REPÚBLICA DE COLOMBIA

ALCALDÍA MAYOR DE BOGOTÁ D.C.

UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PUBLICOS

UAESP

ANEXO No. 03 ESPECIFICACIONES TECNICAS

MODALIDAD DE SELECCIÓN: SELECCION ABREVIADA – SUBASTA INVERSA

OBJETO: TIC-025 Adquisición de licenciamiento de la solución FIREWALL y servicios relacionados, para control de la seguridad informática perimetral y administración de la seguridad informática en los dispositivos de usuario final de la Unidad Administrativa Especial de Servicios Públicos -UAESP.

BOGOTÁ D.C., JULIO DE 2026

Dependencia solicitante: Oficina de Tecnologías de la Información y las Comunicaciones

Fecha: Julio del 2026

NORMATIVA APLICABLE

Se enumera a continuación la normativa técnica aplicable que debe ser tenida en cuenta para la ejecución y desarrollo del Proyecto por parte del CONTRATISTA y objeto de seguimiento por parte de la SUPERVISION:

- ✓ Ley 23 de 1989: Sobre derechos de autor.
- ✓ Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- ✓ Ley 594 de 2000: Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- ✓ Ley 603 DE 2000: Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
- ✓ Ley 1150 de 2007: Seguridad de la información electrónica en contratación en línea.
- ✓ Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- ✓ Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- ✓ Ley 1341 de 2009: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- ✓ Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- ✓ Decreto 2364 de 2012: Firma electrónica. Decreto 2609 de 2012 Expediente electrónico.
- ✓ Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

- ✓ Decreto 2693 de 2012: Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
- ✓ Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- ✓ Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- ✓ Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- ✓ Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- ✓ Resolución 460 de 2022: Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- ✓ Circular 001 de 2022 Presidencia de la República: Recomendaciones de uso de servicios en la nube como medida para mitigar riesgos de seguridad digital.
- ✓ Decreto 767 de mayo 16 del 2022: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto **Único Reglamentario del** Sector de Tecnologías de la Información y las Comunicaciones.

1. Objeto a contratar

TIC-025 Adquisición de licenciamiento de la solución FIREWALL y servicios relacionados, para control de la seguridad informática perimetral y administración de la seguridad informática en los dispositivos de usuario final de la Unidad Administrativa Especial de Servicios Públicos -UAESP.

2. Alcance del objeto

El alcance del presente proceso de contratación comprende la renovación del licenciamiento de la plataforma institucional de ciberseguridad Fortinet de la Unidad Administrativa Especial de Servicios Públicos – UAESP, la adquisición e implementación de las plataformas FortiAnalyzer y FortiSIEM, y la prestación de los servicios profesionales especializados requeridos para su configuración, integración, optimización, soporte técnico y fortalecimiento de las capacidades técnicas institucionales mediante procesos de transferencia de conocimiento y capacitación oficial con voucher de certificación, con el propósito de garantizar la continuidad operativa, fortalecer las capacidades de monitoreo y gestión centralizada de eventos de seguridad y contribuir a la evolución tecnológica de la plataforma institucional de ciberseguridad. Lo anterior, de conformidad con las Especificaciones Técnicas establecidas.

3. Estado actual de la plataforma institucional de ciberseguridad Fortinet

Como resultado de los proyectos de fortalecimiento de la infraestructura tecnológica adelantados por la Unidad Administrativa Especial de Servicios Públicos – UAESP, actualmente la Entidad cuenta con una plataforma institucional de ciberseguridad basada en tecnologías Fortinet, orientada a la protección de la infraestructura de red, los servicios institucionales y los equipos de usuario final.

La plataforma actualmente implementada se encuentra en operación y constituye el componente principal de la arquitectura institucional de seguridad informática, proporcionando capacidades de seguridad perimetral, protección avanzada de endpoints, detección y respuesta frente a amenazas, administración centralizada y mecanismos de integración entre los diferentes componentes del ecosistema Fortinet. Su implementación permitió fortalecer la postura de ciberseguridad de la Entidad mediante una arquitectura integrada, soportada sobre soluciones físicas, virtuales y servicios SaaS del fabricante.

- Dos (2) dispositivos FortiGate 200G implementados en esquema de Alta Disponibilidad (HA), responsables de la seguridad perimetral de la infraestructura tecnológica institucional.
- Un (1) FortiGate Virtual Machine (FortiGate VM) desplegado sobre Microsoft Azure para la protección de la infraestructura tecnológica alojada en la nube.
- Una plataforma FortiEDR Protect & Respond con capacidades FortiXDR, implementada bajo el modelo SaaS sobre FortiCloud, con capacidad licenciada para quinientos (500) endpoints, encargada de la protección, detección, investigación y respuesta frente a amenazas sobre los equipos institucionales.

Durante la implementación de la plataforma FortiEDR/FortiXDR se realizó el despliegue de la consola de administración, la instalación de los agentes de protección, la organización de los equipos mediante grupos de colectores, la definición de políticas de seguridad, la configuración de playbooks de respuesta y la integración con la infraestructura Fortinet existente, manteniendo la administración centralizada desde la plataforma FortiCloud. Asimismo, la solución fue integrada con los servicios corporativos de directorio activo mediante GPO para el despliegue de agentes y con los dispositivos FortiGate institucionales, permitiendo mejorar la visibilidad de eventos y fortalecer los mecanismos de correlación y respuesta frente a incidentes de seguridad.

Como resultado de dicha implementación, la UAESP dispone actualmente de una plataforma plenamente operativa, con políticas de seguridad, grupos de administración, configuraciones, excepciones, dashboards, eventos históricos e integraciones que hacen parte de la operación diaria de la Entidad. En consecuencia, el presente proceso contractual no contempla la sustitución de la plataforma existente, sino la continuidad de su operación mediante la renovación del licenciamiento vigente y el fortalecimiento de sus capacidades de monitoreo, análisis y gestión centralizada de eventos de seguridad mediante la incorporación de las nuevas plataformas.

3.1. Infraestructura de seguridad perimetral.

La Unidad Administrativa Especial de Servicios Públicos – UAESP dispone actualmente de una plataforma de seguridad perimetral basada en tecnología Fortinet, conformada por dos (2) dispositivos FortiGate 200G implementados bajo un esquema de Alta Disponibilidad (High Availability – HA), encargados de proteger el acceso a la infraestructura tecnológica institucional y garantizar la continuidad de los servicios críticos de la Entidad.

Esta plataforma constituye el punto central de control de las comunicaciones entre la red institucional, los servicios publicados, la infraestructura alojada en Microsoft Azure y las conexiones hacia Internet, permitiendo la aplicación de políticas de seguridad, inspección del tráfico, segmentación de redes, servicios VPN, filtrado de contenido, control de aplicaciones, inspección de amenazas y demás funcionalidades propias de una plataforma de seguridad perimetral de nueva generación.

Como parte de la operación institucional, los dispositivos FortiGate soportan la conectividad de los servicios tecnológicos de la Entidad y se encuentran integrados con la infraestructura de directorio activo, las plataformas de protección de endpoints y los diferentes servicios corporativos que conforman el ecosistema tecnológico de la UAESP, constituyéndose en un componente crítico para la continuidad operativa de la Entidad.

En consecuencia, el presente proceso contractual contempla la renovación del licenciamiento oficial del fabricante, garantizando la continuidad de las funcionalidades actualmente implementadas, el acceso a actualizaciones, inteligencia de amenazas y soporte oficial del fabricante, preservando la arquitectura existente y evitando afectaciones sobre la operación institucional.

3.2 Plataforma de protección de endpoints.

a UAESP cuenta actualmente con una plataforma de protección avanzada de endpoints basada en FortiEDR Protect & Respond con capacidades FortiXDR, implementada bajo el modelo Software as a Service (SaaS) sobre la plataforma FortiCloud del fabricante Fortinet, con una capacidad licenciada para trecientos ochenta (380) endpoints, destinada a la protección de los equipos institucionales frente a amenazas avanzadas mediante mecanismos de prevención, detección, investigación y respuesta.

