Anexo Técnico

RENOVACIÓN DE LA SUSCRIPCIÓN DEL SISTEMA DE MICROSEGMENTACIÓN PARA LA GRANJA DE SERVIDORES Y DMZ DE LA FAC.

Requerimientos Técnicos Mínimos requeridos

La FAC requiere la RENOVACIÓN DE LA SUSCRIPCIÓN DEL SISTEMA DE MICROSEGMENTACIÓN PARA LA GRANJA DE SERVIDORES Y DMZ DE LA FAC, correspondiente a trescientas (300) cargas de trabajo (Workloads) para servidores y seis (6) nodos de para Kubernetes y contenedores, actualmente implementadas en la infraestructura tecnológica institucional.

La renovación deberá incluir el acceso a la consola de administración alojada en la nube del fabricante, las actualizaciones, el soporte técnico especializado tanto del fabricante como del partner o canal autorizado que suministre la suscripción por el periodo de duración de la misma, así como las capacidades requeridas para garantizar la continuidad operativa, la administración y el aprovechamiento de las funcionalidades de microsegmentación actualmente desplegadas, reglas de seguridad, cargas de trabajo protegidas y demás configuraciones existentes, conforme a las especificaciones definidas en el anexo técnico.

Las anteriores actividades forman parte integral del alcance funcional de la suscripción y de las capacidades disponibles sobre la plataforma actualmente implementada por la FAC, por lo que no constituyen servicios profesionales independientes, consultorías especializadas, bolsas de horas, dedicación permanente de personal, ni generan costos adicionales a los asociados con la suscripción objeto de renovación

Ítem	**Requerimiento Técnico**
Objeto	Renovación de la suscripción del sistema de microsegmentación para la granja de servidores y dmz de la FAC, actualmente implementada en la Institución.
Cantidad	300 Workload para servidores y 06 Nodos para Kubernetes y contenedores.
Alcance	Suscripción para la protección, segmentación y control de comunicaciones de trescientas (300) cargas de trabajo (Workloads) para servidores y seis (6) Nodos para Kubernetes y contenedores actualmente implementadas en la FAC, incluyendo acceso a la consola de administración alojada en la nube del fabricante, actualizaciones de la plataforma, soporte técnico especializado por parte del fabricante y del partner autorizado, así como las capacidades orientadas a garantizar la continuidad operativa, administración y aprovechamiento de las funcionalidades de microsegmentación durante la vigencia de la suscripción contratada.
Soporte	Soporte técnico del contratista y fabricante durante la vigencia de la suscripción.
Actualizaciones	Incluye acceso a nuevas versiones, actualizaciones, parches y mejoras liberadas por el fabricante durante la vigencia de la suscripción.

Vigencia, activación y acreditación de la suscripción.	• La vigencia de la suscripción objeto de renovación deberá contar con una vigencia mínima de treinta y seis (36) meses contados a partir de la fecha de activación de la misma. • La renovación deberá quedar registrada, validada y garantizada por el fabricante antes de la finalización del plazo de ejecución contractual, mediante certificación expedida por el fabricante o por el partner autorizado correspondiente, en la cual consten la cantidad de cargas de trabajo contratadas, la vigencia reconocida por el fabricante, y la certificación del soporte técnico. • La entrada en vigencia de la suscripción renovada iniciará una vez finalice la vigencia de la suscripción actualmente activa en la FAC, con el fin de garantizar la continuidad de las capacidades de microsegmentación y evitar superposición de períodos de cobertura. • Para efectos de acreditación del cumplimiento contractual, el contratista deberá entregar la documentación y certificaciones que evidencien la renovación de la suscripción, el registro de los beneficios contratados y el cumplimiento de las condiciones técnicas exigidas por la FAC. • La validación de dicha documentación por parte del supervisor constituirá evidencia suficiente del cumplimiento de las obligaciones asociadas a la renovación de la suscripción, sin perjuicio de que la cobertura contratada inicie en una fecha posterior.

