupuesto oficial es la suma de SETECIENTOS OCHENTA Y NUEVE MILLONES NOVECIENTOS OCHENTA Y CUATRO MIL CIENTO SETENTA Y NUEVE PESOS MCTE ($789.984.179)

Los precios se determinaron de acuerdo a cotización a proveedores especializados en el desarrollo del objeto contractual. Se toma como referencia la cotización de menor valor. La bolsa de elementos se conserva el valor.

ITEM	DESCRIPCION	UND	CANT	VR UNIT	VR TOTAL	VR UNIT	VR TOTAL	VR UNIT	VR TOTAL
1. SUMINISTRO									
1.1	firewall Hardware plus 1 Year Premium and Unified Threat Protection (UTP), con Inspección de tráfico en tiempo real, Detección y prevención de intrusiones (IPS), Protección contra malware y virus, Control de aplicaciones y visibilidad, Autenticación y autorización de usuarios, Cifrado de tráfico (IPSec, SSL/TLS), Protección contra ataques DDoS, Velocidad de hasta 100 Gbps de tráfico firewall, Conectividad de alta velocidad (10GbE, 40GbE, 100GbE), Soporte para IPv4 y IPv6, Capacidad para manejar hasta 10.000 usuarios simultáneos, Compatible con protocolos de enrutamiento (OSPF, BGP, RIP)	Und	1	198.057.660	198.057.660	198.255.719	198.255.719	200.038.238	200.038.238
1.2	Hardware plus 1 Year Enterprise Bundle WAF para aplicaciones, Protección contra ataques web (OWASP Top 10), Detección y prevención de intrusiones (IPS,	Und	1	159.064.832	159.064.832	159.223.897	159.223.897	160.655.480	160.655.480

	Protección contra malware y virus, Control de acceso y autenticación de usuarios, Cifrado de tráfico (SSL/TLS), Protección contra ataques DDoS, Velocidad de hasta 2 Gbps de tráfico web, Procesamiento de hasta 10.000 solicitudes por segundo, Soporte para IPv4 y IPv6, Compatible con protocolos de enrutamiento (OSPF, BGP, RIP)								
1.3	Swich cord de 48 puertos de fibra Layer 2/3 FortiGate switch controller compatible switch with 48x25G(SFP28) +8x100G (QSFP28)+2x10G(SFP+). Dual AC power supplies	Und	1	105.028.830	105.028.830	105.133.859	105.133.859	106.079.118	106.079.118
1.4	Switch-48 puertos de cobre Layer 2/3 FortiGate switch controller compatible switch with 48 x GE/10GE SFP/SFP+ slots and 6 x 40GE QSFP+ or 4 x 100GE QSFP28. Dual AC power supplies	Und	1	80.647.842	80.647.842	80.728.490	80.728.490	81.454.320	81.454.320
1.5	25 GE SFP28 passive direct attach Cable 25 GE SFP28 passive direct attach cable 3m for systems with SFP28 slots.	Und	4	693.160	2.772.640	693.853	2.775.412	700.092	2.800.368
1.6	100GE QSFP28 Passive Direct Attach Cable, 3m 100GE QSFP28 Passive Direct Attach Cable, 3 m for Systems with QSFP28 slots	Und	6	1.435.787	8.614.722	1.437.223	8.623.338	1.450.145	8.700.870

1.7	10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	Und	22	475.890	10.469.580	476.366	10.480.052	480.649	10.574.278
1.8	10GE copper SFP+ RJ45 Transceiver (30m range) 10GE copper SFP+ RJ45 transceiver module (30m range) for systems with SFP+ slots	Und	14	2.222.034	31.108.476	2.224.256	31.139.584	2.244.254	31.419.556
1.9	soporte 1 Year FortiCare Premium Support para swich cord fibra	Und	1	10.964.989	10.964.989	10.975.965	10.975.965	11.074.650	11.074.650
1.10	soporte 1 Year FortiCare Premium Support para swich cord de cobre	Und	1	9.305.680	9.305.680	9.314.988	9.314.988	9.398.739	9.398.739
1.11	Servicios de instalación, puesta en servicio del firewall, solución Waff y switche Core	Glb	1	39.840.000	39.840.000	39.879.840	39.879.840	40.238.400	40.238.400
1.12	Bolsa para elementos de red Jack, Faceplate, conectores, Patchcord Fibra óptic, Patchcord, Cable UTP, canaletas, tuberías... y tendido,fusión y conectorización de fibra óptica	Glb	1	7.977.000	7.977.000	7.977.000	7.977.000	7.977.000	7.977.000
				SUBTOTAL	663.852.251	SUBTOTAL	664.508.144	SUBTOTAL	670.411.017
				IVA 19%	126.131.928	IVA 19%	126.256.547	IVA 19%	127.378.093
				TOTAL	789.984.179	TOTAL	790.764.691	TOTAL	797.789.110

El presupuesto estimado es de $789.984.179, por el cual se solicita CDP

Vigencia 2024	Montería	Berastegui	Lorica	Sahagún	Montelíbano	Planeta Rica
$ 789.984.179	77,31%	10,38%	5,98%	4,74%	0,98%	0,61%
	$610.736.769	$82.000.358	$47.241.054	$37.445.250	$7.741.845	$4.818.903

El valor del contrato a suscribir se pagará de la siguiente manera: 1) Un Anticipo equivalente al 40% del valor del contrato, que deberá será amortizado en su totalidad en el pago final, y un 60% una vez se implemente la ejecución y entrega del objeto contractual en su totalidad.

