1. OBJETO

Contratar los servicios de Centro de Operaciones de Seguridad, administración, protección, pruebas y gestión de incidentes de seguridad relacionadas con la plataforma tecnológica que soportan las actividades misionales y de Fiscalización de la ***Agencia Nacional de Minería (ANM)***. (Línea PAA No. 130005426 _613000126).

2. ALCANCE AL OBJETO

Para el cumplimiento del objeto contractual, el contratista deberá desarrollar, como mínimo, las siguientes actividades cuya descripción y detalle se relaciona en el presente anexo:

- Gestión y monitoreo de la Seguridad Informática sobre la plataforma tecnológica de la Agencia Nacional de Minería a través de un Centro de Operaciones de Seguridad (SOC) que incluya la gestión de eventos e Información de Seguridad (SIEM) y de cualquier equipo de seguridad administrado, así como la administración, mantenimiento, monitoreo, actualización, configuración, aseguramiento, fortalecimiento, operación continua y despliegue de equipos, plataformas de Seguridad y Protección contra Amenazas Avanzadas. **Ver Detalle de la plataforma en el anexo técnico.** literal **7.1 y 7.2. del presente documento**

- Implementación y configuración de colectores, supervisores para la implementación del servicio de correlación de eventos SIEM para el número de fuentes establecidas en el literal **7.1 del presente documento**

- Monitoreo de eventos en plataforma defender for office 365 y defender for office y defender End point, Microsoft Sentinel con las condiciones establecidas en el **literal 7.1 del presente documento.**

- Adquisición de Nuevos productos FORTIPAM y FORTISIEM, implementación, puesta en marcha, capacitación y soporte técnico por doce (12) meses **del literal 7.4 del presente documento.**

- Administración de la Plataforma PAM (FORTIPAM). Gestión para 20 usuarios. Según condiciones del **literal 7.3.** del presente documento.

- Gestión de incidentes conforme los eventos monitoreados por el SOC o los solicitados por el equipo de la ANM. (Ver acuerdos de niveles de servicio para incidentes)

- Realización de Pruebas de seguridad conforme el alcance **del literal 7.5 del** presente documento así: una prueba de vulnerabilidad con su respectivo Re-test a los seis (6) meses de ejecución del contrato, una prueba de Pentest para diez (10) portales públicos de la ANM. (es decir, diez (10) pruebas uno para cada portal).

- Renovación de licenciamiento de productos FORTINET.

- Renovación de licenciamiento de productos VICARIUS.

Informacion publica

NOTA GENERAL: El oferente debe contemplar en su propuesta la totalidad del hardware, software, accesorios, suscripciones y servicios requeridos para el cabal cumplimiento de cada uno de los ítems solicitados en el presente anexo técnico. La omisión de cualquier componente necesario para la correcta operación de la solución no eximirá al contratista de su obligación de suministrarlo sin costo adicional para la Entidad.

3. CUADRO DE CANTIDADES Y PLAZO DE EJECUCION

ITEM	COD UNSPSC	Descripción del Producto	ESPECIFICACIONES TÉCNICA	UNIDAD DE MEDIDA (Suscripción /Global)	CANTIDAD
1	**81111801**	Servicio de Centro de Operaciones de Seguridad (SOC).	Monitoreo Ciberseguridad Monitoreo Fotianalizer.300G y –200F, SIEM, WAF Antivirus alterno para servidores **Ver detalle literal 7.1 del Anexo de Especificaciones y Requerimientos Mínimos**	MES	12
2	**81111801**	Monitoreo de eventos en plataforma defender for office 365 y defender for end point.	Monitoreo Ciberseguridad m para la Plataforma Microsoft Windows Defender -365 Eventos para 1850 Buzones - 922 Equipos de Cómputo **Ver detalle literal 7.1 del Anexo de Especificaciones y Requerimientos Mínimos**	MES	12
3	**81111801**	Servicio de Administración Para la plataforma FORTIPAM (Gestión de Usuarios Privilegiados)	Administración de la plataforma Ver detalle de aplicación **Literal 7.3 del Anexo de Especificaciones y Requerimientos Mínimos**	MES	12

Informacion publica

4	**81111801**	Servicio de Pruebas de seguridad: Ingeniería social / vulnerabilidades y Re-test,/ Pruebas de Ethical Hacking .	• 1 prueba Vulnerabilidad: 100 Ips 1 Re tests a 100 Ips 1 Prueba ingeniería social – **Ver detalle 7.5 del Anexo de Especificaciones y Requerimientos Mínimos** 1 prueba de Ethical Hacking para 10 portales	UNIDAD	N/A
5	**81111801**	Servicios SAS de correlacionador de eventos SIEM	10 fuentes correlacionadas cada fuente con: 512 EPS Retención Filtrados 3 meses en línea 12 of line Plataformas Fortinet, **Literal 7.2 del Anexo de Especificaciones y Requerimientos Mínimos**	MES	2
6	43233200	Renovación licenciamientos y/o actualización de productos Fortinet : **Ver literal 7.7 del Anexo de Especificaciones y Requerimientos Mínimos**	- 2 NGFW Fortinet 1100E	MES	12
			- 2 FortiWeb 1000E	MES	12
			- 1 FortiAnalyzer 300G	MES	12
			VPN/ZTNA 1700 End Points	MES	12
7	43233200	Renovación de licenciamiento VRX VICARUIS	Renovación de licenciamiento y los servicios conexos la renovación de 150 licencias de VrX.	MES	12
8	43233200	Adquisición de Producto Fortinet	1 x FortiSIEM en VM para 50 dispositivos y 1000 EPS con soporte a 12 meses y servicio de implementación y puesta en marcha	UNIDAD	1
9	43233200	Adquisición de solución FORTIPAM	+ Renovación Soporte fabrica para 20 licencias de usuarios. Ver detalle de aplicación **Literal 7.4 del Anexo de Especificaciones y**	UNIDAD	1

Informacion publica

			Requerimientos Mínimos		

4. CLASIFICADOR UNSPSC

CÓDIGO	SEGMENTO	FAMILIA	CLASE
43231500	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software funcional específico de la empresa
43233200	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección
81111800	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas
81111801	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas
81112200	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de software

5. EQUIPO MINIMO DE TRABAJO REQUERIDO

Para la ejecución del proyecto el contratista deberá conformar un equipo de trabajo multidisciplinario, conformado como mínimo con los siguientes roles:

Rol	Responsabilidades	Disponibilidad	Cantidad
Coordinador del Proyecto	Como mínimo el rol deberá: • Realizar la coordinación para la prestación del servicio bajo óptimas condiciones como mínimo con los alcances expuestos para cada uno de ellos. • Atender las solitudes (PQRS) del personal de la ANM de carácter técnico o administrativo. • Coordinas las acciones de facturación. • Realizar la entrega y presentación de informes mensuales.	Tiempo parcial acorde con las necesidades del proyecto	1
Profesional senior redes y seguridad informática	Como mínimo el rol deberá: • Gestionar las solicitudes técnicas realizadas por la ANM	Tiempo Completo Inmediata una vez que realizada la	1

Informacion publica

	• Administrar y mantener los dispositivos de seguridad perimetral. • Administrar las plataformas de End point y PAM adquiridas por la ANM.	solicitud por parte de la ANM.- Disponibilidad 100% - Atención inmediata	
Analista de Ciberseguridad	Como mínimo el rol deberá: • Asesorar y acompañar a la ANM en la gestión de remediación de Vulnerabilidades	Tiempo parcial 40 horas	1
Equipo de Gestión de incidentes	Equipo multidisciplinario encargado de realizar el análisis de los eventos y gestionar correctamente los incidentes presentados por las diferentes fuentes correlacionadas o las solicitadas por el equipo de la ANM.	Tiempo Completo 7 X 24 de manera inmediata una vez que realizada la solicitud por parte de la ANM.	N/A

4.1. COORDINADOR DEL PROYECTO

La activación de los servicios propios del alcance del presente contrato deberá contar con un Coordinador de proyecto, que cumpla con el siguiente perfil definido:

ROL	**COORDINADOR DEL PROYECTO**	
FORMACIÓN ACADÉMICA	**PREGRADO**	Título profesional en cualquiera de las siguientes ingenierías: Sistemas, y/o Telemática, y/o Teleinformática, y/o Telecomunicaciones, y/o Electrónica, y/o Electrónica y Telecomunicaciones, y/o Mecatrónica, y/o de control, y/o en conectividad y redes, y/o en computación, y/o en informática, y/o de software, y/o en sistemas de información, y/o de diseño y automatización electrónica, y/o de automatización electrónica, y/o de diseño de automatización o computacional. También será válido el título profesional en disciplinas académicas pertenecientes a alguno de los siguientes Núcleos Básicos del Conocimiento (NBC), de conformidad con la clasificación establecida por el Ministerio de Educación Nacional y registrada en el Sistema Nacional de Información de la Educación Superior – SNIES: • Ingeniería de Sistemas, o Telemática o electrónica o telecomunicaciones

Informacion publica

	POSTGRADO	El Coordinador del Proyecto deberá acreditar título de posgrado (especialización, maestría o doctorado) en alguna de las siguientes áreas del conocimiento: • Seguridad Informática, Seguridad de la Información o Ciberseguridad, o • Gerencia o Gestión de Proyectos de Tecnología de la Información, o • Gestión de Riesgo Tecnológico o Continuidad de Negocio, o • Gerencia de proyectos en ingeniería También será válido el título de posgrado en disciplinas académicas pertenecientes a alguno de los siguientes Núcleos Básicos del Conocimiento (NBC), de conformidad con la clasificación establecida por el Ministerio de Educación Nacional y registrada en el Sistema Nacional de Información de la Educación Superior – SNIES: • Ingeniería de Sistemas, o Telemática, o Electrónica o Telecomunicaciones. Nota: El requisito de posgrado podrá ser homologado por dos (2) años adicionales de experiencia específica en dirección de proyectos de seguridad de la información, y viceversa.
	CERTIFICACIONES	Acreditar como requisito al menos una (1) de las siguientes certificaciones vigentes: - -Certified Information Systems Security Professional (CISSP) de ISC2 - Certified Ethical Hacker CEH mínimo en versión 6 de EC- Council - Certified Computer Hacking Forensic Investigator (CHFI) - EC-Council Certified Security analyst - Certified Information Security Manager de ISACA - Certified in Risk and Information Systems Control (CRISC) de ISACA - Certified Penetration Testing Engineer (CPTE). - Certified Information Systems Auditor de ISACA. - Certification LPT (Licensed Penetration Tester) de EC- Council - ISO 27001:2022 Auditor Lider - Certified Information Security Manager (CISM) - Master Business Continuity Planner (MBCP) - Certified Business Continuity Professional (CBCP) - Associate Business Continuity Professional (ABCP) - Certificación posea certificaciones como Scrum Master o Project Management Professional (PMP), owner, CAPM, PRINCE2,

Informacion publica

		- CompTIA Security+, - GIAC Security Essentials (GSEC) - Lead Manager NIST Cybersecurity Framework.
EXPERIENCIA	**GENERAL**	Experiencia mínima de 5 años en gerencia o supervisión de proyectos relacionados con seguridad de la Información o seguridad informática.
	ESPECIFICA	Acreditar en los último 5 años de experiencia dirigiendo o coordinando proyectos de Seguridad de la información. Esto se podrán acreditar a través de certificaciones en donde se evidencie la ejecución de obligaciones y/o actividades en dirección, coordinación, liderazgo técnico o gerencia de proyectos de ciberseguridad, seguridad de la información o riesgo tecnológico.
CANTIDAD MÌNIMA DE PERSONAS		UNA (1) TIEMPO PARCIAL ACORDE CON LAS NECESIDADES DEL PROYECTO

4.2. Profesional senior redes y seguridad informática

ROL	**PROFESIONAL SENIOR -PERFIL 1**	
FORMACIÓN ACADÉMICA	**PREGRADO**	Título profesional en cualquiera de las siguientes ingenierías: Sistemas, y/o Telemática, y/o Teleinformática, y/o Telecomunicaciones, y/o Electrónica, y/o Electrónica y Telecomunicaciones y/o Mecatrónica, y/o de control, y/o en conectividad y redes, y/o en computación, y/o en informática, y/o de software, y/o en sistemas de información, y/o de diseño y automatización electrónica, y/o de automatización electrónica, y/o de diseño de automatización y/o computacional. También será válido el título profesional en disciplinas académicas pertenecientes a alguno de los siguientes Núcleos Básicos del Conocimiento (NBC), de conformidad con la clasificación establecida por el Ministerio de Educación Nacional y registrada en el Sistema Nacional de Información de la Educación Superior – SNIES: Ingeniería de Sistemas, o Telemática o ciberseguridad o electrónica o telecomunicaciones ●
	CERTIFICACIONES	Acreditar como requisito al menos dos (2) de las siguientes certificaciones vigentes:- Certified Information Systems Security Professional (CISSP) de ISC2 - Certified Ethical Hacker CEH mínimo en versión 6 de EC-Council Certified Computer Hacking Forensic Investigator (CHFI) - EC-Council Certified Security analyst - Certified Information Security Manager de ISACA - Certified in Risk and Information Systems Control (CRISC)