Como parte integral de la suscripción y de las capacidades disponibles en la plataforma de microsegmentación actualmente implementada en la FAC, se deberán contemplar los componentes y funcionalidades requeridas para garantizar la continuidad operativa, la administración, el soporte técnico y el adecuado aprovechamiento de la solución durante la vigencia de la suscripción contratada, incluyendo aquellas orientadas al fortalecimiento de la implementación existente y al uso efectivo de las capacidades disponibles dentro de la plataforma:

- Como parte de las capacidades incluidas dentro de la suscripción, la plataforma deberá contar con acceso a soporte técnico especializado por parte del fabricante y del partner autorizado y garantía, bajo un esquema de atención 7x24, incluyendo como mínimo, acceso al portal de soporte, soporte a casos y recursos técnicos asociados, durante toda la vigencia de la suscripción contratada, sin que ello implique la asignación permanente de personal, la contratación de servicios profesionales independientes o costos adicionales para la FAC.

- Los incidentes técnicos podrán ser reportados al contratista vía web, chat y teléfono.

- El **SOPORTE TECNICO** debe incluir como parte de las capacidades incluidas dentro de la suscripción, mecanismos de soporte y atención de incidentes relacionados con la Consola de administración alojada en la nube del fabricante, incluyendo los eventos que afecten la disponibilidad, acceso, administración, visualización de información, gestión de políticas de segmentación, integración de cargas de trabajo y demás funcionalidades propias de la plataforma de microsegmentación.

- El **SOPORTE TECNICO** debe permitir consultas al contratista a través de llamadas telefónicas, correo electrónico.

- El **SOPORTE TECNICO** debe permitir sesiones remotas y atención de acuerdo con lo requerido por la supervisión del contrato y o administrador de la plataforma designado por la FAC, en caso de requerirse, en horario hábil y no hábil. Esto con respecto a la plataforma objeto del presente contrato.

Los siguientes son los términos de respuesta del **SOPORTE TECNICO**, los tiempos definidos a continuación corresponden al tiempo máximo de respuesta inicial, atención o escalamiento del incidente por parte del fabricante o del partner autorizado, contado a partir de la apertura formal del caso por parte de la FAC. Dichos tiempos no corresponden al tiempo de solución definitiva del incidente, el cual dependerá de su complejidad, criticidad y de las actividades técnicas requeridas para su tratamiento.

PRIORIDAD		**DESCRIPCIÓN**	**TÉRMINO DE RESPUESTA**
1	CRITICA	La operación está detenida o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la institución y/o está en situación de emergencia.	Inicio de atención o escalamiento en máximo (2) horas a través del fabricante, partner autorizado o por el mecanismo definido por el administrador de la plataforma y/o el supervisor del del contrato.
2	ALTA	Experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida.	Inicio de atención o escalamiento en máximo 4 horas, de manera remota o la indicada por el administrador de la plataforma y/o el supervisor del contrato.
3	MEDIA	Experimenta una pérdida de servicio menor, el impacto es un inconveniente.	Inicio de atención o escalamiento en máximo 8 horas, de manera remota o la indicada por el administrador de la plataforma y/o el supervisor del contrato.
4	BAJA	No impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas.	Inicio de atención o escalamiento en máximo 24 horas, de manera remota o la indicada por el administrador de la plataforma y/o el supervisor del contrato.

- **CERTIFICACIÓN Y RESPALDO DEL FABRICANTE**

El oferente deberá acreditar que se encuentra autorizado por el fabricante de la solución de microsegmentación ofertada para comercializar, renovar, administrar, soportar y realizar actividades de optimización y fortalecimiento de la plataforma actualmente implementada en la FAC.

Dicha acreditación deberá realizarse mediante certificación vigente expedida por el fabricante o su representante autorizado, en la cual conste que el oferente mantiene una relación comercial activa y cuenta con las capacidades técnicas necesarias para suministrar la suscripción objeto del presente proceso.

La certificación deberá ser presentada junto con la oferta y será objeto de verificación durante la evaluación técnica del proceso.

ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN.