5. FUENTE DE LOS RECURSOS

Plan de Fomento a la Calidad 2023, Estampilla Departamental y Recaudo Impuesto Registro Departamental

6. JUSTIFICACIONES DE LOS FACTORES DE SELECCIÓN

El artículo 94 del Acuerdo No.111 de 7 de junio de 2017, desarrolla el principio de selección objetiva, señalando los criterios bajo los cuales se debe dar la escogencia del contratista. Es objetiva la selección en la cual se escogerá el ofrecimiento más favorable para el cumplimiento de los fines que persigue la Universidad. En consecuencia, los factores de escogencia y calificación que establezcan la Entidad en los pliegos de condiciones o sus equivalentes tendrán en cuenta los siguientes criterios:

La capacidad jurídica, capacidad financiera y las condiciones de experiencia de los proponentes serán objeto de verificación de cumplimiento como requisitos habilitantes para la participación en el proceso de selección y no otorgarán puntaje. La exigencia de tales condiciones debe ser adecuada y proporcional a la naturaleza del contrato a suscribir y a su valor.

La oferta más favorable será aquella que teniendo en cuenta los factores técnicos y económicos de escogencia y la ponderación matemática y detallada de los mismos, contenidos en los Pliegos de condiciones o solicitudes de oferta, resulte ser la más ventajosa para la entidad, sin que la favorabilidad la constituyan factores diferentes a los contenidos en dichos documentos y siempre que la misma resulte coherente con la consulta de precios y condiciones del mercado

6.1 CRITERIOS DE VERIFICACIÓN

a) **CAPACIDAD TÉCNICA**

EXPERIENCIA

El proponente deberá acreditar su experiencia específica, mediante la presentación de máximo tres (3) contratos ejecutados y terminados, cuyo objeto u alcance se relacione con el **SUMINISTRO E INSTALACION DE SWICH O FIREWAL O NETWORKING**, cuyo valor final sumado, sea igual o superior al cien por ciento (100%) del presupuesto oficial expresado en salarios mínimos legales mensuales vigentes.

El SMLMV (Salario Mínimo Legal Mensual Vigente) que se tomará para la conversión del valor de cada contrato a SMLMV, será el del año en que finalizaron los servicios, de acuerdo con la certificación del contrato que se relacione en la propuesta.

FORMACIÓN Y EXPERIENCIA DEL PERSONAL DE TRABAJO

En el siguiente anexo se relaciona el personal mínimo requerido que se exige para el desarrollo del objeto contractual, para lo cual el proponente deberá relacionarlo dentro de su oferta, cumpliendo las exigencias frente a formación, y experiencia, garantizando su participación para todo el plazo de ejecución, así:

FUNCIÓN A DESEMPEÑAR	EXPERIENCIA Y FORMACION
INGENIERO INSTALADOR	Debe ser una persona para que cumpla la función de Ingeniero instalador que será Ingeniero de Sistemas, Electrónico o afines, quien se compromete a dedicar el cien por ciento (100%) de duración a la ejecución total del Contrato. Este profesional debe tener experiencia en instalación, configuración en Networking, firewall. Debe aportar fotocopias de diplomas y actas de grado, tarjeta o matricula profesional, Debe aportar certificación en ciberseguridad

OTROS REQUISITOS HABILITANTES

- El proponente deberá suministrar una certificación de fábrica dirigida a la entidad donde haga constar que el proponente es Partner de la marca y/o distribuidor autorizado.

DOCUMENTOS DE VERIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO (SG-SST) –REQUISITOS MÍNIMOS PARA HABILITACIÓN

1. Certificado de afiliación a la Administradora de Riesgos Laborales - ARL.
2. Política de Seguridad y Salud en el trabajo (Firmado, fechado y actualizado).
3. Documento que contenga la designación del diseño del Sistema de Gestión de Seguridad y Salud en el Trabajo, correspondiente a la siguiente tabla:

	Empresas con diez (10) o menos trabajadores, clasificadas con riesgo I, II o III	Empresas de once (11) a cincuenta (50) trabajadores clasificadas con riesgo I, II o II	Empresas de más de cincuenta (50) trabajadores, clasificadas con riesgo I, II, III, IV o V y de cincuenta (50) o menos trabajadores con riesgo IV o V
Técnico con licencia en salud ocupacional vigente, que acredite mínimo un (01) año de experiencia certificada y la aprobación del curso virtual de las 50 horas en SST.	Si	No	No
Tecnólogo con licencia en salud ocupacional vigente, que acredite mínimo dos (02) años de experiencia certificada y la aprobación del curso virtual de las 50 horas en SST.	Si	Si	No

Profesional con licencia en salud ocupacional vigente y aprobación del curso virtual de las 50 horas en SST.	Si	Si	Si

4. Documento de aplicación de los estándares mínimos del SG-SST, acorde a la normatividad vigente.
5. Documento con el Reglamento de Seguridad e Higiene industrial (aprobado por el Representante Legal).
6. Reglamento interno de trabajo (aprobado por el Representante Legal).