Como parte del proyecto de implementación, la Entidad realizó el despliegue de la consola centralizada de administración, la instalación de los agentes sobre los equipos institucionales, la organización de los dispositivos mediante grupos de colectores, la definición de políticas de seguridad, la configuración de excepciones, la implementación de mecanismos de respuesta automática y la integración con la infraestructura Fortinet existente, incluyendo los dispositivos FortiGate corporativos y los servicios de directorio activo para facilitar el despliegue y administración de los agentes.

Actualmente la plataforma opera como uno de los principales mecanismos de protección de la infraestructura tecnológica institucional, incorporando funcionalidades de prevención de ejecución maliciosa, protección contra ransomware, control de dispositivos USB mediante Device Control, análisis forense, búsqueda de amenazas (Threat Hunting), administración centralizada e inteligencia de amenazas proporcionada por el fabricante.

Dado que esta plataforma hace parte de la operación diaria de la Entidad, el presente proceso contractual contempla la renovación del licenciamiento actualmente implementado, garantizando la continuidad de las capacidades técnicas existentes, la conservación de las políticas de seguridad, grupos de colectores, configuraciones, excepciones, eventos históricos e integraciones, así como el acceso permanente a las actualizaciones y servicios oficiales del fabricante.

3.3 Infraestructura de seguridad en Microsoft Azure

Como parte de la estrategia de modernización tecnológica y adopción de servicios en la nube, la Unidad Administrativa Especial de Servicios Públicos – UAESP dispone actualmente de una infraestructura de seguridad implementada sobre Microsoft Azure, la cual es protegida mediante un FortiGate Virtual Machine (FortiGate VM) licenciado bajo el esquema Bring Your Own License (BYOL).

Este dispositivo hace parte integral de la arquitectura institucional de ciberseguridad y constituye el componente encargado de proteger la infraestructura tecnológica desplegada en la nube, permitiendo la aplicación de políticas de seguridad equivalentes a las implementadas en la infraestructura on-premise y garantizando un modelo homogéneo de administración y protección para los diferentes ambientes tecnológicos de la Entidad.

El FortiGate VM se encuentra integrado con la arquitectura de red institucional mediante mecanismos de interconectividad segura entre la infraestructura local y los recursos desplegados en Microsoft Azure, permitiendo la protección de los servicios institucionales alojados en la nube, la segmentación de redes, la inspección del tráfico, el control de acceso y la aplicación de las políticas corporativas de seguridad definidas por la UAESP.

La plataforma hace parte del ecosistema Fortinet actualmente implementado en la Entidad y se integra funcionalmente con los dispositivos FortiGate físicos, así como con las plataformas de protección de endpoints e inteligencia de seguridad, permitiendo mantener una arquitectura unificada de administración y una visión integral de los eventos de seguridad generados tanto en la infraestructura local como en los ambientes de nube.

En consecuencia, el presente proceso contractual contempla la renovación del licenciamiento oficial del FortiGate VM, garantizando la continuidad de la operación de la infraestructura de seguridad desplegada en Microsoft Azure, el acceso a las actualizaciones de software, servicios de inteligencia de amenazas, soporte oficial del fabricante y la preservación de la configuración actualmente implementada, evitando afectaciones sobre los servicios institucionales que dependen de esta plataforma.

3.4 Estado actual del licenciamiento institucional

Con el fin de proporcionar a los proponentes una visión general de la infraestructura objeto del presente proceso contractual, a continuación se presenta un resumen de los principales componentes que conforman la plataforma institucional de ciberseguridad actualmente implementada en la UAESP, indicando su estado de operación, el modelo de implementación y el alcance previsto dentro del presente proceso de contratación, diferenciando claramente los componentes cuya continuidad se garantiza mediante la renovación del licenciamiento de aquellos que serán incorporados para fortalecer las capacidades institucionales de monitoreo y gestión de eventos de seguridad.

Componente	Modelo actual	Estado	Capacidad/Licencia	Objeto del proceso
FortiGate 200G	Appliance físico HA	Operativo	Dos (2) equipos	Renovación
FortiGate VM	Máquina virtual Azure (BYOL)	Operativo	Una (1) licencia	Renovación
FortiEDR Protect & Respond con capacidades FortiXDR	SaaS FortiCloud	Operativo	500 Seats	Renovación

Componente	Modelo actual	Estado	Capacidad/Licencia	Objeto del proceso
FortiAnalyzer	No implementado	No disponible	N/A	Adquisición e implementación
FortiSIEM	No implementado	No disponible	N/A	Adquisición e implementación

3.5 Arquitectura funcional de la plataforma institucional de ciberseguridad

La plataforma institucional de ciberseguridad de la Unidad Administrativa Especial de Servicios Públicos – UAESP se encuentra implementada bajo una arquitectura integrada basada en tecnologías Fortinet, en la cual los diferentes componentes de seguridad operan de manera complementaria para proteger la infraestructura tecnológica institucional, los servicios corporativos y los equipos de usuario final.

Actualmente, la seguridad perimetral es proporcionada mediante dos (2) dispositivos FortiGate 200G implementados en alta disponibilidad para la infraestructura local y un (1) FortiGate Virtual Machine desplegado sobre Microsoft Azure para la protección de los recursos tecnológicos alojados en la nube. Estos componentes constituyen el punto central para la aplicación de las políticas institucionales de seguridad, control de acceso, inspección del tráfico y protección de las comunicaciones.

De manera complementaria, la protección de los equipos de usuario final se realiza mediante la plataforma FortiEDR Protect & Respond con capacidades FortiXDR, implementada bajo el modelo Software as a Service (SaaS), la cual proporciona capacidades de prevención, detección, investigación y respuesta frente a amenazas avanzadas sobre los endpoints institucionales, manteniendo la administración centralizada desde la plataforma FortiCloud.

La solución actualmente implementada opera mediante mecanismos de integración entre sus diferentes componentes, permitiendo compartir información relacionada con eventos de seguridad, amenazas, políticas y mecanismos de respuesta, fortaleciendo la capacidad institucional para la protección de la infraestructura tecnológica y facilitando la administración centralizada de la plataforma.

En este contexto, el presente proceso contractual no contempla la sustitución de la arquitectura actualmente implementada, sino la renovación de los componentes existentes y el fortalecimiento de sus capacidades mediante la incorporación de las plataformas FortiAnalyzer y FortiSIEM, las cuales permitirán centralizar el almacenamiento de registros, fortalecer los procesos de monitoreo, correlación de eventos, análisis de incidentes y generación de información para la gestión de la seguridad de la información.