Ref	Descripción
1.01	Debe poder ejecutarse en entornos virtualizados, principalmente basados en VMWare ESXi 5.5, ESXi 6.0 y / o hipervisores KVM
1.02	Debe integrarse con VMware vCenter, Nutanix y otros hipervisores.
1.03	Debe poder ejecutarse en un entorno OpenStack o en cualquier otra plataforma de virtualización.
1.04	Debe soportar implementaciones bare metal y Legacy (Servidores físicos)
1.05	Debe Soportar la instalación de agente en Sistemas Operativos Windows 2003, 2008 (64 bit), 2008 R2 (64 bit), 2012 (64 bit), 2012 R2 (64 bit), 2016, 2019, 2022, 2025, Vista, Windows XP, Windows 7, Windows 10, Solaris, HPUX, AIX, FreeBSD, macOS. De igual manera soportar ambientes tipo OpenShift y Kubernetes y Nubes como AWS, AZURE, GCP
1.06	Debe poder soportar el enforcement de políticas en clústeres K8s basados en CNI Calico, Openshift OVN, y Cilium
1.07	En este tipo de ambientes, el tráfico entrante y saliente deben poderse permitir o ser bloqueado.
1.08	Debe Soportar Linux RHEL, CentOS, Ubuntu, Debian, Rocky, Alma, Oracle Linux y SUSE. El proveedor deberá enumerar todas las distribuciones admitidas.
1.09	Debe poder implementarse en múltiples segmentos de red (VLAN) y dentro de un mismo segmento de red (VLAN)

1.10	Debe permitir el uso de direcciones IP fijas y dinámicas.
1.11	Debe admitir redes y cargas de trabajo IPv6.
1.11	Adicional a las nubes públicas, debe soportar la implementación en nubes privadas y permitir la creación de reglas entre los diferentes entornos.

2. Arquitectura de la solución

Ref	Descripción
2.01	Debe poder monitorear TODOS los flujos de tráfico desde el centro de datos: Este-Oeste (servidor-servidor) y Norte-Sur (red cliente-servidor o servidor-externo, es decir, internet o salientes). La solución también debe monitorear los flujos de tráfico entre máquinas virtuales que se ejecutan en el mismo hipervisor.
2.02	Se requiere que la solución esté basada en una arquitectura distribuida y escalable para soportar, hasta 2,000 hipervisores y servidores on premise / 100,000 máquinas virtuales
2.03	Debe requerir un mínimo de recursos informáticos, de memoria, almacenamiento y de red (ancho de banda, IP, etc.) 1% de Uso de CPU y 2% bajo carga.
2.04	El monitoreo no debe consumir más que los recursos configurados por el cliente (CPU, memoria)
2.05	No debe afectar ni interrumpir la actividad continua de las aplicaciones comerciales del centro de datos, ni afectar el rendimiento de la red, ni siquiera causar ningún tipo de tiempo de inactividad, incluso para la instalación.
2.06	Debe ofrecer una consola central de administración, en el modelo de Software como Servicio.
2.07	De requerirse, debe poderse adicionar la funcionalidad de engaño del mismo fabricante capaz de interactuar de forma independiente y en paralelo con diferentes tipos de atacantes potenciales, sin requerir hacer cambios de enrutamiento
2.08	Debe basarse en una arquitectura resiliente que incluya los diferentes componentes de administración.
2.09	Debe proporcionar mecanismos de respaldo de los eventos y configuraciones y reglas definidas.
2.10	Toda comunicación interna entre los componentes de la solución debe ser completamente segura y autenticada.
2.11	De requerirse, debe contar con la capacidad de adicionar la Funcionalidad de Firewall de DNS sobre el mismo agente de Micro-segmentación (mismo fabricante).