6.2 CRITERIOS DE PONDERACIÓN

Una vez realizada la verificación jurídica, financiera y técnica y determinado que se reúnen los requisitos mínimos exigidos, el comité evaluador ponderará las propuestas con base en los siguientes criterios de calificación:

FACTOR	PUNTAJE MAXIMO
Factor Calidad	30
Propuesta Económica	60
Apoyo a la Industria Nacional	10
TOTAL	**100 PUNTOS**

6.2.1 FACTOR CALIDAD – DESEMPEÑO DEL CONTRATO EN CONTRATOS SIMILARES (30 PUNTOS)

Si el proponente presenta una (1) certificación de cualquiera de los contratos aportados para acreditar la experiencia, en donde se exprese que como contratista cumplió con el objeto contractual de manera **EXCELENTE**, Se le otorgará 30 puntos

6.2.2 EVALUACIÓN ECONÓMICA (60 PUNTOS)

6.2.2.1 OFERTA ECONÓMICA

El proponente presentará su oferta económica en el formato indicado por la entidad, el cual contiene la descripción de los servicios requeridos por la Universidad.

La UNIVERSIDAD efectuará como correcciones aritméticas las originadas por todas las operaciones aritméticas a que haya lugar en el formulario, en particular las siguientes:

- La multiplicación entre columnas.
- Las sumatorias parciales.
- La totalización de sumatorias.
- La liquidación del valor del IVA.
- La suma del costo total de la oferta

- El ajuste al peso.

Realizadas las correcciones aritméticas y verificadas los requisitos anteriores, se asignará una calificación de acuerdo con el siguiente procedimiento:
A la oferta más económica, se le asignarán 60 puntos.
A las demás ofertas, se les asignará puntaje proporcional respecto de su valor, aplicando la siguiente fórmula:
POI = 60 x (1-(OE-OMB)/OMB)
Donde
PO = Puntaje obtenido
OE = Valor de la oferta sometida a evaluación
OMB = Oferta más barata.

6.2.3 APOYO A LA INDUSTRIA NACIONAL (máximo 10 puntos)

EL PROPONENTE debe manifestar, si los servicios que oferta cumplen con las condiciones establecidas en Parágrafo del artículo 2 de la Ley 816 de 2003 correspondiente a la industria nacional

Para este aspecto, al proponente se le asignarán máximo DIEZ (10) puntos de acuerdo con lo indicado en siguiente tabla, según la procedencia de los servicios ofrecidos:

Origen de los Bienes y Servicios	Puntaje
Bienes y Servicios Nacionales	10
Bienes y Servicios Extranjeros	5
Mixtos (Nacionales y Extranjeros)	3

7. ESTIMACION DE RIESGOS Y FORMA DE MITIGARLOS

De conformidad con el Título XI - de los Riesgos en la Contratación art. 102 al 110 del Acuerdo No. 111 del 7 de junio de 2017, la tipificación, asignación y estimación de los riesgos previsibles en la presente contratación se detalla a continuación:

TIPIFICACION	ESTIMACION	ASIGNACION	MITIGACION
Incumplimiento de obligaciones contractuales	100%	CONTRATISTA	Control Supervisor
Incumplimiento del pago de aportes al sistema de seguridad social o alteración de los soportes de pago del mismo	100%	CONTRATISTA	Control Supervisor – Oficina de Contratación – Garantía de Cumplimiento
Información errónea o desactualizada, aportada por la	100%	ENTIDAD	Control de contratación

entidad para la ejecución del contrato			
Incumplimiento en el pago del valor del contrato	100%	ENTIDAD	Expedición del certificado de disponibilidad presupuestal y del Registro presupuestal de compromiso.
Cambio en las normas tributarias	100%	CONTRATISTA	No hay mitigación
Cambio de la TRM	100%	CONTRATISTA	Análisis de mercado en estudios previos. No hay mitigación en la ejecución

8. SUPERVISIÓN E INTERVENTORÍA

8.1 SUPERVISIÓN

La supervisión del contrato estará a cargo de un profesional universitario de la Subdirección de Sistemas y Tecnologías de la Información y Comunicación, se sugiere el ingeniero ALIRIO MONTALVO VILLADIEGO, En todo caso el ordenador del gasto podrá variar unilateralmente la designación del supervisor, comunicando por escrito al designado, con copia a la Oficina de Contratación.

8.2 INTERVENTORÍA:

"No Aplica".

9. ANEXOS

Solicitud de CDP
Cotización,

10. Aprobaciones

Cargo	Nombre	Firma
Director de Planeación y Desarrollo	MARCELO ESCALANTE BARGUIL	

Proyectó Luis Esteban García Cuida
Revisó: Lina Manchego Lina Manchego.