Informacion publica

		de ISACA Certified Penetration Testing Engineer (CPTE). Certified Information Systems Auditor de ISACA. - Certification LPT (Licensed Penetration Tester) de EC-Council Certified Information Security Manager (CISM) Master Business Continuity Planner (MBCP) Certified Business Continuity Professional (CBCP) Associate Business Continuity Professional (ABCP) - Certificación BS2599-2 Fortinet NSE 4 o equivalentes a la administración de dispositivos FORTINET FIREWALL, WAF, ANALIZER y ZTNA. La acreditación en el ecosistema Fortinet abarca las certificaciones actuales equivalentes: Fortinet Certified Associate (FCA), Professional (FCP) o Expert (FCX) / NSE 4 o superior.
EXPERIENCIA	**GENERAL**	Experiencia mínima de 5 años en seguridad de la Información o seguridad informática.
	ESPECIFICA	Debe acreditar experiencia de al menos 5 años en administración de productos FORTINET – WAF – ANALIZER – FORTIGATE., ZTNA
CANTIDAD MÌNIMA DE PERSONAS		UNA (1) con ASIGNACION DE TIEMPO 5 X 8 LUNES A VIERNES TIPO REMOTO con disponibilidad de desplazamiento a la Sede Central de la ANM en Bogotá bajo requerimiento de la supervisión

4.3. Analista de Ciberseguridad

ROL	**ANALISTA DE CIBERSEGURIDAD**	
FORMACION ACADÉMICA	**PREGRADO**	Título profesional en cualquiera de las siguientes ingenierías: Sistemas, y/o Telemática, y/o Teleinformática, y/o Telecomunicaciones, y/o Electrónica, y/o Electrónica y Telecomunicaciones, y/o Mecatrónica, y/o de control, y/o en conectividad y redes, y/o en computación, y/o en informática, y/o de software, y/o en sistemas de información, y/o de diseño y automatización electrónica, y/o de automatización electrónica, y/o de diseño de automatización o computacional. También será válido el título de profesional en disciplinas académicas pertenecientes a alguno de los siguientes Núcleos Básicos del Conocimiento (NBC), de conformidad con la clasificación establecida por el Ministerio de Educación Nacional y registrada en el Sistema Nacional de Información de la Educación Superior – SNIES: • Ingeniería de Sistemas, o Telemática, o Electrónica o Telecomunicaciones.
	POSGRADO	Estudios de posgrado cuyo título se relacione con:

Informacion publica

		Seguridad Informática, y/o seguridad de la información, y/o seguridad en redes telemáticas, y/o seguridad digital, y/o ciberseguridad y/o ciberdefensa, y/o riesgos informáticos y/o auditoria de sistemas. También será válido el título de posgrado en disciplinas académicas pertenecientes a alguno de los siguientes Núcleos Básicos del Conocimiento (NBC), de conformidad con la clasificación establecida por el Ministerio de Educación Nacional y registrada en el Sistema Nacional de Información de la Educación Superior – SNIES: • Ingeniería de Sistemas, o Telemática, o ciberseguridad, auditoria, o riesgo tecnológico o Electrónica o Telecomunicaciones. Nota: El título de posgrado podrá ser homologado por dos (2) años de experiencia profesional adicional, debidamente certificada, en actividades específicas de seguridad informática, y/o ciberseguridad, y/o gestión de vulnerabilidades y/o respuesta a incidentes.
	CERTIFICACIONES	Acreditar como requisito al menos Tres (3) de las siguientes certificaciones vigentes: - Certified Information Systems Security Professional (CISSP) de ISC2 - Certified Ethical Hacker CEH mínimo en versión 6 de EC-Council Certified Computer Hacking Forensic Investigator (CHFI) - EC-Council Certified Security analyst - Certified Information Security Manager de ISACA - Certified in Risk and Information Systems Control (CRISC) de ISACA Certified Penetration Testing Engineer (CPTE). Certified Information Systems Auditor de ISACA. - Certification LPT (Licensed Penetration Tester) de EC-Council - ISO 27001 Líder Auditor Certified Information Security Manager (CISM) Master Business Continuity Planner (MBCP) Certified Business Continuity Professional (CBCP) Associate Business Continuity Professional (ABCP) - Auditor interno ISO 22301 - Certificación BS2599-2 . -Fortinet NSE 4 o superior
EXPERIENCIA	**ESPECIFICA**	Experiencia mínima de 5 años en seguridad de la Información o seguridad informática.
CANTIDAD MINIMA DE PERSONAS		UNA (1) X 40 HORAS DURANTE EL PERIODO (Bolsa de horas asignadas bajo demanda por la supervisión)

5. REQUERIMIENTOS GENERALES DE LA EJECUCIÓN DEL CONTRATO

1. Todos los documentos generados durante la ejecución del contrato deberán ser entregados en algún formato legible por Microsoft Office Word, Excel y PowerPoint 2019 o superiores.

Informacion publica

2. Las implementaciones deberán ser planeadas a través de cronogramas que deberán ser entregados oportunamente en formato de Microsoft Project 2019, o superiores.

3. Todo el material (documentos, audios, tablas, videos, etc.) generado durante la ejecución debe ser entregado a la ANM, señalando claramente los nombres de los autores y la transferencia de los derechos patrimoniales sobre los mismos a la ANM. El contratista puede conservar una copia de resguardo documental para efectos de archivo, auditoría e informes de cumplimiento hasta por 12 meses adicionales culminada la ejecución del contrato. Sobre el software de terceros (Fortinet, Vicarius, etc.) solo se ceden licencias de uso/suscripciones por 12 meses, reservándose la transferencia de derechos patrimoniales a la ANM de manera exclusiva sobre entregables documentales, guías de hardening, tableros BI y reglas de correlación personalizadas.

4. El contratista, en su calidad de receptor de información en virtud del contrato, deberá adoptar e implementar las medidas técnicas, administrativas y organizativas necesarias para proteger la información que le sea suministrada por la ANM, garantizando en todo momento su confidencialidad, integridad y disponibilidad, y evitando su pérdida, alteración, acceso no autorizado o divulgación indebida. Lo anterior, de conformidad con la normativa vigente, las políticas de seguridad de la información de la Entidad y los lineamientos del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

   Así mismo, el contratista deberá suscribir el acuerdo de confidencialidad adoptado por la ANM y velar por su estricto cumplimiento durante la ejecución del contrato y con posterioridad a su terminación, respecto de toda la información a la que tenga acceso.

5. Mensualmente se debe presentar a la entidad, en formato digital, un informe detallado por cada uno de los servicios prestados además de un informe general que incluya el avance en la ejecución de las actividades, el cual contenga como mínimo lo siguiente: Nombre del Contratista, número de contrato por cada uno de los servicios contratados, descripción de actividades adelantadas, estado de atención de los casos reportados al SOC, relación de documentación de la ANM utilizada, documentación generada durante el período de ejecución a reportar y demás temas asociados a la ejecución según el cronograma acordado.

6. Mensualmente el proveedor debe realizar una presentación del informe entregado de la ejecución del contrato a la fecha, de forma presencial en las instalaciones de la ANM o por videoconferencia con coordinación previa. La fecha para la realización de esta socialización se informará a través del supervisor con por lo menos cinco días hábiles de antelación.

7. El proponente y su personal, excepto previo consentimiento por escrito del Contratante, no podrán revelar en ningún momento a cualquier persona o entidad ninguna información confidencial adquirida en el curso de la prestación de los servicios; ni el proveedor ni su personal podrán publicar o dar a conocer las recomendaciones formuladas en el curso de, o como resultado de la prestación de los servicios.

8. La propiedad de los resultados, informes y documentos que surjan del desarrollo del contrato es exclusiva de la ANM, quien podrá utilizarlos indefinidamente, difundirlos y divulgarlos cuando lo estime necesario, sin contraprestación alguna a favor del proveedor. No obstante, las obras proseguibles por derecho de autor, los objetos, procedimientos o diseños técnicos que sean creados por las partes en cumplimiento del objeto del contrato, tendrán el reconocimiento de los derechos morales a favor del autor-creador de acuerdo con las disposiciones legales.

Informacion publica

9. La Entidad para efectos de establecer los derechos patrimoniales de autor, dará aplicación a lo establecido en el artículo 20 de la Ley 23 de 1982, modificado por el artículo 28 de la Ley 1450 de 2011 en concordancia con el artículo 10 de la Decisión Andina 351 de 1993, en el sentido de que el PROVEEDOR es el titular originario de los derechos morales en desarrollo y ejecución del presente contrato, los cuales le serán plenamente reconocidos. En relación con los derechos patrimoniales sobre los productos del contrato, estos pertenecerán a la Agencia Nacional de Minería. La difusión de los resultados, informes y documentos que surjan del desarrollo del presente contrato, en todo caso, deberá ser autorizada por la ANM.

10. El contratista para atender los requerimientos del presente documento debe contar con escalabilidad vigente, durante y hasta la finalización del contrato.

11. El contratista deberá de manera proactiva, monitorear y detectar el uso y/o consumo elevado de CPU, Memoria y demás elementos que afecten el correcto performance de los equipos de seguridad perimetral.

12. El contratista deberá realizar de manera semestral un análisis de riesgo sobre los equipos perimetrales administrados y ser presentado junto con el informe mensual del periodo correspondiente

6. ESPECIFICACIONES TÉCNICAS GENERALES REQUERIDAS

El proponente se compromete con la Entidad a:

1. Presentar al inicio de ejecución del contrato, un plan de trabajo detallado para la instalación y configuración de la solución ofertada, así como los demás servicios contratados.

2. Realizar un diagnóstico preliminar del estado de la seguridad de la información y la seguridad informática de la Agencia Nacional de Minería, que contemple la identificación y evaluación de riesgos, vulnerabilidades y brechas, así como la definición de recomendaciones técnicas y un plan de acción priorizado orientado a su mitigación y fortalecimiento. El documento que contenga dicho diagnóstico y sus resultados deberá ser elaborado y entregado a la Entidad dentro del mismo primer (1) mes de ejecución contractual, para su revisión y aprobación por parte de la supervisión.

3. Adelantar las actividades necesarias para el empalme con el personal de la ANM y el posterior ajuste instalación, configuración e implementación de la solución de seguridad ofertada, garantizando su continuo monitoreo y estableciendo los canales de comunicación segura requeridos con la ANM.

4. Realizar la gestión del cambio requerido sobre la plataforma tecnológica de la ANM, administrar las configuraciones, cambios y actualizaciones requeridas para la protección ante intrusos y entregar un informe mensual sobre las acciones preventivas implementadas en pro del fortalecimiento de todo lo que comprende como seguridad perimetral, seguridad en Cloud y accesos de confianza cero de la ANM.

5. Realizar el monitoreo permanente (7x24x365) de los servicios tecnológicos prestados por la ANM desde su centro de operaciones de seguridad SOC, realizar la gestión de incidentes de seguridad, la emisión de alertas sobre posibles ataques identificados y la correlación de eventos de seguridad a través del servicio SIEM, con el fin de evitar posibles incidentes, los cuales deberán ser relacionados en el informe mensual suministrado a la ANM durante la ejecución del contrato.

Informacion publica

6. Realizar un (1) análisis de vulnerabilidades según condiciones establecidas en **el Literal 7.5.** relacionado sobre la plataforma tecnológica de la ANM y generar un informe basado en un análisis de riesgos CISA y agregado por activo de las vulnerabilidades identificadas y las recomendaciones sugeridas para subsanarlas.
7. Todos los ítems ofrecidos en la propuesta económica podrán estar sujetos a verificación a través de por lo menos una visita antes o durante la operación del servicio de Monitoreo, correlación y atención de incidentes contratados. Dichas visitas serán previamente coordinadas con el proveedor.
8. La solución para implementar deberá quedar completamente empalmada, configurada y en funcionamiento en un tiempo no mayor a 30 días calendario, contados a partir de la fecha de suscripción del acta de inicio, incluyendo los equipos adquiridos si así aplica; sin embargo, se podrán activar progresivamente los servicios ofrecidos, una vez se finalice cada implementación y podrán ser facturados de manera fraccionada, correspondiente al servicio prestado en el mes, esto previo autorización previa de la supervisión.
9. El proponente deberá tomar las acciones requeridas para que la activación de los servicios objetos del presente contrato, no alteren en horario hábil la disponibilidad de los servicios tecnológicos disponibles en la ANM.
10. El proponente deberá cumplir con la experiencia y perfil requeridos para el equipo de trabajo, durante la ejecución del contrato.