3. Visibilidad

Ref	Descripción
3.01	Debe registrar y presentar todos los flujos de comunicación del datacenter, complementada con información contextual y detallada sobre las cargas de trabajo y las aplicaciones (procesos) de comunicación.
3.02	Debe descubrir automáticamente cualquier flujo de comunicación nuevo en tiempo real
3.03	Debe incluir la visualización de las comunicaciones del centro de datos en mapas gráficos, creados automáticamente a partir de los parámetros y filtros definidos por el administrador
3.04	La solución debe proporcionar mapeo/visualización de todos los flujos que esta establezca, así como también todas sus dependencias en relación con las aplicaciones en diversos entornos no importando el número de conexiones que se establezcan.
3.05	Debe permitirle navegar fácilmente por el mapa y enfocarse en una parte específica de interés, incluyendo aplicaciones específicas
3.06	La solución debe admitir la agrupación de activos basados en etiquetas y tags
3.07	No debe ser una limitante el número de etiquetas y tags, de haber una limitante por favor de señalarlo.
3.08	La solución debe permitir la aplicación de etiquetas o tags en función de: ● IP ● Nombre de host ● Nombre de la imagen del contenedor ● Comando de contenedor ● Etiqueta acoplable ● Nombres de pod ● ID de imagen
3.09	Debe proporcionar una revisión histórica de los datos agregados en una ventana de tiempo predefinida, de al menos 60 días de histórico.
3.10	Debe permitir crear y monitorear políticas de comunicación de aplicaciones desde el mapa de visualización, sin requerir consolas o ventanas adicionales del mismo producto, permitiendo comparar en una sola vista, las políticas y el mapa de visualización.
3.11	Es necesario que pueda recopilar sin requerir infraestructura adicional, como mínimo los siguientes flujos de tráfico: ● Nombre de host ● Dirección IP ● Puerto ● Protocolo ● Proceso

	● Usuario ● FQDN En caso de que alguna de estas capacidades presente restricciones o comportamientos diferenciados de acuerdo con la versión del sistema operativo, distribución o entorno tecnológico soportado, el oferente deberá indicarlo expresamente en su propuesta técnica.

4. Threat Prevention

Ref	Descripción
4.01	Debe detectar, analizar e informar cualquier intento de movimiento lateral sospechoso.
4.02	Deben poderse crear White list para escaneos de red detectados que incluyan etiquetas y puertos
4.03	Debe proporcionar capacidades de detección de anomalías basadas en cambios en los patrones de comunicación del centro de datos
4.04	Debe proporcionar detección de actividad sospechosa basada en patrones conocidos de comunicaciones maliciosas
4.05	Debe incluir dentro de la misma solución, servidores de reputación del mismo fabricante, que permitan identificar dominios clasificados como maliciosos en diferentes categorías.
4.06	Debe incluir dentro de la misma solución, servidores de reputación del mismo fabricante, que permitan identificar IPs clasificadas como maliciosas.
4.07	Debe incluir dentro de la misma solución, servidores de reputación del mismo fabricante, que permitan identificar Archivos/Hashes clasificados como maliciosos

5. Administración y configuración de la solución

Ref	Descripción
5.01	La solución debe permitir administrarse en una única interfaz centralizada de monitoreo y control
5.02	Debe presentar centralmente el estado de implementación y operación de todos los componentes del sistema
5.03	Debe admitir el control de acceso granular basado en roles
5.04	Es necesario registrar todas las acciones de los usuarios del sistema y las llamadas a la API REST en un registro de auditoría estándar
5.05	Debe proporcionar múltiples vistas adecuadas para video walls, analistas de SOC y administración

5.06	Debe permitir activar / desactivar centralizadamente, todos los componentes del sistema, así como controlar su modo de operación (cuando corresponda)
5.07	Debe poder capturar paquetes completos con alcance / duración limitados
5.08	Debe proporcionar informes automáticos periódicos de las actividades y descubrimientos de la solución y enviar de ser necesario, correos electrónicos de soporte
5.09	Debe ofrecer una API REST que permita el acceso programático a las funcionalidades del producto.
5.10	Debe proteger completamente la comunicación del usuario con la API REST
5.11	Debe poder sugerir etiquetas basado en el tráfico detectado (AI)