4. ESPECIFICACIONES TÉCNICAS

Renovación del licenciamiento para los dispositivos FortiGate 200G implementados en Alta Disponibilidad (HA).		
No.	**CANTIDAD**	**DESCRIPCIÓN**
1	Dos (2)	**Producto**: Renovación del licenciamiento de los dispositivos FortiGate 200G. **Tipo de requerimiento**: Renovación de licenciamiento. **SKU de referencia:** FC-10-F200G-950-02-36 (o el SKU vigente equivalente definido por el fabricante para la misma modalidad de licenciamiento y vigencia requerida). **Descripción funcional**: Se deberá suministrar la renovación del licenciamiento oficial del fabricante para los dos (2) dispositivos FortiGate 200G actualmente implementados en la infraestructura tecnológica de la UAESP, garantizando la continuidad de la operación de la plataforma de seguridad perimetral, sin pérdida de funcionalidades, servicios de seguridad, capacidades de protección o niveles de soporte actualmente implementados. En caso de que el fabricante sustituya o actualice el licenciamiento asociado al SKU de referencia, deberá suministrarse la licencia equivalente o superior que garantice como mínimo las mismas capacidades funcionales y técnicas. **Características técnicas mínimas:** • Licencias oficiales, nuevas y suministradas por un canal autorizado del fabricante. • Compatibilidad total con los dispositivos FortiGate 200G actualmente instalados. • Compatibilidad con la configuración existente, sin requerir reinstalaciones o migraciones por cambio de licenciamiento. • Mantener la operación en esquema de Alta Disponibilidad (HA). • Garantizar la interoperabilidad con el Firewall Virtual FortiGate VM, la plataforma FortiEDR/FortiXDR y las nuevas plataformas FortiAnalyzer y FortiSIEM. • Permitir la actualización de firmware a las versiones soportadas por el fabricante durante la vigencia del licenciamiento. • Mantener la totalidad de las funcionalidades, servicios de seguridad e integraciones actualmente implementadas en la plataforma institucional de ciberseguridad o sus equivalentes funcionales definidos por el fabricante. **Servicios incluidos:**

Renovación del licenciamiento para los dispositivos FortiGate 200G implementados en Alta Disponibilidad (HA).		
No.	**CANTIDAD**	**DESCRIPCIÓN**
		• Soporte técnico oficial del fabricante durante toda la vigencia del licenciamiento. • Acceso a actualizaciones de software y firmware. • Acceso a los servicios de inteligencia de amenazas, bases de firmas de seguridad y demás servicios asociados al licenciamiento ofertado. • Acceso al portal oficial del fabricante para la descarga de software, documentación técnica y gestión de casos de soporte. • Todos los beneficios y prestaciones asociados al esquema de licenciamiento ofertado por el fabricante para el SKU suministrado. Nota: El SKU relacionado corresponde a la referencia técnica identificada durante el estudio de mercado y se incluye con fines de identificación del licenciamiento requerido. En caso de que el fabricante sustituya, actualice o descontinúe dicho código comercial, el contratista deberá suministrar el SKU vigente equivalente o superior, garantizando como mínimo las mismas funcionalidades, capacidades técnicas, modalidad de soporte y servicios asociados, sin generar costos adicionales para la UAESP.

Renovación del licenciamiento del Firewall Virtual FortiGate VM implementado en Microsoft Azure.		
No.	**CANTIDAD**	**DESCRIPCION**
2	Una (1)	**Producto:** Renovación del licenciamiento del Firewall Virtual FortiGate VM para Microsoft Azure. **Tipo de requerimiento:** Renovación de licenciamiento. **SKU de referencia:** FC2-10-FGVVS-814-02-12 (o el SKU vigente equivalente definido por el fabricante para la misma modalidad de licenciamiento y vigencia requerida). **Descripción funcional**: El contratista deberá suministrar la renovación del licenciamiento oficial del Firewall Virtual FortiGate VM actualmente implementado en la infraestructura Microsoft Azure de la UAESP, garantizando la continuidad de la operación de los servicios de seguridad perimetral desplegados en la nube, sin pérdida de funcionalidades, configuraciones, capacidades de protección o niveles de soporte actualmente disponibles. En caso de que el fabricante sustituya o actualice la referencia comercial asociada al licenciamiento, deberá suministrarse el licenciamiento equivalente o superior que garantice como mínimo las mismas capacidades funcionales y técnicas.

Renovación del licenciamiento del Firewall Virtual FortiGate VM implementado en Microsoft Azure.		
No.	**CANTIDAD**	**DESCRIPCION**
		Características técnicas mínimas: • Licenciamiento oficial del fabricante para Firewall Virtual FortiGate VM. • Compatibilidad con la infraestructura Microsoft Azure actualmente implementada por la UAESP. • Capacidad mínima para una máquina virtual de 2 vCPU, de acuerdo con el licenciamiento actualmente implementado. • Compatibilidad con arquitecturas BYOL (Bring Your Own License). • Mantener la totalidad de las funcionalidades, servicios de seguridad e integraciones actualmente implementadas o sus equivalentes funcionales definidos por el fabricante. • Compatibilidad con FortiGate físicos, FortiEDR/FortiXDR, FortiAnalyzer y FortiSIEM. • Permitir la actualización de software y firmware durante la vigencia del licenciamiento. **Servicios incluidos:** • Soporte técnico oficial del fabricante durante toda la vigencia del licenciamiento. • Acceso a actualizaciones de software y firmware. • Acceso a los servicios de inteligencia de amenazas y demás servicios de seguridad incluidos en el licenciamiento ofertado. • Acceso al portal oficial del fabricante para descarga de software, documentación técnica y gestión de casos de soporte. • Todos los beneficios y prestaciones asociados al esquema de licenciamiento suministrado por el fabricante. Nota: El SKU relacionado corresponde a la referencia del licenciamiento actualmente implementado en la infraestructura Microsoft Azure de la UAESP. En caso de que el fabricante sustituya, actualice o descontinúe dicho código comercial, el contratista deberá suministrar el SKU vigente equivalente o superior, garantizando como mínimo las mismas funcionalidades, capacidades técnicas, modalidad de soporte y servicios asociados, sin generar costos adicionales para la UAESP.

Renovación del licenciamiento de la plataforma FortiEDR/FortiXDR para la protección de endpoints y servidores institucionales.		
No.	**CANTIDAD**	DESCRIPCION
3	Una (1), para 380 dispositivos.	**Producto**: Renovación del licenciamiento de la plataforma FortiEDR/FortiXDR. **Tipo de requerimiento**: Renovación de licenciamiento.

Renovación del licenciamiento de la plataforma FortiEDR/FortiXDR para la protección de endpoints y servidores institucionales.		
No.	**CANTIDAD**	DESCRIPCION

		SKU de referencia: FC2-10-FEDR1-393-01-12 o la referencia equivalente que la sustituya oficialmente durante la vigencia del proceso de contratación.
		
		Descripción funcional: El contratista deberá suministrar la renovación del licenciamiento oficial del fabricante para la plataforma FortiEDR Protect & Respond con capacidades FortiXDR actualmente implementada en la UAESP, garantizando la continuidad de las capacidades de protección, prevención, detección, investigación, respuesta y análisis de amenazas sobre los endpoints institucionales, sin pérdida de funcionalidades, configuraciones, integraciones, inteligencia de amenazas o niveles de soporte actualmente disponibles.
		
		La renovación deberá garantizar la continuidad de la administración centralizada desde la consola de gestión Cloud actualmente implementada, manteniendo las políticas de seguridad, grupos de colectores, excepciones, configuraciones, eventos históricos e integraciones existentes. En caso de que el fabricante sustituya o actualice la referencia comercial de la solución, el contratista deberá suministrar el licenciamiento equivalente o superior que garantice, como mínimo, las mismas capacidades funcionales y técnicas actualmente implementadas por la UAESP.
		
		Características técnicas mínimas:
		
		La solución deberá soportar como mínimo la capacidad actualmente licenciada por la UAESP (380 endpoints).
		
		• Mantener la consola de administración Cloud actualmente implementada.
		• Garantizar la continuidad de las funcionalidades Protect & Respond, incluyendo como mínimo:
		  ○ Execution Prevention.
		  ○ Anti-Ransomware.
		  ○ Exfiltration Prevention.
		  ○ Device Control.
		  ○ Communication Control.
		  ○ Threat Hunting.
		  ○ Forensics.
		  ○ Vulnerability Management.
		  ○ Detección basada en comportamiento (Behavioral Detection).
		  ○ Capacidades XDR actualmente habilitadas.