7. REQUERIMIENTOS TÉCNICOS ESPECÍFICOS

No	ITEM	Descripción
7.1	Centro de Operaciones de Seguridad (SOC).	Realizar gestión, administración y monitoreo de la Seguridad Informática sobre la plataforma tecnológica de la Agencia Nacional de Minería a través de un Centro de Operaciones de Seguridad (SOC) propio, con la Gestión de Eventos e Información de Seguridad (SIEM) con 10 fuentes y todos los equipos de seguridad de la ANM del alcance del presente contrato 7X24X365 sin Interrupciones. El monitoreo no se limita exclusivamente al SIEM, también debe monitorear todos los eventos de los 2 dispositivos Fortianalizer y/o cualquiera de los dispositivos de seguridad objeto de la presente contratación de la infraestructura de la agencia. **Nota:** La Agencia Nacional de Minería – ANM estima, en el marco de la presente contratación, la adquisición de una solución SIEM en modalidad virtualizada, incluyendo el respectivo licenciamiento con capacidad para cincuenta (50) dispositivos y mil (1000) EPS, así como indicadores de compromiso (IOC) y soporte por doce (12) meses, contados a partir de su implementación y

Informacion publica

		puesta en marcha, como extensión de la plataforma Fortinet actualmente implementada en la entidad. En consecuencia, el servicio de SOC ofertado deberá contemplar el monitoreo, administración, correlación y gestión de eventos de seguridad asociados a dicha solución SIEM, incluyendo su integración dentro de la operación del servicio de monitoreo y gestión de seguridad de la información de la ANM.
	LITERAL B. Monitoreo de eventos en plataforma Defender for Endpoint y Antivirus Alterno para 300 Servidores.	El proveedor debe a través de los servicios del SOC realizar el monitoreo de eventos de la plataforma Microsoft Defender y generar las alertas necesarias e incidentes a los administradores de las plataformas de la ANM. El proveedor debe implementar herramientas automatizadas o procedimentales para realizar un seguimiento y monitoreo efectivo generando los respectivos informes. El proveedor podrá incluir estas fuentes en el SIEM, o realizar la implementación y monitoreo a través de herramientas propias.
7.2.	SOFTWARE COMO SERVICIO: correlacionador de eventos SIEM	**El proveedor debe configurar** La Agencia Nacional de Minería – ANM estima, en el marco de la presente contratación, la adquisición de una solución SIEM en modalidad virtualizada, incluyendo el respectivo licenciamiento con capacidad para cincuenta (50) dispositivos y mil (1000) EPS, así como indicadores de compromiso (IOC) y soporte por doce (12) meses, contados a partir de su implementación y puesta en marcha, como extensión de la plataforma Fortinet actualmente implementada en la entidad. En consecuencia, el servicio de SOC ofertado deberá contemplar la implementación de este producto en modalidad de SOFTWARE COMO SERVICIO (SAAS) durante el periodo de implementación del servicio SIEM de propiedad de la ANM (2 MESES). El oferente debe realizar la configuración de los, colectores y cualquier configuración para la prestación de monitoreo, administración, correlación y gestión de eventos de seguridad

Informacion publica

		asociados a dicha solución SIEM, incluyendo su integración dentro de la operación del servicio de monitoreo y gestión de seguridad de la información de la ANM cuyas características se encuentran establecidas en el numeral 7.2.del presente documento.
7.3	Gestión Plataforma FORTIPAM - Plataforma de acceso de Usuarios Privilegiados.	Servicios para la administración y el monitoreo de sesiones de trabajo de usuarios administradores de los servicios tecnológicos de la ANM, haciendo uso de la plataforma FORTIPAM
7.4	Adquisición de la plataforma FORTIPAM para 20 Usuarios	Adquisición, implementación, puesta en marcha, trasmisión de conocimiento o capacitación y soporte por 12 meses para la solución de acceso privilegiado FORTIPAM.
7.5	Pruebas técnicas en Seguridad de la Información.	Se debe realizar durante la vigencia una prueba de vulnerabilidades para 100 IP internas de la red de la ANM, Posteriormente ejecutar a los 6 meses o según disponga la ANM el Re-Test, Se debe ejecutar pruebas de Pen Test o Ethical Hacking para 10 portales públicos de la ANM, se debe ejecutar una prueba de ingeniería social para 1750 usuarios de la ANM incluyendo un estudio de fuentes abiertas OSINT.
7.6.	Renovación de licenciamiento VRX VICARUIS	Renovación de licenciamiento y los servicios conexos la renovación de 150 licencias de VrX. por 12 meses
7.7	Renovación licenciamientos y/o actualización de productos Fortinet: Ver literal 7.7	- 2 NGFW Fortinet 1100E - 2 FortiWeb 1000E - 1 FortiAnalyzer 300G -VPN/ZTNA 1700 End Points
7.8	Adquisición de Producto Fortinet	1 x FortiSIEM en VM para 50 dispositivos y 1000 EPS con soporte a 12 meses

7.1. CENTRO DE OPERACIONES DE SEGURIDAD (SOC-Security Operation Center)

La ANM requiere de un servicio de SOC, que debe estar ubicado en las instalaciones del proveedor, a través del cual se realiza el respectivo monitoreo del correlacionador de eventos SIEM y de los equipos de seguridad administrados, se debe atender los incidentes de seguridad ocurridos en la plataforma tecnológica de la ANM y de los servicios externos en modalidad CLOUD.

El SOC debe monitorear los eventos de seguridad de la plataforma 365 a través de los componentes proporcionados por Microsoft 365 tales como Defender for office, Defender for End Point, Intune, Microsoft Sentinel, entre otras, por ende, debe hacer las configuraciones necesarias para realizar el monitoreo de estos componentes de manera automatizada.

Nota 1: Durante la vigencia del contrato que se llegue a suscribir la ANM puede adquirir infraestructura que remplace, complemente o mejore los servicios que presta la actual infraestructura, que también debe ser

Informacion publica

incorporada. También debe contemplarse dentro de lo requerido por la ANM aquellos servicios que se encuentran alojados en la infraestructura de Data Center contratado con terceros, servicios en cloud tales como Microsoft 365, Azure, entre otros en modelos AaS (As a Service) y que se integran con la infraestructura de TI de la Agencia.

Nota 2: Se Aclara que La ANM a la fecha no tiene el servicio implementado de Microsoft Sentinel, se estima que la ANM implemente esta plataforma durante la vigencia en curso, no obstante se reserva el derecho de hacer su implementación. En caso de que sea implementado La ANM cubrirá los costos de licenciamiento e ingesta de Microsoft Azure/Sentinel. El contratista se encargará de realizar el tuning de reglas y el monitoreo de incidentes desde su SOC una vez la Entidad ponga en producción dicha plataforma.

No.	DESCRIPCIÓN	CUMPLIMIENTO
	FUNCIONALIDADES Y CAPACIDADES GENERALES	(Favor Diligenciar) **SI / NO**
7.1.1.	El servicio del SOC deberá contar con mínimo dos (2) centros de datos ubicados geográficamente en diferentes ciudades en Colombia o el secundario en el exterior, pero su centro de operaciones principal debe encontrase en la ciudad de Bogotá. El centro de datos ubicado en el exterior se aceptará siempre y cuando este ubicado en uno de los países autorizados por la Superintendencia de Industria y Comercio para el tratamiento y transferencia de datos personales. El oferente debe dar sustento a un plan documentado de continuidad de servicios de seguridad del SOC. La plataforma de Monitoreo SOC puede ser CLOUD. Manteniendo los criterios técnicos mencionados	
7.1.2.	El centro de datos donde se encuentra alojado físicamente el SOC debe contar con mínimo certificación TIER III del Uptime Institute o ICREA Nivel IV. (La certificación TIER III o ICREA Nivel IV se exigirá exclusivamente para la infraestructura del Data Center (Principal y/o Secundario) que aloja los servidores centrales, el almacenamiento y el core de procesamiento del SOC/SIEM, y no para la sede u oficinas administrativas de trabajo de los analistas)	
7.1.3.	El servicio debe ser prestado en la modalidad 7x24X365. (Siete días a la semana veinticuatro horas al día), incluye días festivos, y fines de semana, es decir sin interrupción alguna, durante la vigencia contractual.	
7.1.4.	El servicio debe ser prestado en idioma español, que facilite la interacción de las áreas de operación con el personal de la Agencia.	
7.1.5.	El servicio debe incluir Threat Intelligence o Inteligencia Global, que permita usar un servicio mundial de amenazas identificadas.	
7.1.6.	El SOC debe contar con soluciones de revisión de Logs automatizados para monitorear eventos en fuentes que no puedan ser correlacionadas directamente a través de las plataformas establecidas por el SOC o por el SIEM.	

Informacion publica

7.1.7. 2	El SOC debe estar acreditado como **MSSP (Managed Security Service Provider) por el fabricante FORTINET**, correspondiente a la plataforma **FortiSIEM** requerida para la prestación del servicio y en alineación con la homogeneidad tecnológica de la Entidad. Adicionalmente, el proponente deberá contar con **reporte SOC 2 (Tipo II) vigente, reporte SOC 3 vigente**, o **acreditación del marco de madurez SOMM (Security Operations Maturity Model.**	
7.1.8.	El SOC debe ser parte de los foros de respuesta a incidentes, así como del CSIRT al menos desde hace un (1) año al momento de presentación de la oferta.	
7.1.9.	Se deben prestar los servicios técnicos necesarios para el inicio de la prestación de los servicios. La ANM se encargará de garantizar la interconexión y configuraciones necesarias para garantizar que el proveedor tenga acceso desde sus instalaciones a la información, tales como logs, entre otros, que se requieren para la prestación de los servicios.	
	SEGURIDAD DE LA INFORMACIÓN	
7.1.10.	Para la prestación del servicio el proveedor debe contar con herramientas y métodos para controlar la fuga de información desde el SOC, tales como herramientas DLP (Prevención de Pérdida de Datos), monitoreo de correo electrónico, bloqueo de puertos USB, etc, para disminuir la probabilidad de fuga de información de ANM a la que tenga acceso con ocasión de la prestación del servicio.	
7.1.11.	Para la prestación del servicio el proveedor debe contar con procesos o procedimientos formales debidamente documentados para dar de baja la información de la ANM (eliminación segura) ya sea por solicitud de la Entidad (si así se solicita) y una vez finalice la prestación de los servicios de tal forma que se garantice la correcta disposición de la información de la entidad. Los documentos podrán ser solicitados por la supervisión del contrato en la ANM, en cualquier momento durante la ejecución y se podrá solicitar soportes que evidencien las actividades y herramientas utilizadas TITULARIDAD Y REVERSIÓN DE REGISTROS (LOGS): Los registros históricos de eventos (logs) generados o procesados con ocasión de la prestación del servicio, así como la información contenida en el SIEM propio adquirido para la ANM, son de propiedad exclusiva de la Agencia Nacional de Minería, independientemente de que durante la fase de transición el monitoreo se preste sobre el SIEM del proveedor bajo la modalidad SaaS. El contratista deberá mantener disponibles los logs por un período mínimo de retención en línea de tres (3) meses y garantizar mecanismos de exportación en formato abierto y no propietario. A la terminación o liquidación del contrato, por cualquier causa, el contratista deberá hacer entrega formal a la ANM de la totalidad de los registros, configuraciones, reglas de correlación y evidencias generadas durante la ejecución, dentro de los diez (10) días hábiles siguientes a la finalización del servicio, de forma previa a cualquier	

Informacion publica

	eliminación o disposición de dicha información conforme al procedimiento de eliminación segura descrito en el presente numeral.	
7.1.12.	El proveedor debe contar con procesos o procedimientos formales debidamente documentados y acciones que garanticen el control de la información sobre cualquier equipo portátil que salga de las instalaciones del SOC.	
	CONFIGURACION Y ADMINISTRACION CORRELACIONADOR DE EVENTOS (SIEM)	
7.1.13.	La Agencia Nacional de Minería – ANM actualmente cuenta con un servicio SIEM bajo la modalidad de Software como Servicio (SaaS). No obstante, mediante la presente contratación, la entidad tiene como propósito adquirir e implementar una solución SIEM propia dentro de su infraestructura tecnológica, compuesta por una (1) instancia SIEM virtualizada con capacidad para cincuenta (50) dispositivos, mil (1000) EPS, indicadores de compromiso (IOC) y soporte de fabricante. En consecuencia, el servicio de monitoreo SOC objeto de la presente contratación deberá contemplar la configuración, administración, operación y monitoreo continuo de dicha solución SIEM propiedad de la ANM, manteniendo el alcance y las condiciones operativas requeridas para la gestión de eventos e incidentes de seguridad de la información.	
7.1.14.	El servicio de monitoreo debe incluir la capacidad de detección de anomalías en el comportamiento de las aplicaciones, equipos y usuarios de la plataforma.	
7.1.15.	El servicio de SOC debe incluir la generación de indicadores de cumplimiento para los activos monitoreados,	
7.1.16.	El monitoreo debe realizar la detección de uso de eventos o accesos a la plataforma que no concuerden con el patrón histórico de uso o acceso.	
7.1.17.	Se deben Identificar, reportar y controlar al menos los siguientes eventos de seguridad, mínimos para monitorear: - Accesos no autorizados - Denegación de servicio. - Explotación de vulnerabilidades. - Fuerza bruta/login. - Escaneo de puertos. - Principales orígenes de ataque. - Principales destinos de ataque. a. Ubicación geográfica del ataque.	