6. Gestión de políticas de seguridad

Ref	Descripción
6.01	La solución debe incluir un set de reglas/políticas predefinidas (mejores prácticas) que puedan ser implementadas desde el día 1.
6.02	Debe proporcionar la capacidad de crear, administrar y monitorear políticas flexibles de tráfico Este-Oeste y Norte-Sur hasta el nivel de poder especificar una sola carga de trabajo y / o aplicación (proceso) en el origen y en el destino
6.03	La solución debe poder sugerir políticas automáticamente a partir de los datos recopilados (AI). Debe basarse en el aprendizaje del tráfico de las aplicaciones definidas, para posteriormente simular las políticas sugeridas.
6.04	El aprendizaje realizado de los flujos de las comunicaciones de, debe poder recopilar en paralelo múltiples aplicaciones y no de manera secuencial.
6.05	En el caso que se estén utilizando puertos dinámicos, la solución debe sugerir una regla que incluya todos los puertos detectados.
6.06	Estas políticas deben sugerir procesos que incluyan todos sus posibles paths
6.07	Debe guardar las revisiones de políticas y permitir volver a las versiones anteriores
6.08	Debe alertar sobre la violación de la política y proporcionar información detallada sobre la violación de la conexión
6.09	La solución debe permitir aplicar políticas basados en tags o etiquetas.
6.10	La solución debe aplicar una política basada en una dirección IP
6.11	La solución debe aplicar una política basada en un puerto o protocolo.
6.12	La solución debe aplicar políticas basadas en procesos/aplicaciones en sistemas operativos Windows.

6.13	La solución debe aplicar políticas basadas en procesos/aplicaciones en sistemas operativos Linux
6.14	La solución debe aplicar una política basada en FQDN
6.15	La solución debe admitir el uso de reglas basados en Listas Negras.
6.16	La solución debe admitir el uso de reglas basados en Listas Blancas.
6.17	La solución debe permitir segmentación de zonas/entornos.
6.18	La solución debe permitir segmentación de aplicaciones.
6.19	La solución deberá out-of-the box crear casos de cuarentena en donde se puede aplicar rápidamente mediante una etiqueta equipos a cuarentena y así aislar activos en cuestión de segundos/minutos.
6.20	Adicional al aprendizaje de las aplicaciones mediante procesos de automatización de IA, la solución deberá proporcionar plantillas que sugieran políticas para aplicaciones de uso común.
6.21	La solución deberá proporcionar los siguientes mecanismos para definir políticas. ● Escribir/definir reglas manualmente ● Definir reglas a partir de representaciones visuales de flujos de tráfico ● API REST ● Asistente de plantillas ● OS Query ● Sugerencia automática de reglas para infracciones de políticas ● IA
6.22	La solución debe proporcionar una manera de modelar las políticas basados en flujos históricos y así poder evaluar el impacto de las políticas en las operaciones del negocio.
6.23	Es necesario se pueden colocar las políticas en modo de monitoreo para evaluar el impacto de una política sin bloquear los flujos de tráfico. Se deben poder mostrar estas simulaciones visualmente en un mapa
6.24	La solución debe permitir deshabilitar reglas individualmente para solucionar posibles problemas identificados.
6.25	Debe poder permitir la creación de reglas cuya acción pueda ser Permitir, Alertar o Bloquear, no debe restringirse a utilizar una única acción para poder crear las reglas, de manera que ofrezca flexibilidad en la implementación de los procesos de micro-segmentación.
6.26	La solución debe poder revertir una política a una versión anterior.
6.27	La solución debe permitir revisar el último hit de una regla en particular, que facilite la revisión y depuración de las políticas y eliminar reglas no utilizadas.

6.28	La solución de micro-segmentación no debe depender o basarse en los firewalls del sistema operativo Windows y Linux (Iptables) para realizar el enfocerment de las póliticas de micro-segmentación.

7. Integraciones

Ref	Descripción
7.01	Debe proporcionar alertas en tiempo real que contengan informes completos de eventos de seguridad.
7.02	Debe admitir la personalización de alertas por gravedad, contenido, etc.
7.03	Debe poder enviar alertas por email
7.04	Debe admitir el enmascaramiento de información confidencial de alertas de correo electrónico (es decir, contraseñas)
7.05	Es necesario poderse integrar con soluciones tipo SIEM (especificar producto)
7.06	Debe tener la capacidad de integrarse con soluciones de análisis de vulnerabilidades, permitiendo generar segmentaciones automáticas basadas en la información obtenida por la integración
7.07	Debe integrarse con soluciones SOAR
7.08	Debe poderse integrar con soluciones tipo NGAV/EDR
7.09	Debe poder enviar alertas y auditar datos a Slack
7.10	Debería poder exportar IOC a formato STIX
7.11	Debe admitir una API para una integración personalizable con servicios externos.
7.12	Debe permitir integración con API REST que permita las siguientes funcionalidades: ● Definición de política ● Aplicar etiquetas ● Lectura de datos de flujo de tráfico ● Visualización de incidentes
7.13	Deben estar disponibles funciones proactivas / preventivas, vinculación / comunicación con otras soluciones de seguridad. El proveedor debe enumerar todos los sistemas a los que se puede conectar la solución.
7.14	La solución debe integrarse con los siguientes proveedores de la nube para proporcionar información adicional sobre las cargas de trabajo. ● AWS ● Microsoft Azure ● GCP