Renovación del licenciamiento de la plataforma FortiEDR/FortiXDR para la protección de endpoints y servidores institucionales.		
No.	**CANTIDAD**	DESCRIPCION
		• Mantener las políticas de seguridad, grupos de colectores, excepciones, configuraciones y eventos históricos existentes. • Garantizar la integración con la infraestructura Fortinet actualmente implementada y con las plataformas FortiAnalyzer y FortiSIEM objeto del presente proceso. • Permitir la actualización de la plataforma, consola y agentes a las versiones oficialmente soportadas por el fabricante durante toda la vigencia del licenciamiento. • Mantener la totalidad de las funcionalidades actualmente implementadas o sus equivalentes funcionales definidas por el fabricante, sin degradación del servicio. **Servicios incluidos:** • Renovación del licenciamiento oficial del fabricante. • Soporte técnico oficial del fabricante durante toda la vigencia del licenciamiento. • Acceso a actualizaciones de la consola, agentes y componentes de la solución. • Acceso a inteligencia de amenazas, firmas, indicadores de compromiso (IOC) y demás servicios asociados al licenciamiento. • Validación del correcto funcionamiento de la plataforma posterior a la renovación del licenciamiento. • Soporte técnico oficial del fabricante durante toda la vigencia del licenciamiento con acceso al portal oficial del fabricante para la gestión de casos de soporte, descarga de software y documentación técnica. • Todos los beneficios y prestaciones asociados al esquema de licenciamiento suministrado por el fabricante. Nota: La renovación deberá garantizar la continuidad de la totalidad de las capacidades actualmente implementadas por la UAESP, incluyendo las funcionalidades Protect & Respond, las capacidades FortiXDR y Device Control utilizadas para la administración y control de dispositivos USB y medios removibles. En caso de que el fabricante modifique la modalidad de licenciamiento o sustituya las referencias comerciales actualmente disponibles, el contratista deb gerá suministrar el licenciamiento vigente equivalente o superior, garantizando como mínimo las mismas funcionalidades, capacidades técnicas, capacidad licenciada (380 Seats) y niveles de soporte oficial del fabricante, sin generar costos adicionales para la UAESP.

Adquisición e implementación de la plataforma FortiAnalyzer para la gestión centralizada de registros (logs), análisis, monitoreo y generación de reportes de seguridad de la infraestructura Fortinet de la UAESP.		
No.	**CANTIDAD**	DESCRIPCION
4	Dos (2)	**Producto:** Plataforma FortiAnalyzer VM. **Tipo de requerimiento:** Adquisición e implementación. **SKU de referencia:** FC1-10-AZVMS-465-01-12 *(o el SKU vigente equivalente definido por el fabricante para la misma capacidad de procesamiento de registros y modalidad de licenciamiento requerida).* La máquina virtual deberá implementarse con los recursos mínimos recomendados por el fabricante para soportar el volumen de eventos licenciado, permitiendo su escalabilidad futura. **Descripción funcional:** El contratista deberá suministrar el licenciamiento oficial de la plataforma FortiAnalyzer e implementar la solución completamente integrada con la infraestructura Fortinet de la UAESP, permitiendo la administración centralizada de registros (logs), el análisis de eventos de seguridad, la generación de reportes técnicos y ejecutivos, la visualización mediante dashboards y el apoyo a las actividades de monitoreo, auditoría y gestión de incidentes de seguridad. La solución deberá quedar completamente instalada, configurada, integrada y operativa al finalizar la ejecución del contrato. **Características técnicas mínimas:** • Plataforma FortiAnalyzer VM licenciada oficialmente por el fabricante. • Capacidad mínima para el procesamiento y almacenamiento de 5 GB diarios de registros (logs) o superior, conservando un histórico mínimo de 90 días en línea sin degradación del desempeño. • Compatibilidad con la infraestructura de virtualización definida por la UAESP, conservando un histórico mínimo de 90 días en línea sin degradación del desempeño. • Integración con los dos (2) dispositivos FortiGate 200G implementados en Alta Disponibilidad (On-Premise). • Integración con el Firewall Virtual FortiGate VM implementado en Microsoft Azure. • Gestión centralizada de registros, eventos y auditoría de los dispositivos Fortinet integrados. • Generación de reportes técnicos, operativos, ejecutivos y programados. • Capacidades de búsqueda, consulta y análisis histórico de registros. Configuración de alertas, eventos y notificaciones. • Compatibilidad para su integración con la plataforma FortiSIEM objeto del presente proceso.

Adquisición e implementación de la plataforma FortiAnalyzer para la gestión centralizada de registros (logs), análisis, monitoreo y generación de reportes de seguridad de la infraestructura Fortinet de la UAESP.		
No.	**CANTIDAD**	DESCRIPCION
		Servicios incluidos: • Suministro del licenciamiento oficial del fabricante. • Soporte técnico oficial del fabricante durante toda la vigencia del licenciamiento. • Instalación y configuración de la plataforma. • Parametrización inicial de la solución de acuerdo con los requerimientos de la UAESP. • Integración con los FortiGate On-Premise, FortiGate VM Azure. Configuración de la recepción, clasificación y almacenamiento de logs. • Configuración de políticas de retención de registros. • Configuración de alertas y notificaciones automáticas. • Configuración de reportes técnicos, operativos y ejecutivos programados. • Configuración de la totalidad de los dashboards estándar disponibles y aplicables a la infraestructura implementada. • Desarrollo y parametrización de mínimo cinco (5) dashboards personalizados, definidos juntamente con la supervisión del contrato. • Validación de la recepción de registros de todos los dispositivos Fortinet integrados. • Afinamiento (tuning) inicial de la plataforma para optimizar el procesamiento y almacenamiento de eventos. • Ejecución de pruebas funcionales y puesta en operación. • Elaboración de la documentación técnica de la implementación, que incluya como mínimo: arquitectura, direccionamiento, integraciones, políticas, dashboards, alertas, reportes, respaldos, procedimientos de operación y recuperación e inventario. • Transferencia de conocimiento al personal técnico de la UAESP, mínimo 6 horas, que pueden ser presencial, virtual o mixto, permitiendo su grabación. Debe incluir material de apoyo, ejercicios prácticos basados en la infraestructura implementada y el desarrollo de casos de uso relacionados con la administración, operación, monitoreo, generación de reportes, análisis de eventos, atención de incidentes y mejores prácticas para la gestión de la plataforma FortiAnalizer. **Nota:** La solución deberá suministrarse completamente implementada y en operación, garantizando la integración exclusiva con la infraestructura Fortinet actualmente implementada por la UAESP (FortiGate On-Premise, FortiGate VM en Microsoft Azure). En caso de que el fabricante sustituya o actualice la referencia comercial del producto, el contratista deberá suministrar la referencia vigente

Adquisición e implementación de la plataforma FortiAnalyzer para la gestión centralizada de registros (logs), análisis, monitoreo y generación de reportes de seguridad de la infraestructura Fortinet de la UAESP.		
No.	**CANTIDAD**	DESCRIPCION
		equivalente o superior, garantizando como mínimo las mismas capacidades funcionales, técnicas y de integración, sin generar costos adicionales para la entidad.

Adquisición e implementación de la plataforma FortiSIEM All-In-One para la gestión centralizada, correlación, monitoreo y análisis de eventos de seguridad de la infraestructura tecnológica de la UAESP.		
No.	**CANTIDAD**	DESCRIPCION
5	Cincuenta (50)	**Producto:** Plataforma FortiSIEM All-In-One. **Tipo de requerimiento:** Adquisición e implementación. **SKU de referencia:** FC1-10-FSM98-180-02-12 *(o el SKU vigente equivalente definido por el fabricante para la capacidad requerida).* **Descripción funcional:** El contratista deberá suministrar el licenciamiento oficial de la plataforma FortiSIEM All-In-One e implementar la solución completamente integrada con la infraestructura tecnológica designada por la UAESP de conformidad con los capacidades mínimas requeridas para su correcto funcionamiento, priorizando las fuentes de información criticas definidos por la UAESP, permitiendo la recolección, normalización, correlación y análisis centralizado de eventos de seguridad, el monitoreo de la infraestructura tecnológica, la generación de alertas, dashboards, reportes y el apoyo a la gestión de incidentes de seguridad. La solución deberá quedar completamente instalada, configurada, integrada, documentada y operativa al finalizar la ejecución del contrato. **Características técnicas mínimas:** • Plataforma FortiSIEM All-In-One licenciada oficialmente por el fabricante, con la versión estable soportada y vigente por el fabricante al momento de la implementación. • Capacidad mínima correspondiente al licenciamiento base de cincuenta (50) dispositivos (Devices), conforme al dimensionamiento definido para el presente proceso contractual. • Recolección, normalización y correlación de eventos de seguridad provenientes de múltiples fuentes de información. • Gestión centralizada de alertas e incidentes. • Dashboards ejecutivos, operativos y técnicos. • Generación de reportes programados y personalizados.