Informacion publica

	b. Orígenes/destinos reportados por fuentes de inteligencia de seguridad. c. Acceso por parte de los usuarios a dominios diferentes a los autorizados. d. Cambios sobre Plataformas (software instalado, desinstalado, cambio de políticas del directorio activo) e. Conexiones (accesos remotos, intentos de conexión) f. Eliminación de logs h. Actividades de cuentas de altos privilegios i. Usuarios (bloqueados, agregados, eliminados, desbloqueados, cambio de contraseñas)	
7.1.18.	El proveedor debe realizar el diseño y modelamiento de servicio de monitoreo específico para ANM	
7.1.19.	Se debe realizar las configuraciones necesarias para monitorear la plataforma Defender for Office y Defender for End point, Intune, Ms Sentinel correspondiente a la plataforma de administración de end point o aquella adquirida por la ANM para tal fin y atender los casos (requerimientos e incidentes) que se generen a través de la Oficina de Tecnología e Información de la ANM, para lo cual la Entidad brindará los accesos y asignará los correspondientes perfiles.	
7.1.20.	El servicio de monitoreo debe estar en la capacidad de comprobar la integridad de los eventos correlacionados.	
7.1.21.	El equipo de monitoreo debe estar en capacidad de realizar análisis de la solución de recolección y correlación (SIEM) debe permitir identificar patrones anómalos de comportamiento por usuario y/o IP.	
7.1.22.	El equipo de monitoreo deberá verificar constantemente el estado de la conexión con el correlacionado a través de un mecanismo eficaz que, ante la eventual pérdida de la conexión entre el componente de recolección y el motor de correlación, genere de manera inmediata la notificación,	
7.1.23.	Al inicio de la ejecución del contrato, el proveedor deberá prestar el servicio de monitoreo SOC sobre la solución SIEM actualmente operada bajo la modalidad de Software como Servicio (SaaS), garantizando la continuidad del monitoreo y la gestión de eventos de seguridad de la información de la ANM. Una vez se implemente y ponga en funcionamiento la solución SIEM propia dentro de su infraestructura tecnológica, el proveedor deberá realizar las configuraciones, integraciones y actividades de migración necesarias para continuar la prestación del servicio SOC sobre dicha plataforma, garantizando la continuidad operativa, el monitoreo permanente y la correlación de eventos de seguridad, incluyendo la integración, normalización y correlación de las fuentes definidas por la ANM.	

Informacion publica

7.1.24.	El servicio de SOC debe realizar correlación de incidentes de seguridad entre proveedores y entre sectores.	
7.1.25.	El servicio debe tener la posibilidad de integrar las vulnerabilidades (detectadas por ANM) con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas durante la prestación del servicio	
7.1.26.	El servicio debe estar en la capacidad de generar recomendaciones y notificaciones preventivas para evitar incidentes de seguridad.	
	PROCESOS INTERNOS DEL SOC	
7.1.27.	El SOC deberá contar con procesos de priorización de atención de incidentes, los cuales se deben basar en una metodología clara de riesgos e impacto.	
7.1.28.	El SOC deberá contar con un grupo interdisciplinario interno para la atención de incidentes de alto impacto, bajo un procedimiento debidamente documentado. El cual debe ser socializado y coordinado con los responsables en la ANM.	
7.1.29.	El SOC deberá contar con procesos definidos para la detección, categorización y alertamiento temprano y oportuno de incidentes de seguridad.	
7.1.30.	El SOC debe disponer de procesos para la gestión de cambio sobre la plataforma que soporta el servicio y se debe ajustar al Procedimiento de Control de Cambios definido por la Oficina de Tecnología e Información de la Agencia Nacional de Minería.	
7.1.31.	El SOC debe disponer de herramientas colaborativas internas para el intercambio de información entre los funcionarios.	
7.1.32.	Se debe contar con roles y responsabilidades del grupo de operaciones del SOC debidamente definidos, en lo que respecta al monitoreo, atención, manejo y contención de incidentes de seguridad.	
7.1.33.	El modelo de operación del SOC debe basarse en estándares y metodologías reconocidos a nivel mundial en la implementación de CSIRT y CERT.	
7.1.34.	Debe prestar el servicio de administración sobre equipos WAF con Balanceo de Carga en el Data Center ANM CLL 26, para las aplicaciones de la ANM que requieran alta disponibilidad descritas. Este servicio permitirá distribuir las cargas de trabajo de manera eficiente en varios recursos. Las características técnicas de los equipos WAF disponibles en la entidad cuentan son las siguientes Desempeño SSL: 10.000 Transacciones por segundo SSL con llaves de 2048 bitsTipo de instalación: Proxy Inverso (Capa 7) y Full Proxy. Alta disponibilidad: activo/pasivo Protocolos de internet: IPv4 e IPv6 NOTA: La administración de los dispositivos ubicados en el Datacenter Principal de la ANM corresponde a un tercero distinto al contratista. Sin perjuicio de lo anterior, el contratista será responsable del monitoreo continuo, la generación de alertas, el seguimiento a incidentes y la coordinación obligatoria con dicho tercero para la ejecución de cambios, configuraciones o cualquier intervención sobre los equipos, sin que ello implique la asunción de funciones de administración directa. El contratista deberá asegurar la debida articulación entre las partes y la continuidad en la operación de la solución.	

Informacion publica

7.1.35.	El SOC debe contar con capacidad de hacer dos (2) "Assessment", así: 1 una vez iniciado el contrato y el segundo a los seis meses, esto sobre los dispositivos perimetrales, dicho Assessment deberá permitir como mínimo: a. Tener un panorama real sobre la efectividad de los accesos otorgados por los dispositivos, b. Hacer auditoria en los cambios de configuración y permisos c. Detectar reglas solapadas, mal usada y sin uso. El oferente debe presentar a la ANM la metodología y el proceso que utilizará para estas evaluaciones y deberá coordinarla con la ANM ciñéndose al procedimiento de gestión de cambios de la ANM que se encuentre vigente en dicho momento.	
	AUDITORÍA	
7.1.36.	Los procesos, tecnologías y personas que operan en el SOC, deben haber sido auditados por un ente externo en lo que respecta a un modelo de madurez de centro de operaciones de seguridad (SOMM - Security Operations Maturity Model) o marco de referencia equivalente, por lo menos una vez durante los últimos tres años.	
7.1.37.	El SOC y en general el proponente debe permitir a la ANM realizar auditorías sobre los procesos, tecnologías y personas que operan en el SOC, en caso de ser requerido, todas las veces que la ANM lo requiera.	
	PROTECCIÓN FÍSICA Y LÓGICA DEL SOC	
7.1.38.	El SOC debe estar protegido al menos con tres anillos de seguridad física.	
7.1.39.	El SOC debe tener protección física contra los siguientes posibles daños: Incendio, terremoto, manifestación social.	
7.1.40.	El acceso al área física o remoto donde se encuentran los analistas de gestión de eventos e incidentes de seguridad del SOC debe contar con factor de autenticación fuertes.	
7.1.41.	El SOC deberá estar protegido contra fallas en el suministro de energía y otras anomalías causadas por falla en los servicios de suministro.	
7.1.42.	El SOC deberá estar protegido para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado	
7.1.43.	En las instalaciones del SOC se deben aplicar políticas de seguridad física para oficinas, recintos e instalaciones donde se encuentran los equipos.	
7.1.44.	Las instalaciones del SOC deben tener controles para los puntos de acceso por donde pueda ingresar personal no autorizado a las instalaciones del SOC	
7.1.45.	El SOC deberá garantizar controles de acceso a cualquier repositorio de información que se requiera tato para la ANM, como para los demás clientes gestionados para evitar el acceso no autorizado.	
7.1.46.		

Informacion publica

	El proponente deberá contar con las herramientas necesarias para protección de la información para su visualización, procesamiento y almacenamiento.	
	DASHBOARD, REPORTEARÍA Y GESTIÓN DE INCIDENTES	
7.1.47.	El oferente deberá entregar un portal Web, basado en Business Intelligence, por medio del cual se pueda tener acceso a reportes, eventos, incidentes, estadísticas y análisis en tiempo real de los eventos capturados.	
7.1.48.	Generación automática de incidentes, a través de una plataforma integrada al recolector/correlacionador, con generación de la alarma y ticket correspondiente.	
7.1.49.	Generación automática de la notificación de los incidentes al menos a través de correo electrónico, llamadas telefónicas y mensajes de texto.	
7.1.50.	El proveedor debe contar con acceso a informes detallados sobre alertas mundiales que puedan afectar la seguridad sobre la infraestructura de la ANM y deberá poder compartirlas con la entidad.	
7.1.51.	Se deben entregar informes periódicos a la ANM, en donde se relacionen los incidentes de seguridad informática de categoría alta o crítica, una vez sean detectados y posteriormente indicar las acciones que se deben adelantar y los resultados de estas. La periodicidad de estos informes será establecida con la supervisión del contrato.	
7.1.52.	Se debe presentar la información de los eventos, incidentes, vulnerabilidades, indicadores de compromiso y mapa de riesgo a través de un portal web, el cual debe permitir a la ANM iniciar y tener la trazabilidad de eventos e incidentes de todas las plataformas que se encuentren dentro del actual proceso de contratación.	
7.1.53.	La ANM debe tener acceso a reportes para las actividades de mitigación pendientes.	
7.1.54.	Se debe prestar a la ANM a través de un portal web una vista completa sobre los activos, presentando al menos la siguiente información: propiedades de los activos, eventos e incidentes, indicadores de compromisos, vulnerabilidades y trazabilidad de la mitigación del problema con asignación individual a los activos/usuarios.	
7.1.55.	El proveedor debe poner a disposición de la ANM una base de conocimiento y buenas prácticas para la gestión de vulnerabilidades, respuesta y atención de incidentes de seguridad. La base de datos de conocimiento debe tener un histórico en todo momento de por lo menos dos (2) años.	
7.1.56.	Se deberán diseñar reportes gerenciales que incluyan mapas de calor, cumplimiento respectos a normas internacionales y estado de los activos y se deberán presentar	

Informacion publica

	periódicamente a la ANM, en las reuniones de seguimiento programadas para este contrato.	
7.1.57.	El proveedor y la ANM debe tener acceso a un Dashboard tipo web que soporte diferentes vistas acordes a las diferentes partes interesadas, incluyendo: alta dirección, equipo de operaciones y seguridad de la información.	
7.1.58.	El dashboard debe permitir exportar los datos soportando múltiples formatos, incluyendo por lo menos los formatos: csv, xml y pdf.	
7.1.59.	El dashboard debe presentar el estado de seguridad de la ANM. En tiempo Real	
7.1.60.	Se debe poder contar con acceso web a los informes y evidencias que permitan verificar el cumplimiento de los Acuerdos de Nivel de Servicio de manera mensual y presentarlos periódicamente a la ANM, en las reuniones de seguimiento programadas para este contrato.	
7.1.61.	Se debe poder contar con acceso web al cálculo, generación y presentación en línea de mapa de riesgos asociado a los activos monitoreados y presentarlos periódicamente a la ANM, en las reuniones de seguimiento programadas para este contrato.	
	OTRAS CONDICIONES DEL SERVICIO	
7.1.62.	El proveedor debe contar con personal certificado en la gestión o administración de la herramienta de recolección y correlación de eventos (SIEM). En los equipos de seguridad perimetral objeto de renovación de licenciamiento conforme el perfil establecido en el **LITERAL 4.2.** Profesional senior redes y seguridad informática, quien será el encargado de administrar los dispositivos de seguridad de la ANM y será el canal directo de comunicación entre el personal asignado por ANM, en el horario de Atención 5 X 8 LUNES A VIERNES con tiempos de respuesta de acuerdo con los ANS establecidos en el LITERAL 12 del presente documento	
7.1.63.	El proponente deberá certificar con su propuesta que ha realizado la verificación de antecedentes de los colaboradores o empleados que interactúen con el SOC, de acuerdo con los reglamentos, la ética y las leyes pertinentes. Los cuales deben ser soportados a la ANM en el momento que esta lo disponga.	
7.1.64.	El proveedor deberá contar con personal dedicado por turno a la operación del SOC que garanticen la capacidad Operativa 7x24X365	
7.1.65.	El proponente debe tener personal dedicado a la atención de incidentes diferente al personal involucrado en otros servicios como administración de plataformas, entre otros.	

MONITOREO DE EVENTOS EN PLATAFORMA DEFENDER FOR OFFICE 365 Y DEFENDER FOR END POINT

Informacion publica

Los Servicios de seguridad requeridos para la protección de buzones de correo electrónico y antivirus de la Agencia Nacional de Minería son:

No.	DESCRIPCIÓN	CUMPLIMIENTO
	ESPECIFICACIONES GENERALES	
7.1.66.	El proponente deberá ofrecer una metodología de monitoreo y seguimiento a los incidentes o eventos generados por la plataforma Ms 365 Defender for End point, Defender for Office, Itune, Sentinel y Antivirus . entre otros.	
	FUNCIONALIDADES DE LA SOLUCIÓN	
7.1.67.	La entidad requiere monitorear los eventos del servicio de seguridad de correo electrónico y de Antivirus con capacidades para 1850 buzones y 1200 estaciones.	
	ADMINISTRACIÓN	
7.1.68.	El servicio debe ser administrado por el oferente desde su centro de operaciones	
7.1.69.	El servicio no debe requerir la instalación de agentes o infraestructura en las instalaciones de ANM	
	GENERACIÓN DE REPORTES	
7.1.70.	El servicio debe incluir reportes en línea donde se permita ver el estado de seguridad, indicadores, reportes y datos en tiempo real, apoyado en tecnologías de BI (Business Intelligence) adaptado a Seguridad (BIS)	
7.1.71.	El Portal debe permitir a los usuarios que defina la ANM la visualización de alertas escaladas a través del mismo.	
7.1.72.	El Portal de reportes de incidentes debe permitir a los usuarios que defina la ANM iniciar y realizar la trazabilidad de alertas relacionadas en este portal	
7.1.73.	El proveedor y la ANM deben tener acceso a una base de conocimiento y buenas prácticas de seguridad que apoye la gestión de vulnerabilidades, respuesta y atención de incidentes de seguridad. La base de datos de conocimiento debe tener un histórico en todo momento de por lo menos dos (2) años.	
7.1.74.	El portal debe estar en capacidad de presentar informes gráficos de estado de los activos de seguridad basados en ubicación, unidad de negocio. El formato grafico	

Informacion publica

	debe soportar diferentes métodos para la representación de la información como gráficos, estadísticas, entre otros.	
7.1.75.	El dashboard debe permitir exportar los datos soportando múltiples formatos, incluyendo por lo menos los formatos: csv, xml y pdf.	
7.1.76.	Se debe poder contar con acceso a web a los informes y evidencias que permitan verificar el cumplimiento a los Acuerdos de Nivel de Servicio de manera mensual.	
7.1.77.	La ANM debe contar con la posibilidad de solicitar la creación de nuevos tableros de control o vistas sobre el portal web.	
7.1.78.	El proveedor debe generar recomendaciones y notificaciones preventivas para evitar incidentes de seguridad, dirigidas tanto a personal técnico de la ANM, como a usuarios finales, los mensajes para usuarios serán acordados con personal de la Entidad y se remitirán por parte de la Agencia.	