	● Nube Oracle
7.15	Debe poderse integrar con soluciones de prevención de amenazas en nube (Wiz)

8. Kubernetes

Ref	Descripción
8.01	Ofrecer protección de los contenedores en las fases de compilación, despliegue y ejecución con políticas integradas que se alineen con el framework de cumplimiento de NIST.
8.02	Los agentes de la solución deben funcionar como un DaemonSet directamente en el nodo del clúster.
8.03	Debe recopilar todos los flujos de datos de comunicación entre los POD, así como aquellos que se originan en infraestructuras no basadas en microservicios o que están destinados a ellas.
8.04	Debe ser compatible con las siguientes plataformas de contenedores: EKS; AKS; GKE; OpenShift 3.x/4.x; RKE ARO ROSA Kubernetes nativo
8.05	Poder visualizar todo el flujo de datos de los POD en el mismo mapa de flujo de datos, es decir, el mapa de flujo de datos debe ser único para servidores, equipos de escritorio, cargas de trabajo en la nube y PODs
8.06	Debería ser posible configurar reglas de permisos, alertas y bloqueo para las comunicaciones dentro del entorno. Estas reglas también deberían basarse en etiquetas.
8.07	La política de segmentación de OVN debe implementarse mediante una plantilla predefinida, que sirva de base para crear las reglas a partir de dicha plantilla.
8.08	En el caso de reglas de bloqueo, debe ser compatible como mínimo con OpenShift mediante CNI OVN.
8.09	Debe contar con integración nativa con las plataformas mencionadas anteriormente para recopilar metadatos y etiquetas, y transformarlos automáticamente en etiquetas dentro de la solución, sin necesidad de ajustes ni personalizaciones en la plataforma Kubernetes ni en los pods. Se debe utilizar exclusivamente el objeto "Labels"; no es necesario utilizar ni crear ningún otro objeto en YAML ni en Kubernetes.

8.10	También debería reflejar automáticamente cualquier cambio en los metadatos y etiquetas del clúster, ajustando las reglas de segmentación ya creadas.
8.11	Poder visualizar todo el flujo de datos de los POD en el mismo mapa de flujo de datos, es decir, el mapa de flujo de datos debe ser único para servidores, equipos de escritorio, cargas de trabajo en la nube y POD.
8.12	Debe proporcionar información de comunicación entre los POD, incluyendo qué proceso (contenedor) originó o recibió la comunicación, el puerto y el protocolo utilizados, así como la imagen y la línea de comandos utilizadas, lo que permite identificar el uso indebido dentro de la plataforma Kubernetes.
8.13	Debe mostrar el flujo de datos este-oeste (interno) y norte-sur (comunicación hacia y desde Internet);
8.14	La instalación del agente debe realizarse a través de HELM.
8.15	La solución no debería limitar el número de PODs utilizados por nodo del clúster, ya que esto solo debería estar limitado por la compatibilidad oficial de la plataforma Kubernetes.
8.16	La solución no debería causar ningún impacto ni retraso en el despliegue de recursos en el entorno Kubernetes (Pods, Servicios, etc.).
8.17	La solución debería permitir la creación sencilla de reglas de protección (bloqueo) y, con una sola regla, impedir que el acceso externo al clúster acceda a una aplicación interna del clúster, reduciendo el esfuerzo administrativo y la dificultad para comprender la regla final (por ejemplo, Bloquear máquina virtual externa -> Aplicación K8s).

T1. HERNANDEZ HERNANDEZ LUSBIN	MY. LUIS MAURICIO LEON PINZON
Comité Estructurador Técnico	Gerente del Proyecto