Adquisición e implementación de la plataforma FortiSIEM All-In-One para la gestión centralizada, correlación, monitoreo y análisis de eventos de seguridad de la infraestructura tecnológica de la UAESP.		
No.	**CANTIDAD**	DESCRIPCION
		• Capacidades de búsqueda y análisis histórico de eventos. • Integración con la plataforma FortiAnalyzer. • Integración con los dos (2) dispositivos FortiGate 200G implementados en Alta Disponibilidad (On-Premise). • Integración con el Firewall Virtual FortiGate VM implementado en Microsoft Azure. • Integración con la plataforma FortiEDR/FortiXDR. • Integración con Microsoft Active Directory (Controlador de Dominio On-Premise y su réplica en Microsoft Azure). • Integración con Microsoft 365 mediante los mecanismos soportados por el fabricante. • Integración con Aruba Central, siempre que el fabricante disponga de mecanismos de integración soportados mediante API u otros conectores oficiales. • Integración con plataformas institucionales como Zabbix y GLPI, cuando técnicamente sean parametrizables mediante los mecanismos soportados por el fabricante. • Integración con servidores físicos y/o virtuales críticos para la operación institucional, incluyendo, entre otros, el servidor Proxy Reverso, servidores de virtualización Hyper-V y demás activos críticos que determine la UAESP durante la implementación. • Configuración e integración de las fuentes de información priorizadas por la UAESP, hasta completar la capacidad total de licenciamiento adquirido (50 dispositivos (Devices)) contemplada en el licenciamiento FortiSIEM All-In-One objeto del presente proceso. La priorización de los dispositivos y fuentes de información se realizará conjuntamente entre el contratista y la supervisión del contrato, considerando la criticidad de los activos institucionales y procurando integrar, como mínimo, la infraestructura Fortinet, Microsoft Active Directory, Microsoft 365, Aruba Central (cuando exista integración soportada), plataformas institucionales como Zabbix y GLPI (cuando sean técnicamente parametrizables), así como los servidores físicos y virtuales críticos definidos por la UAESP. • Compatibilidad con futuras integraciones mediante APIs, Syslog, SNMP, WMI, SSH y demás mecanismos soportados oficialmente por el fabricante. • La máquina virtual deberá implementarse utilizando los recursos mínimos de CPU, memoria y almacenamiento recomendados oficialmente por el fabricante para soportar la capacidad licenciada de cincuenta (50) dispositivos, permitiendo su crecimiento futuro, independiente de su arquitectura despliegue (Nube u On-premise).

Adquisición e implementación de la plataforma FortiSIEM All-In-One para la gestión centralizada, correlación, monitoreo y análisis de eventos de seguridad de la infraestructura tecnológica de la UAESP.		
No.	**CANTIDAD**	DESCRIPCION
		• La capacidad de almacenamiento deberá dimensionarse conforme a las recomendaciones oficiales del fabricante para la retención definida por la UAESP durante la implementación. **Servicios incluidos:** • Suministro del licenciamiento oficial del fabricante. • Instalación y configuración de la plataforma. • Parametrización inicial de la solución. • Integración con FortiAnalyzer. • Integración con FortiGate On-Premise. • Integración con FortiGate VM Azure. • Integración con FortiEDR/FortiXDR. • Integración con Microsoft Active Directory y Microsoft 365. • Integración de las fuentes de información priorizadas por la UAESP hasta completar la capacidad licenciada de cincuenta (50) dispositivos. • Configuración de reglas iniciales de correlación basadas en las mejores prácticas del fabricante y ajustadas a la infraestructura priorizada por la UAESP. • Configuración de alertas y notificaciones. • Configuración de dashboards estándar aplicables a la infraestructura implementada. • Desarrollo y parametrización de mínimo cinco (5) dashboards personalizados definidos conjuntamente con la UAESP. • Configuración de reportes automáticos. • Validación funcional de todas las integraciones implementadas. • Afinamiento (tuning) inicial de reglas de correlación, desempeño y generación de alertas. • Soporte técnico oficial del fabricante durante toda la vigencia del licenciamiento. • Elaboración de la documentación técnica de la implementación, que incluya como mínimo: arquitectura, fuentes integradas, reglas, dashboards, alertas, reportes, respaldos, gestión de usuarios, roles, procedimientos de operación y recuperación. • Transferencia de conocimiento al personal técnico de la UAESP con una duración mínima de seis (6) horas, en modalidad presencial, virtual o mixta, permitiendo su grabación. Deberá incluir material de apoyo, ejercicios prácticos basados en la

Adquisición e implementación de la plataforma FortiSIEM All-In-One para la gestión centralizada, correlación, monitoreo y análisis de eventos de seguridad de la infraestructura tecnológica de la UAESP.		
No.	**CANTIDAD**	DESCRIPCION
		infraestructura implementada y el desarrollo de casos de uso relacionados con la administración, operación, monitoreo, correlación de eventos, generación de alertas, creación de dashboards, investigación de incidentes y mejores prácticas para la gestión de la plataforma FortiSIEM. Nota: El presente requerimiento corresponde exclusivamente al licenciamiento base de FortiSIEM All-In-One y las funcionalidades incluidas de manera nativa por el fabricante. La capacidad mínima de cincuenta (50) dispositivos corresponde al dimensionamiento definido para el presente proceso y constituye el alcance mínimo esperado de la implementación. En consecuencia, el contratista deberá realizar el acompañamiento técnico necesario para identificar, priorizar e integrar las cincuenta (50) fuentes de información que la UAESP defina durante la ejecución del contrato, siempre que sean compatibles con los mecanismos de integración soportados oficialmente por el fabricante. Los componentes adicionales de FortiSIEM, tales como IOC Service, Advanced Agents (Log & FIM) u otros servicios complementarios, no hacen parte del presente ítem y serán evaluados de manera independiente en caso de requerirse dentro del presente estudio. Cuando una fuente de información no pueda integrarse por limitaciones técnicas del producto origen, ausencia de conectores oficiales, restricciones de licenciamiento o incompatibilidades documentadas por el fabricante, el contratista deberá entregar el respectivo concepto técnico debidamente soportado, proponiendo, cuando sea posible, mecanismos alternativos de integración soportados oficialmente.

Suministro e implementación del licenciamiento FortiSIEM Advanced Agents para ampliar las capacidades de recolección de información y monitoreo sobre los activos tecnológicos definidos por la UAESP.		
No.	**CANTIDAD**	**DESCRIPCION**
6	Cincuenta (50)	**Producto:** FortiSIEM Advanced Agents (Log Collection & File Integrity Monitoring - FIM). **Tipo de requerimiento**: Adquisición e implementación de licenciamiento complementario.