7.2. CORRELACIONADOR DE EVENTOS SIEM

La Agencia Nacional de Minería – Actualmente cuenta con el servicio de correlacionador SIEM a través de la modalidad de Software como Servicio (SaaS). El marco de la presente contratación comprende la adquisición y puesta en marcha de una solución SIEM en modalidad virtualizada, incluyendo el respectivo licenciamiento con capacidad para cincuenta (50) dispositivos y mil (1000) EPS, así como indicadores de compromiso (IOC) y soporte por doce (12) meses, contados a partir de su implementación y puesta en marcha, como extensión de la plataforma Fortinet actualmente implementada en la entidad. El contratista deberá implementar la solución y prestar los servicios relacionados en el presente documento.

En consecuencia, el servicio de SOC ofertado deberá contemplar la implementación de este producto en modalidad de SOFTWARE COMO SERVICIO (SaaS) durante el periodo de implementación del servicio SIEM de propiedad de la ANM (2 MESES APROXIMADAMENTE).

El oferente debe realizar la configuración de los colectores y cualquier configuración para la prestación de monitoreo, administración, correlación y gestión de eventos de seguridad asociados a dicha solución SIEM, incluyendo su integración dentro de la operación del servicio de monitoreo y gestión de seguridad de la información de la ANM cuyas características se encuentran establecidas a continuación:

Informacion publica

	RECOLECCIÓN Y CORRELACIONADOR DE EVENTOS (SIEM)	
7.2.1.	El proveedor deberá contar con una solución de recolección y correlación de eventos (SIEM) debidamente certificada en modalidad (SAAS) , la cual deberá disponer de servicios de soporte y mantenimiento por parte del fabricante o de un canal autorizado, durante el tiempo en que el servicio sea prestado sobre la plataforma SIEM del proveedor. La supervisión del contrato podrá solicitar, tanto al inicio como durante la ejecución contractual, las evidencias que acrediten la vigencia del soporte y mantenimiento del SIEM utilizado para la prestación del servicio, así como realizar las verificaciones que considere necesarias. **NOTA 1:** Al inicio de la ejecución del contrato, el proveedor deberá prestar el servicio de monitoreo SOC sobre la solución SIEM operada bajo la modalidad de Software como Servicio (SaaS), garantizando la continuidad del monitoreo y la gestión de eventos de seguridad de la información de la ANM. Una vez se implemente y ponga en funcionamiento la solución SIEM propia de la ANM dentro de su infraestructura tecnológica, el proveedor deberá realizar las configuraciones, integraciones y actividades de migración necesarias para continuar la prestación del servicio SOC sobre dicha plataforma, garantizando la continuidad operativa, el monitoreo permanente y la correlación de eventos de seguridad. **NOTA 2:** Una vez la solución SIEM propia de la ANM se encuentre implementada y operativa dentro de la infraestructura tecnológica de la entidad, el proveedor deberá garantizar la ejecución de las actividades asociadas a la recolección y correlación de eventos (SIEM) descritas en el presente numeral y demás apartes aplicables del anexo técnico a través del mismo, siempre que correspondan técnicamente a la arquitectura, funcionalidades y alcance de la solución implementada.	
7.2.2.	Tanto el SIEM utilizado por el SOC como el ofertado debe aparecer clasificado como "Retador" o "líder" en el cuadro mágico de Gartner (SIEM/MSSP) en el reporte correspondiente a 2023 o 2024.	
7.2.3.	Se debe incluir la capacidad de detección de anomalías en el comportamiento de las aplicaciones, equipos y usuarios de la plataforma.	
7.2.4.	Se debe incluir la generación de indicadores de cumplimiento para los activos monitoreados,	
7.2.5.	Se debe realizar la detección de uso de eventos s o accesos a la plataforma que no concuerden con el patrón histórico de uso o acceso.	
7.2.6.	Identificar al menos los siguientes eventos de seguridad, mínimos para monitorear: - Accesos no autorizados - Denegación de servicio. - Explotación de vulnerabilidades. - Fuerza bruta/login. - Escaneo de puertos. - Principales orígenes de ataque. - Principales destinos de ataque. a. Ubicación geográfica del ataque. b. Orígenes/destinos reportados por fuentes de inteligencia de seguridad. c. Acceso por parte de los usuarios a dominios diferentes a los autorizados.	

Informacion publica

d. Cambios sobre Plataformas (software instalado, desinstalado, cambio de políticas del directorio activo)
e. Conexiones (accesos remotos, intentos de conexión)
f. Eliminación de logs
h. Actividades de cuentas de altos privilegios
i. Usuarios (bloqueados, agregados, eliminados, desbloqueados, cambio de contraseñas)

7.2.7. El proveedor debe realizar el diseño y modelamiento de servicio de monitoreo específico para ANM

7.2.8. Las fuentes requeridas a monitorear y correlacionar a la fecha de la propuesta son como mínimo:

No	Fuente	Conector	Dirección IP	Hostname
1	Cluster Fortinet	Syslog_UDP_5150 _COS_ACA	10.0. 12x.x	CLUSTER_ANM_ FG
2	Cluster FortiWeb	Syslog_UDP_5148 _COS_ACA	10.0.10x.x0x	CLÚSTER_ANM_ WAF
3	NGFW – NUBE PRIVADA	Syslog_UDP_5148 _COS_ACA	181.225.XX. 2xx	FGT_1200D (Century)
4	WAF – NUBE PRIVADA	Syslog_UDP_5148 _COS_ACA	181.225.XX. 2x9	WAF_1000E (Century)
5	WINDOWS DA	WIN RM COS ACA	10.0.1x0.6x	ANMXX0X.XXXX. LOCAL
6	DEFENDER	Syslog_UDP_5148 _COS_ACA		Microsoft 365
7	WAF A-ZURE	Syslog_UDP_5148 _COS_ACA		APP CLOUD AZURE
8	Antivirus	Syslog_UDP_5148 _COS_ACA		(Por Definir)

.

7.2.9. Se debe realizar la configuración del colector necesario para incluir en el SIEM la plataforma Defender for Office y Defender for End point, Intune, Ms Sentinel correspondiente a la plataforma de administración de end point o aquella adquirida por la ANM para tal fin y atender los casos (requerimientos e incidentes) que se generen a través de la Oficina de Tecnología e Información de la ANM, para lo cual la Entidad brindará los accesos y asignará los correspondientes perfiles. La ANM, se encargará que la plataforma cuente con los contratos vigentes que garanticen el soporte de fábrica.

7.2.10. Los conectores de captura de eventos deberán enviar en todo momento y en tiempo real los eventos recolectados hacia el motor de correlación, salvo que se requiera habilitar bajo demanda de envió asíncrono de eventos.

7.2.11. Los eventos capturados por la funcionalidad de recolección de eventos deben correlacionarse en tiempo real.

7.2.12. Posibilidad de recolectar eventos de aplicaciones, sistemas o plataformas no predefinidas.

Informacion publica

7.2.13.	La transmisión de los datos entre los componentes recolectores de eventos y el motor de correlación deberán utilizar mecanismos de cifrado y de compresión de datos.	
7.2.14.	Se debe estar en la capacidad de comprobar la integridad de los eventos correlacionados.	
7.2.15.	La solución de recolección y correlación (SIEM) debe soportar esquemas de Alta Disponibilidad (Activo- Activo) y Recuperación de Desastre.	
7.2.16.	La solución de recolección y correlación (SIEM) debe ser alimentada por fuentes de inteligencia externas de amenazas que contengan listas de reputación o dominios catalogados como sospechosos para la generación de indicadores de compromiso.	
7.2.17.	El motor analítico de la solución de recolección y correlación (SIEM) debe permitir identificar patrones anómalos de comportamiento por usuario y/o IP.	
7.2.18.	La solución de recolección y correlación (SIEM) deberá tener la capacidad de recibir logs en formato crudo (RAW) a través de los siguientes mecanismos: Syslog (TCP o UDP), transferencia remota archivos con logs crudos por SCP (Secure Copy), sftp (Secure FTP) o ftp, o Archivos de logs en sistemas mediante NFS y/o CIFS	
7.2.19.	Se requiere hasta tres (3) colectores de logs personalizados con el fin de garantizar el desarrollo de estos para integrar estas fuentes con el servicio de correlación, toda vez que se contará con infraestructura de un tercero que alojará servicios de la Entidad.	
7.2.20.	Los componentes que realizan la recolección de eventos deberán verificar constantemente el estado de la conexión con el correlacionado a través de un mecanismo eficaz que ante la eventual pérdida de la conexión entre el componente de recolección y el motor de correlación, genere de manera inmediata la notificación, adicionalmente el primero deberá almacenar de forma inmediata los eventos bajo una cache de tamaño configurable hasta que se reanude dicha conexión, realizando la transmisión de los eventos hasta vaciar el cache.	
7.2.21.	La solución debe permitir configurar controles de uso de ancho de banda o soluciones que, aunque no utilicen el término literal “control de ancho de banda”, cumplan con el objetivo funcional mediante mecanismos equivalentes, como filtrado, transformación y priorización de eventos desde el origen para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato.	
7.2.22.	La solución de recolección y correlación (SIEM) deberá tener la capacidad de agregación de eventos similares basada en campos definidos por el usuario y bajo una ventana de tiempo parametrizable, enviando al motor de correlación eventos de tipo agregación que contienen la cuenta de eventos previamente agregados.	
7.2.23.	Los componentes que realizan la recolección de eventos deberán tener la capacidad de filtrado de eventos particulares desde el origen, con lo que se reducirá el volumen de eventos que recibirá el motor de correlación.	
7.2.24.	El servicio de SOC debe realizar correlación de incidentes de seguridad entre proveedores y entre sectores.	
7.2.25.	La solución de recolección y correlación de eventos (SIEM) debe tener la capacidad de ofuscar/eliminar campos sensibles, capacidad de agregación y filtrado.	
7.2.26.	El proveedor deberá garantizar que la solución SIEM este en capacidad de colectar, procesar, monitorear y correlacionar más de de 3000 EPS (Eventos por Segundo).sin filtrar y Filtrados 512 EPS Diarios	

Informacion publica

7.2.27.	Los componentes que realizan la recolección de eventos deberán realizar desde el origen la normalización completa de los eventos, es decir únicamente enviarán hacia el SIEM los eventos previamente estructurados en campos específicos para la correlación, retención, análisis y reporteo de los eventos.	
7.2.28.	La solución debe permitir detectar fluctuaciones en la recepción de logs por fuente de información.	
7.2.29.	La solución debe permitir correlacionar la información de Accesos a nivel perimetral (Firewalls), junto con las vulnerabilidades detectadas a nivel de equipos, esto con el fin de simular propagaciones de malware y explotaciones de vulnerabilidades	
7.2.30.	La solución debe tener la posibilidad de integrar las vulnerabilidades (detectadas por ANM) con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas durante la prestación del servicio	
7.2.31.	La solución debe estar en la capacidad de generar recomendaciones y notificaciones preventivas para evitar incidentes de seguridad.	

7.3. ADQUISICION DEL PRODUCTO FORTIPAM de FORTINET.

La Entidad requiere fortalecer los controles de seguridad asociados a la administración de accesos privilegiados sobre su infraestructura tecnológica, con el fin de proteger los activos de información, garantizar la continuidad de la operación institucional y reducir los riesgos derivados del uso indebido, pérdida o compromiso de credenciales con altos niveles de privilegio.

Los usuarios administradores poseen accesos que les permiten realizar configuraciones, modificaciones y actividades críticas sobre servidores, bases de datos, aplicaciones, dispositivos de red y demás componentes de la plataforma tecnológica. La administración inadecuada de estas cuentas representa uno de los principales riesgos de ciberseguridad, pudiendo generar afectaciones a la confidencialidad, integridad y disponibilidad de la información institucional.

En atención a esta necesidad, se requiere la adquisición de la solución FortiPAM (Privileged Access Management) para 20 usuarios administradores, la cual incluye funcionalidades especializadas para la gestión, control, monitoreo y auditoría de accesos privilegiados, permitiendo centralizar la administración de credenciales, registrar las sesiones realizadas por los usuarios autorizados y aplicar controles de acceso basados en principios de mínimo privilegio y trazabilidad.

Adicionalmente, la solución incorpora capacidades de Advanced Malware Protection, que contribuyen a la detección y mitigación de amenazas avanzadas que puedan comprometer las cuentas privilegiadas o los sistemas administrados. Asimismo, incluye el licenciamiento del agente requerido para su operación y el servicio de soporte técnico y actualización por un período de hasta doce (12) meses, garantizando la continuidad operativa de la plataforma, la atención de incidentes y el acceso a mejoras de seguridad liberadas por el fabricante.

Informacion publica

La implementación de esta solución permitirá a la Entidad fortalecer su postura de ciberseguridad, mejorar los mecanismos de control y auditoría sobre actividades administrativas, reducir los riesgos de acceso no autorizado a sistemas críticos y contribuir al cumplimiento de buenas prácticas y estándares de seguridad de la información, así como de los lineamientos institucionales de gestión de riesgos tecnológicos.

En consecuencia, la contratación de la solución FortiPAM para 20 usuarios administradores se considera necesaria y conveniente para garantizar una administración segura de accesos privilegiados, proteger los recursos tecnológicos institucionales y asegurar la adecuada prestación de los servicios soportados por la infraestructura tecnológica de la Entidad.

La adquisición del producto debe incorporar su implementación y puesta en marcha, así como la capacitación una vez implementada la solución y el soporte técnico por 12 meses

7.4. ADMINISTRACION DE LA PLATAFORMA FORTIPAM

Con el fin de garantizar el adecuado funcionamiento, operación y aprovechamiento de la solución de Gestión de Accesos Privilegiados (PAM) implementada por la Entidad, se hace necesario contar con un servicio especializado para la administración de la plataforma FortiPAM.

La solución FortiPAM constituye un componente crítico dentro de la estrategia institucional de ciberseguridad, debido a que centraliza la gestión de cuentas privilegiadas, controla los accesos administrativos a los sistemas de información, registra y audita las sesiones de usuarios con privilegios elevados y permite la aplicación de controles orientados a la protección de la infraestructura tecnológica de la Entidad.

La administración de esta plataforma requiere conocimientos técnicos especializados en gestión de identidades y accesos privilegiados, configuración de políticas de seguridad, administración de credenciales, monitoreo de eventos, análisis de registros, gestión de incidentes de seguridad y aplicación de actualizaciones y buenas prácticas recomendadas por el fabricante. Estas actividades son fundamentales para asegurar la disponibilidad, integridad y efectividad de la solución implementada.

Mediante la contratación del servicio de administración de FortiPAM, la Entidad busca garantizar la correcta configuración y parametrización de la herramienta, la gestión oportuna de usuarios y perfiles, el monitoreo permanente de accesos privilegiados, la atención de requerimientos operativos, la generación de reportes de auditoría, la identificación de posibles riesgos de seguridad y la implementación de acciones preventivas y correctivas que contribuyan a fortalecer la protección de los activos de información institucionales.

Asimismo, este servicio permitirá optimizar el uso de las capacidades adquiridas en la plataforma, mantener actualizadas las configuraciones de seguridad, asegurar la continuidad operativa de los controles de acceso privilegiado y reducir los riesgos asociados a accesos no autorizados, uso indebido de credenciales administrativas y posibles incidentes de ciberseguridad.

En consecuencia, la contratación del servicio especializado para la administración de la solución FortiPAM se considera necesaria para garantizar la adecuada operación de la plataforma, maximizar los beneficios de la inversión realizada por la Entidad y fortalecer el modelo de seguridad y gestión de riesgos tecnológicos institucionales.

7.5. PRUEBAS DE SEGURIDAD: VULNERABILIDADES, PENTEST e INGENIERA SOCIAL.

La ANM busca contar con un servicio para que durante la ejecución del contrato realicen las siguientes actividades:

Informacion publica

a) Identificación y verificación de vulnerabilidades técnicas (test y retest) y pen test.
b) Orientar el personal de la Oficina de Tecnología e Información de la ANM, para la remediación de vulnerabilidades técnicas
c) Prueba de ingeniería social.
d) El oferente debe contar con sus propias herramientas para la realización de las PRUEBAS DE SEGURIDAD. Del presente literal.

No.	DESCRIPCIÓN	CUMPLIMIENTO
	PRUEBAS DE SEGURIDAD	
7.5.1.	Pruebas técnicas de Vulnerabilidad y pen test: El contratista deberá definir los planes de trabajo para realizar pruebas de vulnerabilidades no sean intrusivas ni invasivas, garantizando la integridad, confidencialidad y disponibilidad de los activos a examinar, así mismo garantizar lo correspondiente cuando se realicen las pruebas de penetración.	
7.5.2.	Se realizarán una prueba de vulnerabilidad para un mínimo de **100 direcciones IP**, (incluye equipos y aplicaciones públicas o privadas) y posteriormente de dos a seis meses se debe realizar el RETEST correspondiente. Se debe tomar como línea base los activos que ya tiene la agencia y sobre los cuales ha venido realizando el análisis de vulnerabilidades. Para la segunda prueba, es decir, la prueba de RE-TEST semestral se ejecutará sobre el mismo segmento de 100 direcciones IP evaluadas en la prueba inicial para medir técnicamente la efectividad de los planes de remediación aplicados	
7.5.3.	Para la valoración de las vulnerabilidades se debe utilizar el modelo de Common Vulnerarability Scoring System (CVSS)y Las herramientas deben contar con el correspondiente licenciamiento. La herramienta debe contar con el “Certificante of CVE Compatibility” -MITRE.	
7.5.4.	El contratista deberá recoger toda la información necesaria para la realización del análisis de vulnerabilidades externo e interno y pruebas de penetración a la plataforma cuyo alcance incluye como mínimo: - Computadores - Aplicaciones - Sistemas operativos - Switches - Access point - Impresoras-Escáneres - Cámaras IP	

Informacion publica

	Routers UPS Aires acondicionados Servidores Bases de Datos Telefonía Videoconferencia Solución de seguridad: firewall, antivirus, IPS Sistemas de Información	
7.5.5.	Se debe desarrollar pruebas de vulnerabilidad sobre los elementos de información y tecnología según aplique y como mínimo lo siguiente: Debilidades Java Debilidades de Browser Comprobación de password y protocolos de cifrado débil. Validación de protocolos de cifrado implementados Debilidades direccionamiento y enrutamiento SSID (Service Set IDentifier-Identificador de paquetes) de redes inalámbricas Configuraciones por defecto de servicios y aplicativos. Identificación de los puertos abiertos en los objetivos (TCP: Protocolo de Control de Transmisión, UDP: Protocolo de datagrama de usuario). Identificación de los servicios que se están ejecutando en los objetivos. Rompimiento de claves default Identificación de vulnerabilidades de los sistemas operativos Búsqueda y extracción de información sensible accesible por la red, como la existente en las carpetas compartidas. Debilidades de Session Hijacking (secuestro de session) Códigos de error Debilidades Buffer Overflow (desborde de memoria)	

Informacion publica

	Debilidades por SQL Injection Debilidades por Queries estructurados Debilidades por autenticación de base de datos Ataques a las aplicaciones Sniffing: técnica utilizada para capturar todo el tráfico generado en una red local Extracción de información confidencial. b) Una vez realizado cada análisis de vulnerabilidades se deben adelantar las pruebas de penetración teniendo en cuenta: - Basado en la información que resulte de las pruebas, se determinarán de común acuerdo con la entidad, aquellos objetivos específicos de pruebas de penetración que probablemente tengan mayor éxito en orden de prioridad cubriendo como mínimo 10 direcciones IP internas y/o externas. - Pruebas de penetración sobre vulnerabilidades críticas encontradas lo cual incluye pruebas de penetración interna y externa, al menos una prueba de penetración de caja gris y una prueba de caja negra (a ciegas). - Las pruebas son selectivas y se realiza en conjunto por el personal de la agencia y el asesor. c) Se debe informar el tiempo, recursos, resultados esperados, actividades para revisión y aprobación de la ANM. d) Para todas las vulnerabilidades que se encuentren debe comprobarse que pueden ser explotadas, sin afectar ambientes de producción, dependiendo del alcance de la prueba. e) Identificar las posibles vulnerabilidades presentes en las aplicaciones. f) Búsqueda de información sensible accesible por la red, como la existente en las carpetas compartidas. g) Evaluar si existe información sensible que pueda ser accedida sin autorización. Se debe incluir los resultados de cada una las pruebas, así como los planes de pruebas en informe detallado y ejecutivo (se debe realizar la presentación de los resultados), incluyendo el avance de la línea base de las anteriores pruebas. También se deben incluir las acciones recomendadas para el plan de remediación	
7.5.6.	Se deberá brindar la orientación por parte del “Analista de Ciberseguridad” al personal de la Agencia para la remediación de vulnerabilidades técnicas indicado las acciones a implementar e indicar la priorización de remediación conforme con su criticidad y complejidad. Para ello se deben realizar sesiones con cada uno de los responsables de la remediación.	

Informacion publica

	La cantidad de horas establecidas en el literal 5 - Analista de Ciberseguridad- para el servicio serán distribuidas posterior al análisis inicial y RETEST según la necesidad y cuyo objetivo será soportar la implementación de acciones de remediación para fortalecer la seguridad de los activos de información. A partir de la identificación y diagnóstico de vulnerabilidades, se requiere de un plan de cierre de vulnerabilidades técnicas y la implementación de acciones de remediación.	
7.5.7.	Para cada una de las pruebas que se realizarán durante la ejecución del contrato se deberá contar con un plan específico para el análisis de vulnerabilidades y para las pruebas de penetración, los cuales deberán contar mínimo con la siguiente información: Objetivo y alcance Metodología Pruebas para realizar Recursos Herramientas	
7.5.8.	El contratista deberá elaborar el informe de ejecución del análisis de vulnerabilidades, de las pruebas de penetración y de las pruebas ingeniería social el cual debe incluir por lo menos lo siguiente: Objetivo y alcance Definiciones técnicas (si aplica) Metodología aplicada, incluye fase de levantamiento de información y preparación de pruebas Metodología de valoración del riesgo basado en CVSS. Descripción de la fase de ejecución Detalle de las vulnerabilidades encontradas y clasificadas por tipo de dispositivo de la plataforma de TI. Número del CVE (clasificación internacional) de cada una de las vulnerabilidades Matriz de vulnerabilidad técnica donde se evidencie la gestión con métricas de impacto y explotación por cada vulnerabilidad, descripción, asignación de responsable y tiempos propuestos para el cierre. Se debe incluir la valoración del riesgo Modelo de gestión de vulnerabilidades donde se evidencie el progreso de la gestión de las vulnerabilidades durante el periodo de la asesoría, lo cual incluya como mínimo los siguientes indicadores: Índice de vulnerabilidad: Permite medir en el tiempo la forma como varía el índice teniendo en cuenta el total de vulnerabilidades identificadas frente al número total de máquinas evaluadas (direcciones IP).	

Informacion publica

	TotVul: Total de vulnerabilidades identificadas TotMaq: Total de máquinas evaluadas (Direcciones IP) TotVul(Ext+Alt): Total de vulnerabilidades identificadas TotVul: Total de vulnerabilidades identificadas Cantidad de vulnerabilidades según el tiempo de remediación: Permite medir el número de vulnerabilidades según el tiempo de remediación: corto, mediano y largo plazo. Deberá diseñarse la ficha de cada indicador, la cual debe incluir al menos fecha, el nombre del indicador, propósito, descripción, la fórmula, variables, meta, resultado, escalas. El contratista también podrá diseñar adicionalmente otros indicadores que le permitan a la Entidad, medir el progreso de la gestión de las vulnerabilidades y otros indicadores propuestos para los resultados de las pruebas de ingeniería social.	
7.5.9.	Se deben acordar y realizar reuniones presenciales con el responsable en la Agencia de cada proceso/activo, de tal forma que se presenten los resultados y se indique de forma documentada las acciones de remediación que deben establecerse en cada caso. La evidencia de las reuniones realizadas, las recomendaciones y conclusiones deberá incluirse dentro del informe. Después de cada prueba se debe generar un Plan de acción preventivo y correctivo, se deben presentar resultados de medición entre pruebas y los avances de la Entidad después de cada retest. Se deben presentar los resultados de las pruebas de penetración, las recomendaciones para la implementación del control o controles, el análisis, conclusiones, recomendaciones y pasos a seguir en el proceso de remediación de cada una de las vulnerabilidades.	
7.5.10.	**Prueba de ingeniería social:** Se debe definir un plan de trabajo para la ejecución de una prueba de ingeniería social de carácter presencial o no presencial según se defina con el supervisor del contrato de tal manera que se pueda evidenciar el cumplimiento de controles de seguridad de la información El alcance de las pruebas debe abarcar todas las sedes y debe estar dirigido a todo el personal de la ANM. Las pruebas de ingeniería social que incluyan suplantación o pishing deben abarcar la totalidad de cuentas de correo electrónico, es decir aproximadamente 1850 usuarios.	
7.5.11.	Las pruebas deben ser realizadas con herramientas especializadas, pero no solo limitarse a estas, se debe realizar el diseño completo de la prueba haciendo análisis OSINT previo y verificando la mejor manera de realizar el engaño. El diseño debe ser realizado por un especialista en ingeniería social o con amplia experiencia en OSINT.	
7.5.12.	Aplicar parte de la metodología Open Source Security Testing Methodology – OSSTMM (Manual de la Metodología Abierta del Testeo de Seguridad:	