Suministro e implementación del licenciamiento FortiSIEM Advanced Agents para ampliar las capacidades de recolección de información y monitoreo sobre los activos tecnológicos definidos por la UAESP.		
No.	**CANTIDAD**	**DESCRIPCION**
		SKU de referencia: FC1-10-FSM98-182-02-12 (o el SKU vigente equivalente definido por el fabricante). **Descripción funcional**: El contratista deberá suministrar, instalar, configurar e integrar los agentes avanzados de FortiSIEM sobre los activos tecnológicos que defina la UAESP, con el fin de ampliar las capacidades de recolección de registros, monitoreo de integridad de archivos (File Integrity Monitoring - FIM) y demás funcionalidades soportadas oficialmente por el fabricante para la supervisión avanzada de equipos y servidores. **Características técnicas mínimas:** • Licenciamiento oficial FortiSIEM Advanced Agents. • Compatibilidad con la versión de FortiSIEM implementada en la entidad. • Recolección avanzada de registros mediante agentes instalados sobre los equipos monitoreados. • Capacidades de File Integrity Monitoring (FIM), conforme a las funcionalidades soportadas por el fabricante. • Administración centralizada de los agentes desde la consola FortiSIEM. • Integración nativa con la plataforma FortiSIEM. • Compatibilidad con los sistemas operativos soportados oficialmente por el fabricante. **Servicios incluidos:** • Suministro del licenciamiento correspondiente. • Instalación y configuración de los agentes sobre los activos definidos por la UAESP. • Los agentes deberán instalarse únicamente sobre los servidores, equipos o activos tecnológicos que sean priorizados conjuntamente entre el contratista y la supervisión del contrato, hasta completar la capacidad total del licenciamiento adquirido. • Parametrización inicial de las funcionalidades implementadas. • Integración con la plataforma FortiSIEM. • Validación funcional de los agentes instalados. • Elaboración y entrega de la documentación técnica de la implementación, incluyendo como mínimo la arquitectura de la solución, configuración realizada, parámetros aplicados, activos integrados, procedimientos de instalación, operación, administración, respaldo y recuperación, así como los resultados de las pruebas funcionales efectuadas. • Transferencia de conocimiento al personal técnico de la UAESP con una duración mínima de cuatro (4) horas, en modalidad presencial,

Suministro e implementación del licenciamiento FortiSIEM Advanced Agents para ampliar las capacidades de recolección de información y monitoreo sobre los activos tecnológicos definidos por la UAESP.		
No.	**CANTIDAD**	**DESCRIPCION**
		virtual o mixta, permitiendo su grabación. Deberá incluir material de apoyo, ejercicios prácticos y casos de uso relacionados con la instalación, administración, monitoreo, actualización y operación de los agentes implementados.

Servicio FortiCare Premium Support para la plataforma FortiSIEM.		
No.	**CANTIDAD**	**DESCRIPCION**
7	UN (1)	**Producto:** FortiCare Support for Software based FortiSIEM deployments 1 Year FortiCare Premium Support (1 - 200 points) for FortiSIEM Software deployments. **Tipo de requerimiento**: Servicio de soporte oficial del fabricante asociado a la plataforma FortiSIEM. **SKU de referencia:** FC3-10-FSM97-248-02-12, o la referencia equivalente que la sustituya oficialmente durante la vigencia del proceso de contratación. **Descripción funcional**: El contratista deberá suministrar el servicio oficial FortiCare Premium Support del fabricante para la plataforma FortiSIEM objeto del presente proceso, garantizando durante la vigencia contratada el acceso a los servicios de soporte técnico, asistencia especializada, actualizaciones y demás prestaciones asociadas al nivel de soporte adquirido para el despliegue FortiSIEM. **Cobertura del servicio:** El servicio deberá cubrir la plataforma FortiSIEM implementada por la UAESP y dimensionarse de acuerdo con el esquema de puntos definido por el fabricante y los componentes efectivamente licenciados dentro del presente proceso. **Características técnicas mínimas:** • Servicio FortiCare Premium Support oficial del fabricante para FortiSIEM. • Cobertura durante mínimo un (1) año o durante la vigencia definida para el licenciamiento contratado. • Capacidad de soporte correspondiente al dimensionamiento de la plataforma FortiSIEM adquirida. • Acceso a actualizaciones, correcciones y versiones de software disponibles conforme a las condiciones del fabricante. • Acceso a asistencia técnica oficial del fabricante y mecanismos de escalamiento de casos. • Acceso al portal de soporte, documentación técnica y demás recursos asociados al servicio contratado.

Servicio FortiCare Premium Support para la plataforma FortiSIEM.		
No.	**CANTIDAD**	**DESCRIPCION**
		Servicios incluidos: • Registro y activación del servicio FortiCare sobre la plataforma FortiSIEM de la UAESP. • Validación de la correcta asociación del soporte con el licenciamiento adquirido. • Acceso al soporte técnico oficial del fabricante durante la vigencia contratada. • Acceso a actualizaciones y correcciones de software conforme al nivel de soporte contratado. • Escalamiento de incidentes al fabricante cuando corresponda. Nota: Este componente corresponde al soporte oficial del fabricante para FortiSIEM y es independiente y complementario al servicio de soporte técnico especializado 7x24 prestado por el contratista. El soporte especializado del contratista será el mecanismo de atención técnica de la UAESP y deberá realizar, cuando corresponda, el diagnóstico y escalamiento de los casos hacia el soporte oficial del fabricante.

Suministro e implementación del servicio FortiSIEM IOC Service para el enriquecimiento de eventos de seguridad mediante inteligencia de amenazas e indicadores de compromiso (IOC).		
No.	**CANTIDAD**	DESCRIPCION
8	Una (1)	**Producto**: FortiSIEM IOC Service. **Tipo de requerimiento**: Adquisición e implementación de servicio complementario. **SKU de referencia:** FC2-10-FSM98-149-02-12 (o el SKU vigente equivalente definido por el fabricante). **Descripción funcional**: El contratista deberá suministrar, activar e integrar el servicio FortiSIEM IOC Service con la plataforma FortiSIEM implementada en la entidad, permitiendo enriquecer automáticamente los eventos de seguridad mediante indicadores de compromiso (IOC) e información de inteligencia de amenazas suministrada por el fabricante, con el propósito de fortalecer las capacidades de identificación, priorización y análisis de incidentes de ciberseguridad. **Características técnicas mínimas:** • Licenciamiento oficial del servicio FortiSIEM IOC Service.

Suministro e implementación del servicio FortiSIEM IOC Service para el enriquecimiento de eventos de seguridad mediante inteligencia de amenazas e indicadores de compromiso (IOC).		
No.	**CANTIDAD**	DESCRIPCION
		• Integración nativa con la plataforma FortiSIEM implementada en la UAESP. • Actualización automática y periódica de indicadores de compromiso (IOC) suministrados por el fabricante durante la vigencia del servicio. • Enriquecimiento automático de eventos e incidentes mediante información de inteligencia de amenazas. • Compatibilidad con la versión de FortiSIEM implementada y con futuras actualizaciones soportadas durante la vigencia del licenciamiento. Operación utilizando los mecanismos soportados oficialmente por el fabricante. **Servicios incluidos:** • Suministro del licenciamiento del servicio. • Activación del servicio. • Configuración e integración con FortiSIEM. • Parametrización inicial del enriquecimiento de eventos. • Validación funcional del servicio implementado. • Elaboración de la documentación técnica correspondiente. • Ejecución de pruebas funcionales con eventos de prueba. • Transferencia de conocimiento al personal técnico de la UAESP con una duración mínima de Seis (6) horas, en modalidad presencial, virtual o mixta, permitiendo su grabación. Deberá incluir material de apoyo, ejercicios prácticos y casos de uso relacionados con la administración del servicio, la interpretación de los indicadores de compromiso (IOC), el análisis de eventos enriquecidos y las mejores prácticas para su aprovechamiento dentro de la plataforma FortiSIEM. **Nota** El servicio deberá quedar completamente operativo, verificándose la recepción y actualización automática de los indicadores de compromiso (IOC) durante la vigencia del licenciamiento, de conformidad con las funcionalidades soportadas oficialmente por el fabricante. En ningún caso el contratista podrá sustituir este servicio mediante fuentes abiertas o herramientas de terceros que no hagan parte del licenciamiento oficial suministrado por Fortinet.

Servicio Fortinet SOCaaS (Security Operations Center as a Service) para el monitoreo administrado de la infraestructura FortiGate implementada en la UAESP.		
No.	**CANTIDAD**	**DESCRIPCION**
9	TRES (3)	**Producto**: Fortinet SOCaaS (Security Operations Center as a Service). **Tipo de requerimiento**: Servicio administrado de monitoreo de seguridad. **SKU de referencia :** FC-10-FG2HG-464-02-12 (FortiGate 200G) y FC-10-FG2VM-464-02-12 (FortiGate VM), o las referencias equivalentes que las sustituyan oficialmente durante la vigencia del proceso de contratación. **Descripción funcional:** El contratista deberá suministrar el servicio oficial Fortinet SOCaaS para la infraestructura FortiGate implementada por la UAESP, proporcionando monitoreo administrado de eventos de seguridad, análisis inicial de registros (logs), clasificación y priorización de incidentes (Incident Triage) y escalamiento oportuno hacia la Entidad y/o el fabricante cuando la naturaleza del evento así lo requiera, fortaleciendo las capacidades institucionales de identificación temprana y respuesta frente a incidentes de ciberseguridad. **Cobertura del servicio:** El servicio deberá cubrir la totalidad de la infraestructura FortiGate actualmente implementada por la UAESP, correspondiente a: • Dos (2) dispositivos FortiGate 200G implementados en Alta Disponibilidad (HA). • Un (1) FortiGate Virtual Machine (FortiGate VM) desplegado en Microsoft Azure. **Características técnicas mínimas:** • Servicio oficial Fortinet SOCaaS. • Monitoreo continuo de los eventos generados por los dispositivos FortiGate cubiertos por el servicio. • Recolección y análisis de registros de seguridad (Logs Monitoring). • Clasificación y priorización inicial de incidentes de seguridad (Incident Triage). • Escalamiento de incidentes al fabricante cuando corresponda (SOC Escalation Service). • Acceso a la información, reportes y resultados generados por el servicio. • Prestación del servicio durante toda la vigencia del licenciamiento contratado. **Servicios incluidos:** • Activación y habilitación del servicio SOCaaS.

		• Configuración inicial del servicio sobre la infraestructura FortiGate cubierta. • Validación de la correcta recepción de eventos y registros de seguridad. • Monitoreo administrado de logs durante toda la vigencia del servicio. • Clasificación inicial de incidentes de seguridad. • Escalamiento técnico conforme a los procedimientos definidos por el fabricante. • Acceso a reportes y evidencias generadas por el servicio. **Nota:** El presente componente corresponde a un servicio administrado de monitoreo proporcionado por el fabricante y complementa las capacidades de seguridad de la plataforma Fortinet actualmente implementada.

Prestación del servicio especializado de soporte técnico para la plataforma integral de ciberseguridad Fortinet de la UAESP.		
No.	**CANTIDAD**	**DESCRIPCION**
10	Uno (1)	**Producto**: Servicio especializado de soporte técnico para la plataforma Fortinet. **Tipo de requerimiento**: Servicio profesional especializado. **Descripción funcional**: El contratista deberá prestar el servicio especializado de soporte técnico para la plataforma institucional de ciberseguridad Fortinet implementada en la UAESP, conformada por los dispositivos FortiGate físicos en Alta Disponibilidad (HA), FortiGate VM implementado en Microsoft Azure, FortiAnalyzer, FortiSIEM y FortiEDR/FortiXDR, brindando atención especializada para la gestión de incidentes, diagnóstico y solución de fallas, análisis técnico, optimización de configuraciones existentes, ajustes de parametrización y/o configuraciones, acompañamiento técnico y gestión de escalamiento ante el fabricante cuando sea requerido, garantizando la continuidad operativa de la solución durante la vigencia del contrato. Características técnicas mínimas: • Servicio prestado por ingenieros certificados y con experiencia demostrable en tecnologías Fortinet. • Cobertura mínima de soporte 24 horas al día, 7 días a la semana (24x7) para incidentes críticos y de alta prioridad. • Atención remota y atención presencial en las instalaciones de la UAESP cuando la naturaleza del incidente así lo requiera. • Soporte especializado para FortiGate On-Premise, FortiGate VM Azure, FortiAnalyzer, FortiSIEM y FortiEDR/FortiXDR. • Diagnóstico técnico y análisis de causa raíz de incidentes relacionados con la plataforma.

Prestación del servicio especializado de soporte técnico para la plataforma integral de ciberseguridad Fortinet de la UAESP.		
		• Revisión y optimización de configuraciones existentes cuando sea requerido por la Entidad. • Ejecución de ajustes y/o configuraciones sobre políticas de seguridad, reglas de correlación, dashboards, reportes, alertas, integraciones, excepciones y demás parámetros funcionales de la solución, siempre que no excedan el alcance contractual. • Acompañamiento técnico durante actividades de mantenimiento preventivo, correctivo o actualización programadas por la UAESP. • Gestión, apertura, seguimiento y escalamiento de casos ante el TAC del fabricante cuando la atención del incidente así lo requiera. • Emisión de conceptos técnicos y recomendaciones orientadas al fortalecimiento y mejora continua de la plataforma. • Disponibilidad de herramienta para el registro, seguimiento y cierre de incidentes, garantizando la trazabilidad de las actuaciones realizadas. • Cumplimiento de los Acuerdos de Niveles de Servicio (ANS) establecidos por la UAESP. **Servicios incluidos:** • Recepción y gestión de incidentes mediante mesa de servicios. • Atención y solución de incidentes sobre cualquiera de los componentes de la plataforma Fortinet objeto del contrato. • Clasificación y priorización de incidentes conforme a buenas prácticas ITIL. • Diagnóstico técnico y análisis de causa raíz cuando aplique. • Validación funcional posterior a la implementación de las acciones correctivas realizadas. • Gestión integral de escalamiento y seguimiento de casos ante Fortinet hasta su cierre. • Elaboración de informes técnicos de las actividades ejecutadas cuando sean requeridos por la supervisión del contrato. • Reuniones periódicas de seguimiento técnico con la supervisión del contrato para revisar el estado de la plataforma, incidentes atendidos, cumplimiento de ANS y oportunidades de mejora. **Acuerdos mínimos de Niveles de Servicio (ANS):** • Prioridad P1 (Crítica): Tiempo máximo de respuesta de una (1) hora y tiempo objetivo de solución de cuatro (4) horas. • Prioridad P2 (Alta): Tiempo máximo de respuesta de dos (2) horas y tiempo objetivo de solución de ocho (8) horas. • Prioridad P3 (Media): Tiempo máximo de respuesta de tres (3) horas y tiempo objetivo de solución de dos (2) días hábiles.