Informacion publica

7.5.13.	Para las pruebas de ingeniería social el contratista debe establecer y presentar previamente a la ANM una metodología detallada para la ejecución, especificando, entre otros aspectos, los criterios según los cuales se considerará que la prueba es exitosa. Dicha metodología deberá entregarse a los 15 días hábiles contados a partir del inicio del contrato. Así mismo debe especificar las herramientas tecnológicas que utilizará y en caso de que sobre estas se requiera licenciamiento se debe especificar el cumplimiento del mismo, aportando los soportes correspondientes.	
7.5.14.	El contratista debe proponer una modelo de valoración de éxito de las pruebas de ingeniería social, además de diferentes indicadores, por lo menos dos indicadores por prueba.	
7.5.15.	En la metodología para desarrollar en las pruebas de ingeniería social se deben establecer en las instalaciones de la ANM. Se define como alcance todas las sedes de la ANM y para las pruebas presenciales para la totalidad de oficinas de la Agencia ubicadas en la Sede Central Avenida Calle 26 No. 59-51 Torre 4 – Pisos 8, 9 y 10, las que serán acordadas con el Supervisor de Contrato Las pruebas no presenciales, estarán orientadas a la utilización de medios informáticos tales como como el correo electrónico, redes sociales e Internet, y se realizarán con recursos propios del Contratista. Estas pruebas deben contemplar actividades de ingeniería social para el total de los funcionarios de la ANM, realizando como mínimo una prueba por cada uno de los siguientes controles de la norma ISO27001: - A7 Seguridad en Recursos humanos - A9 Control de Acceso - A11 Seguridad Física y del entorno - A16 Gestión de Incidentes de Seguridad de la información Las actividades deben ofrecer un mensaje de concienciación directo a los usuarios afectados, indicando las falencias encontradas y las mejoras prácticas para mitigarlas, tanto las pruebas como el material de concienciación deben ser aprobado por el supervisor del contrato	
7.5.16.	El contratista deberá elaborar el informe de ejecución de las pruebas de ingeniería social el cual debe incluir por lo menos lo siguiente: - Objetivo y alcance - Definiciones técnicas (si aplica) - Metodología aplicada, incluye fase de levantamiento de información y preparación de pruebas	

Informacion publica

	Metodología de valoración del riesgo. Descripción de la fase de ejecución Detalle de las vulnerabilidades encontradas y clasificadas por tipo de dispositivo de la plataforma de TI. y Resultados.	

7.6. RENOVACION DE LICENCIAMIENTO VrX VICARUIS

La ANM requiere la renovación de licenciamiento y los servicios conexos la renovación de 150 licencias de VrX. por 12 meses, contados a partir de su activación. Con el siguiente alcance que incluya administración de plataforma y soporte de fabricante

Este producto debe ser licenciado a nombre de la Agencia Nacional de Minería.

VrX VICARUIS es plataforma SaaS unificada de gestión y remediación de vulnerabilidades que permite identificar, priorizar y corregir amenazas de ciberseguridad en tiempo real. Combina la detección de vulnerabilidades con herramientas activas como parches, scripts y "patchless protection" (protección sin parches) para proteger aplicaciones, sistemas operativos y software de terceros. Esta solución de gestión de vulnerabilidades es diseñada para ayudar a las organizaciones a identificar, priorizar y mitigar riesgos de seguridad en sus entornos tecnológicos de manera eficiente y automatizada. A diferencia de las herramientas tradicionales que se limitan a detectar vulnerabilidades, Vicarius incorpora capacidades avanzadas de remediación, incluyendo la aplicación de parches virtuales (virtual patching), lo que permite proteger sistemas incluso cuando no es posible aplicar actualizaciones oficiales de inmediato.

Entre sus principales características se destacan:

Descubrimiento y análisis continuo de vulnerabilidades: Monitorea activos en tiempo real para detectar exposiciones en sistemas operativos, aplicaciones y software de terceros.

Priorización inteligente de riesgos: Utiliza inteligencia contextual para clasificar vulnerabilidades según su nivel de criticidad, exposición y probabilidad de explotación.

Remediación automatizada: Permite aplicar soluciones correctivas de forma directa, reduciendo la dependencia de procesos manuales.

Patching sin interrupciones: A través de su enfoque de parcheo virtual, protege activos sin afectar la operación o disponibilidad de los sistemas.

Visibilidad centralizada: Ofrece paneles de control intuitivos que facilitan la toma de decisiones y el seguimiento del estado de seguridad.

Integración con herramientas existentes: Se adapta fácilmente a ecosistemas de TI ya implementados, optimizando los procesos de gestión de seguridad.

7.7. RENOVACIÓN LICENCIAMIENTOS DE EQUIPOS FORTINET:

La ANM requiere la renovación de licenciamiento y los servicios conexos, para los siguientes productos:

Informacion publica

NOTA. Se debe incluir soporte de primer nivel por el oferente, junto con soporte de Fabrica por el tiempo de renovación de los servicios.

EQUIPO	N° DE SERIAL	FECHA INICIO DE LA SUSCRIPCIÓN	PLAZO MÌNIMO (*)
FORTIGATE FG-1100E	FG10E0TB20900139	Dentro de los cinco (5) días siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, deberá entregarse el soporte documental en donde se acredite a la suscripción a los servicios de soporte de fábrica y la renovación del licenciamiento. En todo caso deberá tenerse en cuenta que ante el vencimiento del licenciamiento de cada uno de los dispositivos antes de la fecha de contratación el plazo de la suscripción requerida se contará a partir del cumplimiento de los requisitos de ejecución y firma del acta de inicio.	1 Mes
FORTIGATE FG-1100E	FG10E0TB20900161		
FORTIANALIZER FAZ-300G	FAZ3HGTA24000646		
FORTIWEB FV-1000E	FV-1KE4417900028		
FORTIWEB FV-1000E	FV-1KE4417900031		

PRODUCTO	SERIAL / REFERENCIA	Fecha Vencimiento
FORTIGATE FG-1100E	FG10E0TB20900139	Octubre 31 de 2026
FORTIGATE FG-1100E	FG10E0TB20900161	Octubre 31 de 2026
FORTIANALIZER FAZ-300G	FAZ3HGTA24000646	Octubre 31 de 2026

Informacion publica

FORTIWEB FV-1000E	FV-1KE4417900028	Octubre 31 de 2026
FORTIWEB FV-1000E	FV-1KE4417900031	Octubre 31 de 2026
Endpoint-based Licenses - VPN/ZTNA 1 Year FortiClient VPN/ZTNA Agent Subscription	EMS hosted by FortiCloud with FortiCare Premium EMS FCTEMS8825002644	Octubre 31 de 2026

La renovación deberá realizarse en las mismas condiciones del licenciamiento actual, el cual presenta las siguientes características:

FG10E0TB20900139 y FG10E0TB20900161	
Support Type	**Support Level**
Hardware	Advanced HW
Firmware & General Updates	Web/Online
Enhanced Support	Premium
Telephone Support	Premium
Advanced Malware Protection	Web/Online
NGFW	Web/Online
Web & Video Filtering	Web/Online
AntiSpam	Web/Online
Industrial Security Service	Web/Online
FortiConverter Service	8x5
Security Rating Update	Web/Online

Informacion publica

Elite Service	Web/Online
IoT Detection	Web/Online

NOTA 1: En todo caso el oferente deberá contemplar todas las firmas y suscripciones necesarias para que la plataforma quede totalmente licenciada y con las características activas de Firewall de Nueva Generación.

FAZ3HGTA24000646	
Support Type	**Support Level**
Hardware	Advanced HW
Firmware & General Updates	Web/Online
Enhanced Support	Premium
Telephone Support	Premium
FortiGuard IOC	Web/Online

NOTA 2: En todo caso el oferente deberá contemplar todas las firmas y suscripciones necesarias para que la plataforma quede totalmente licenciada y con las características activas para su funcionalidad de analizador de logs y generador de reportes.

FV-1KE4417900028 y FV-1KE4417900031	
Support Type	**Support Level**
Hardware	Advanced HW
Firmware & General Updates	Web/Online
Enhanced Support	Premium
Telephone Support	Premium
Advanced Malware Protection	Web/Online
FortiWeb Security Service	Web/Online
IP Reputation	Web/Online
PRMA	24x7x4 Courier HW

Informacion publica

Credential Stuffing Defense	Premium
FortiSandbox Cloud	Premium

NOTA 3: En todo caso el oferente deberá contemplar todas las firmas y suscripciones necesarias para que la plataforma quede totalmente licenciada y con las características activas de Firewall de Aplicaciones Web, garantizando que quede habilitada una capacidad mínima de 2Gbps de Throughput de WAF.

ÍTEM	DESCRIPCIÓN
	Endpoint-based Licenses - VPN/ZTNA 1 Year FortiClient VPN/ZTNA Agent Subscription for **1700 endpoints**. Includes EMS hosted by FortiCloud with FortiCare Premium

Para la prestación de todos los servicios el proveedor debe ter en cuenta que la Entidad se encuentran en un proceso de migración hacia el protocolo IPV6, en cumplimento de lo establecido en la normatividad vigente.

7.7.1. PRODUCTOS OBJETO DE RENOVACIÓN:

ÍTEM	DESCRIPCIÓN
1	Renovación de licenciamiento: • FORTIGATE FG-1100E S/N: FG10E0TB20900139. • FORTIGATE FG-1100E S/N: FG10E0TB20900161. • FORTIANALIZER FAZ-300G S/N: FAZ3HGTA24000646. • FORTIWEB FV-1000E S/N: FV-1KE4417900028. • FORTIWEB FV-1000E S/N: FV-1KE4417900031. • EMS - FCTEMS8825002644 **Nota**: El proveedor debe tener en cuenta la vigencia de las licencias señaladas y cotizar de manera proporcional desde la fecha de aplicación de la renovación[1] según corresponda. En todo caso, la activación de la renovación del licenciamiento no podrá ser retroactiva.
2	Suscripción al servicio de soporte de 1er nivel y mantenimiento de Fabrica ilimitado en modalidad para los siguientes equipos: • FORTIGATE FG-1100E S/N: FG10E0TB20900139. • FORTIGATE FG-1100E S/N: FG10E0TB20900161. • FORTIANALIZER FAZ-300G S/N: FAZ3HGTA24000646. • FORTIWEB FV-1000E S/N: FV-1KE4417900028. • FORTIWEB FV-1000E S/N: FV-1KE4417900031. • EMS - FCTEMS8825002644

[1] En todo caso no puede ser anterior la fecha de legalización del contrato correspondiente.

Informacion publica

	NOTA. El oferente será el encargado de prestar soporte de 1er nivel a la ANM y de escalar oficialmente a nombre de la ANM solicitudes a fabrica FORTINET.

7.7.2. CONDICIONES DE ASIGNACIÓN DEL LICENCIAMIENTO.

ITEM	ESPECIFICACIONES TECNICAS MÍNIMAS
1	Con la renovación del licenciamiento, se deberá realizar, de ser necesario, la actualización de firmware a la versión estable más reciente y aprobada por el fabricante, para los equipos relacionados en la presente ficha técnica.
2	En caso de ser necesario el contratista debe diseñar y ejecutar el plan más recomendado para instalación de la renovación del licenciamiento para la Entidad dando el soporte técnico adecuado con los niveles de servicio necesarios para el óptimo funcionamiento, y mitigar problemas que se puedan presentar por indisponibilidad durante la instalación.
3	El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que su personal, pueda atender las solicitudes de soporte y mantenimientos de la ANM.

7.7.3. TIEMPO DE RENOVACION DE LICENCIAMIENTO.

El tiempo de renovación será de doce (12) meses a partir de su activación, para lo siguiente:

Renovación licenciamientos y/o actualización de equipos Fortinet	Renovación licenciamientos y/o actualización productos Fortinet:	TIEMPO	UNIDAD
	- 2 NGFW Fortinet 1100E	12	MESES
	- 2 FortiWeb 1000E	12	MESES
	- 1 FortiAnalyzer 300G	12	MESES
	VPN/ZTNA 1700 End Points	12	MESES

7.8. ADQUISICIÓN DE PRODUCTO FORTISIEM de FORTINET:

La Agencia Nacional de Minería – ANM actualmente cuenta con un servicio de correlación y monitoreo de eventos de seguridad (SIEM) bajo la modalidad de Software como Servicio (SaaS), operado desde la infraestructura del proveedor. No obstante, como resultado del análisis de las necesidades tecnológicas y de ciberseguridad de la entidad, se identificó la necesidad de contar con una solución SIEM propia, implementada dentro de la infraestructura tecnológica de la ANM, con el fin de fortalecer la administración, control, disponibilidad y gestión de la información de seguridad.

Informacion publica

En consecuencia, mediante la presente contratación se contempla la adquisición, implementación y puesta en operación de una (1) solución SIEM virtualizada con capacidad para cincuenta (50) dispositivos, mil (1000) eventos por segundo (EPS), indicadores de compromiso (IOC) y soporte de fabricante, como parte integral de la operación del servicio SOC requerido por la entidad.

Al inicio de la ejecución del contrato, el proveedor deberá garantizar la continuidad del servicio SOC sobre la solución SIEM actualmente operada bajo la modalidad SaaS. El proveedor deberá implementar y poner en funcionamiento la nueva solución SIEM propia de la ANM, por lo que una vez esta sea puesta en funcionamiento dentro de la infraestructura tecnológica de la entidad, el proveedor deberá realizar las actividades de configuración, parametrización, integración y migración necesarias para garantizar la continuidad operativa del servicio sobre dicha plataforma.

Así mismo, el proveedor deberá realizar la configuración e integración de, por lo menos, las fuentes a correlacionar definidas en el numeral 7.2. del presente anexo técnico, efectuando el monitoreo continuo y garantizando la correcta operación, administración y disponibilidad de la plataforma SIEM durante toda la vigencia del contrato.

En todo caso, una vez la solución SIEM propia de la ANM entre en operación, el proveedor deberá garantizar sobre dicha plataforma la ejecución de las actividades de administración, configuración, integración, recolección, normalización, correlación y monitoreo de eventos de seguridad establecidas en el presente anexo técnico, siempre que estas resulten técnicamente aplicables a la solución implementada por la entidad.

8. INFRAESTRUCTURA ACTUAL

Para efectos de ilustrar a los oferentes a continuación, se describe de manera general la actual infraestructura de TI:

Informacion publica

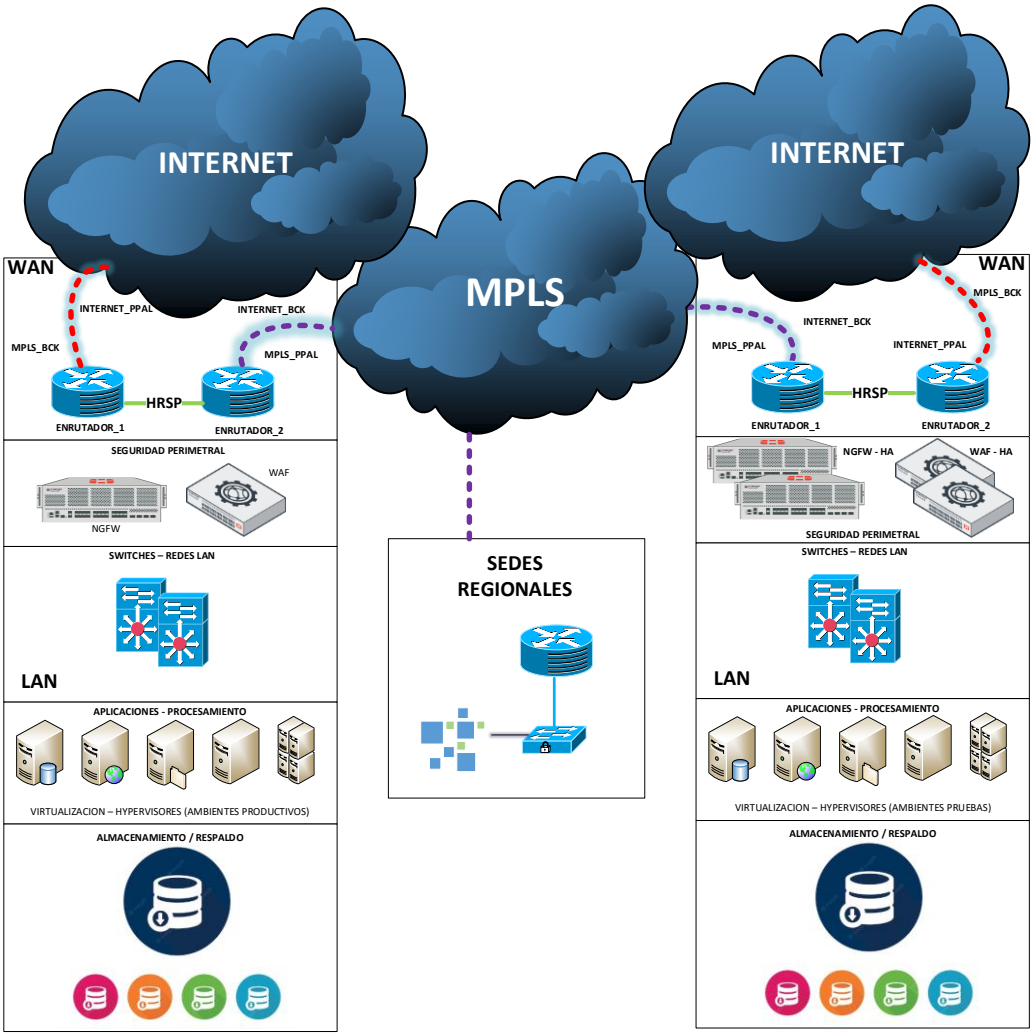

Figura 1. Arquitectura TI ANM en Alta Disponibilidad

a. INFRAESTRUCTURA

La infraestructura a la fecha está compuesta por: 30 servidores físicos, 250 servidores virtuales (Vmware) y 48 servidores Oracle VM, 65 Switches multimarca HPE, Cisco, Alcatel Lucent (Proceso de cambio), Alliend Telesis (Sistemas de CCTV), 2 Cisco SAN y Aruba.

b. SISTEMAS OPERATIVOS ESTACIÓN DE TRABAJO

Windows 8 profesional, 10 profesional, profesional 11 y Mac OS Aproximadamente 1.200 equipos

c. SISTEMAS OPERATIVOS SERVIDORES

Oracle Linux Enterprise

Informacion publica

Red Hat Enterprise Linux for Virtual Datacenters

Windows Server (Estándar y Datacenter), 2008, 2008 R2, 2012, 2012 R2. 2016,2019, 2022 y nuevas versiones liberadas por Microsoft

d. BASES DE DATOS

- MySQL
- SQL SERVER
- Oracle Database Enterprise Edition
- MongoDB
- Postgresql

e. FIREWALL Y EQUIPOS Y APLICACIONES DE SEGURIDAD INFORMÁTICA

- Dos (2) equipos (2) FortiGATE modelo FG-1100E, en alta disponibilidad
- Dos (2) FortiWEB modelo - 1000E, en alta disponibilidad
- Una (1) Suite MVISION Protect Plus EDR for Endpoint
- Una (1) equipo FortiAnalyzer modelo FAZ 200F
- Una (1) equipo FortiAnalyzer modelo FAZ 300Z

f. ALMACENAMIENTO

- Almacenamiento Principal Producción: 3PAR 8400, Conformado por:
  - 4 TiB Efectivos – Discos SSD
  - 45TiB efectivos – Discos SAS a 10K RPM
  - 239 TiB efectivos - discos NLSAS a 7.2K
  - Dos (2) Controladoras activo-activo
- Almacenamiento
  - 2 BladeSystem c7000 Enclosure G2
  - 4 switch SAN Enclosure HP
  - Cisco 8/24c SAN DS-C9132T-24PESK9
  - Switch LAN Enclosure HP
  - GbE2c Layer 2/3 Ethernet Blade Switch
  - PRIMERA (HIPERCONVERGENCIA CENTURY LINK)

g. SISTEMAS OPERATIVOS VIRTUALIZACIÓN

Informacion publica

- Vmware
- Ovm
- Kvm

h. SERVIDORES DE APLICACIÓN

- JBoss Enterprise Application Platform
- Tomcat
- IIS (Internet information Service)
- Weblogic
- Wildfly

i. PORTALES PÚBLICOS

Anna Mineria	https://annamineria.anm.gov.co/sigm/externalLogin
Aranda	https://solicitudesaranda.anm.gov.co
CMC (Catastro Minero Colombiano) - Consulta Web	http://www.cmc.gov.co
Invesflow	https://indexexpedientes.anm.gov.co/Invesflow/
Fiscaminero - Web	https://fiscaminero.anm.gov.co/fiscalizacion/
Formato Liviano	https://selenita.anm.gov.co
Isolución	https://isolucion.anm.gov.co
CMC (Catastro Minero Colombiano) - Nagios	http://nagios.anm.gov.co
Portal Web	https://www.anm.gov.co/
Portal ArcGIs	https://geo.anm.gov.co/
Certificado Registro Minero	https://selenita.anm.gov.co/
sisgestion	https://sisgestion.anm.gov.co/login.aspx
Trámites en Línea	https://tramites.anm.gov.co
WEBSAFI	https://saficontratos.anm.gov.co
Portal Inversionistas	https://mineriaencolombia.anm.gov.co/
Consulta Expediente Minero	https://consultadescargaexp.anm.gov.co
CMC	http://www.cmc.gov.co
ArcGis Enterprise	https://gisanm.anm.gov.co
Catálogo de Metadatos ANM	https://metadatos.anm.gov.co
PQRS	https://pqrs.anm.gov.co/
Tenan AZURE	(as- anm.azurewebsites.net) – Varios proyectos.
Entre Otros	

j. DATA CENTER CON TERCEROS

Informacion publica

La infraestructura que se tiene alojada en el Data Center externo es a través del acuerdo marco de precios NUBE PRIVADA está conformada por la siguiente plataforma:

Servicios:

- Implementación del sistema de información integral de gestión minera SIGMA
- Operación del BPM Área de Control a la Producción
- Operación del portal WEB de la entidad
- Operación del servicio de Mapas
- **EQUIPOS DE SEGURIDAD PERIMETRAL**

- NGFW Fortinet Modelo 1200D
- Fortinet Fortiweb 1000E
- Fortinet FAZ 400F

Los equipos de seguridad perimetral descritos en la figura 1. Deben ser tenidos en cuenta para integración con el sistema de correlación de eventos.

i. MICROSOFT / OFFICE 365

Brindar recomendaciones de buenas prácticas de seguridad para el correcto funcionamiento de los servicios Microsoft 365, asesoría para complementar reglas de cumplimiento y directivas de seguridad de la plataforma.

9. GARANTIA

ITEM	ESPECIFICACIONES TECNICAS MÍNIMAS	CUMPLIMIENTO
1	La garantía debe incluir todos los costos de operación, en los que debe contemplar mano de obra, transporte y los repuestos.	
2.	Las garantías deben ser implementadas durante el término de duración de la licencia y viceversa, deben ser originales y deben estar homologadas por el fabricante del equipo.	
3.	El proveedor, en los cuales que aplique, debe otorgar extensión de garantía directamente con el fabricante, para todos y cada una de las licencias.	
4	La solución SIEM ofertada deberá contar con garantía, soporte técnico y mantenimiento por parte del fabricante o canal autorizado, por el término de doce (12) meses, contados a partir de su puesta en operación, incluyendo acceso a actualizaciones, parches, correcciones, firmas, indicadores de compromiso (IOC), bases de conocimiento y demás componentes necesarios para garantizar la correcta operación, estabilidad y seguridad de la plataforma.	

10. TRANSFERENCIA TECNOLÓGICA

Informacion publica

El proponente que resulte adjudicatario de este proceso deberá realizar la transferencia tecnológica de conocimiento al personal de la Oficina de Tecnología e Información que sea designado para tal fin; en la administración de los servicios alcance del presente contrato.

11. DISPONIBILIDAD DE LOS SERVICIOS DE SEGURIDAD OFRECIDOS

Los servicios ofrecidos en el presente contrato deberán tener una disponibilidad del 99,6% mensual y las compensaciones por su no cumplimiento se aplicarán de acuerdo con la siguiente tabla:

RANGO % DISPONIBILIDAD		INDISPONIBILIDAD EN HORAS CALENDARIO	COMPENSACION SOBRE TARIFA MENSUAL
100	99.60	2.88	0%
99.59	98	14,4	5%
97.99	96	28,8	20%
95.99	90	72	50%
89.99	Menor que 89.99	Más de 72 Horas de Indisponibilidad al mes	100%

12. ACUERDOS DE NIVELES DE SERVICIO ANS

Los Acuerdos de Niveles de Servicio requeridos en la atención de los incidentes reportados al SOC, son:

PRIORIDAD	DESCRIPCIÓN	TIEMPO DE RESPUESTA SOC	TIEMPO MÁXIMO DE SOLUCIÓN
ALTA	Falla que afecte la disponibilidad de uno de los servicios tecnológicos de la ANM	Inmediato, Máximo 15 minutos	1 hora
MEDIA	Falla que afecte alguna de las funcionalidades del servicio	Máximo 1 hora	2 horas
BAJA	Reporte, consulta o solicitud que no afecte la prestación de los servicios tecnológicos	Máximo 12 horas	12 horas

Nota 1. No aplicarán deducciones ni penalizaciones sobre las métricas de disponibilidad si los retrasos se encuentran debidamente sustentados y son atribuibles a la falta de atención o gestión por parte del tercero responsable de la infraestructura física del Data Center. El contratista deberá remitir a la supervisión constancia documental de las solicitudes de cambio y tiempos de escalamiento presentados a dicho tercero.

13. LUGAR DE EJECUCIÓN

Informacion publica

El servicio deberá ser prestado en la Sede Central de la Entidad, en la ciudad e Bogotá en la Avenida Calle 26 No. 59-51, Torre 4 piso 9 Edificio Argos, o en el lugar que le sea comunicado por la Supervisión del Contrato.

CONOCEMOS, ACEPTAMOS Y CUMPLIMOS CON TODOS LOS REQUERIMIENTOS MÍNIMOS OBLIGATORIOS ESTABLECIDOS EN ESTE DOCUMENTO, LOS CUALES SE ENTIENDEN COMO OFERTA TÉCNICA MÍNIMA.

FIRMA DEL OFERENTE: _____

NOMBRE DEL OFERENTE: _____

NOMBRE DE LA EMPRESA OFERENTE: _____

Informacion publica