Prestación del servicio especializado de soporte técnico para la plataforma integral de ciberseguridad Fortinet de la UAESP.		
		• Prioridad P4 (Baja): Tiempo máximo de respuesta de ocho (8) horas hábiles y tiempo objetivo de solución de cinco (5) días hábiles. • El contratista deberá mantener un cumplimiento mensual igual o superior al noventa y cinco por ciento (95 %) de los Acuerdos de Niveles de Servicio establecidos para los incidentes clasificados como P1, P2 y P3. Nota: El presente servicio corresponde a un servicio profesional especializado complementario al soporte oficial suministrado por Fortinet mediante los respectivos licenciamientos (FortiCare o el servicio equivalente vigente del fabricante). En consecuencia, este componente no sustituye ni reemplaza las obligaciones propias del fabricante relacionadas con actualizaciones de software, corrección de errores del producto, reemplazo de hardware, acceso al TAC o garantía del fabricante, sino que proporciona acompañamiento técnico especializado para la atención de incidentes y el soporte funcional de la plataforma integral de ciberseguridad. No forman parte del alcance de este servicio la administración permanente de la plataforma, la operación continua tipo SOC, el monitoreo permanente o cualquier actividad distinta al soporte especializado definido en el presente proceso contractual. **Aplicación, medición y seguimiento de los ANS** Los Acuerdos de Niveles de Servicio (ANS) establecidos en el presente Anexo Técnico serán aplicables a los incidentes y solicitudes de soporte que sean reportados al CONTRATISTA durante la ejecución del contrato. El tiempo de atención de cada incidente se contabilizará a partir de la fecha y hora en que el CONTRATISTA reciba formalmente el reporte por los canales de atención definidos para el servicio, y deberá quedar registrado en el sistema o mecanismo dispuesto para el seguimiento de los casos. Para efectos de la medición, se entenderá como **tiempo de respuesta** el período transcurrido entre la recepción del reporte del incidente y el primer contacto o acción efectiva del CONTRATISTA orientada a su diagnóstico y atención. El **tiempo de solución** corresponderá al período transcurrido entre la recepción del reporte y la solución o restablecimiento del servicio, de acuerdo con las condiciones establecidas para cada nivel de prioridad. Cada incidente deberá contar con los registros correspondientes que permitan verificar las fechas y horas de reporte, respuesta, atención, solución y cierre. La prioridad de los incidentes será determinada de acuerdo con su impacto y criticidad sobre los servicios tecnológicos de la Entidad,

Prestación del servicio especializado de soporte técnico para la plataforma integral de ciberseguridad Fortinet de la UAESP.		
		conforme a la clasificación P1, P2, P3 y P4 establecida en el presente Anexo Técnico. En caso de requerirse la modificación de la prioridad inicialmente asignada, esta deberá encontrarse debidamente justificada y registrada en el mecanismo de gestión de incidentes. El cumplimiento de los ANS se realizará de manera mensual, tomando como referencia la totalidad de los incidentes clasificados como P1, P2 y P3 que hayan sido atendidos y/o cerrados durante el período objeto de medición. El porcentaje de cumplimiento se determinará mediante la siguiente fórmula: **Porcentaje de cumplimiento ANS = (Número de incidentes atendidos dentro de los tiempos establecidos / Número total de incidentes objeto de medición) × 100.** El CONTRATISTA deberá alcanzar un cumplimiento mensual igual o superior al noventa y cinco por ciento (95 %) de los ANS establecidos para los incidentes P1, P2 y P3. Los resultados de la medición deberán ser presentados al supervisor del contrato, junto con los soportes que permitan verificar el cumplimiento de los tiempos establecidos. Cuando se evidencie un incumplimiento de los ANS, el supervisor del contrato podrá requerir al CONTRATISTA la presentación de las explicaciones y/o acciones correctivas correspondientes, sin perjuicio de las medidas contractuales a que haya lugar de conformidad con las condiciones establecidas en el contrato y la normativa aplicable. **NOTA:** Los eventos que se encuentren debidamente justificados y que sean atribuibles a causas no imputables al CONTRATISTA deberán quedar documentados y podrán ser excluidos de la medición, previa validación y aprobación del supervisor del contrato.

Fortalecimiento de las capacidades técnicas institucionales mediante capacitación oficial Fortinet y suministro de vouchers para certificación oficial.		
No.	**CANTIDAD**	**DESCRIPCION**
11	Una (1)	**Producto:** Capacitación especializada y fortalecimiento de capacidades técnicas institucionales, con suministro de vouchers para certificación. **Tipo de requerimiento:** Servicio especializado de capacitación y fortalecimiento de capacidades institucionales.

Fortalecimiento de las capacidades técnicas institucionales mediante capacitación oficial Fortinet y suministro de vouchers para certificación oficial.		
No.	**CANTIDAD**	**DESCRIPCION**

		Descripción funcional: El contratista deberá suministrar un programa de capacitación especializada orientado a fortalecer las competencias técnicas del personal designado por la UAESP para la administración, operación, monitoreo y mejores prácticas de la plataforma institucional de ciberseguridad basada en tecnologías Fortinet implementada durante la ejecución del contrato.
		
		El contratista deberá suministrar los vouchers oficiales, o el mecanismo equivalente definido por el fabricante, para la presentación del examen de certificación.
		
		Características técnicas mínimas.
		
		• El programa de capacitación deberá incluir, como mínimo, formación en:
		  ○ Administración y operación de FortiGate.
		  ○ Configuración y administración de políticas de seguridad.
		  ○ VPN y alta disponibilidad (HA).
		  ○ Funciones de conectividad.
		  ○ Mejores prácticas de seguridad.
		  ○ Filtrado web y control de aplicaciones
		  ○ Monitoreo y diagnóstico de la plataforma.
		  ○ Administración general de la solución implementada.
		• El contenido deberá corresponder a la versión vigente de los productos implementados o a la versión oficialmente soportada por el fabricante al momento de impartir la capacitación.
		• La capacitación deberá contar con una intensidad mínima de treinta y dos (32) horas, distribuidas en sesiones teóricas y/o prácticas, cuya programación y duración serán concertadas con la supervisión del contrato, de acuerdo con la metodología de formación propuesta y las necesidades operativas de la UAESP. Las sesiones no deberán superar las ocho (8) horas diarias.
		• El contratista deberá suministrar el material académico correspondiente a cada participante, en formato físico o digital, de acuerdo con la modalidad de capacitación acordada.
		• El contratista deberá suministrar cinco (5) vouchers oficiales de examen Fortinet, válidos para la presentación del examen de certificación asociado al nivel FortiOS Administrator / NSE 4, o su equivalente vigente dentro del programa de certificación del fabricante.
		• Los vouchers deberán contar con una vigencia mínima de doce (12) meses contados a partir de su entrega a la UAESP.
		• La capacitación podrá impartirse en modalidad presencial, virtual o mixta, siempre que garantice el cumplimiento de los objetivos de aprendizaje definidos para el programa.

Fortalecimiento de las capacidades técnicas institucionales mediante capacitación oficial Fortinet y suministro de vouchers para certificación oficial.		
No.	**CANTIDAD**	**DESCRIPCION**
		Servicios incluidos: • Gestión y coordinación de la capacitación. • Suministro del material oficial del fabricante. • Cronograma de capacitación establecido. • Capacitación para el personal designado por la UAESP para mínimo cinco (5) personas. • Entrega de certificado de asistencia. • Suministro de cinco (5) vouchers oficiales para examen de certificación nivel FortiOS Administrator / NSE 4, o su equivalente vigente dentro del programa de certificación del fabricante. • Orientación sobre el proceso de programación y presentación del examen oficial. **Nota:** La presente capacitación es un servicio independiente y complementario a las actividades de transferencia de conocimiento incluidas en los servicios de implementación de los demás componentes del contrato, por lo que no podrá entenderse sustituida por dichas actividades. El instructor deberá acreditar experiencia demostrable en la implementación, administración o soporte de soluciones Fortinet y contar con certificaciones técnicas vigentes o experiencia equivalente en las temáticas objeto de la capacitación

Firma:



Firma: JORGE ALEXIS RODRIGUEZ MEZA
Cargo: Jefe Oficina de Tecnologías de la Información y las Comunicaciones.
Dependencia Solicitante: Oficina TIC.

Elaboró: Eduardo Andrés Rozo Revelo – Profesional Universitario Oficina TIC
Elaboró: Osbaldo cortés Lozano – Profesional Universitario Oficina TIC
Elaboró: Carlos Andrés Cuartas – Profesional Universitario Oficina TIC

Revisó: Jorge Alexis Rodríguez Meza – Jefe Oficina TIC
Aprobó: Jorge Alexis Rodríguez Meza – Jefe Oficina TIC