NECESIDAD	*La Agencia Nacional de Seguridad Vial – ANSV fue creada por la Ley 1702 de 2013, norma que en su artículo 3° establece que:* *"(…) tendrá como objeto la planificación, articulación y gestión de la seguridad vial del país. Será el soporte institucional y de coordinación para la ejecución, el seguimiento y el control de las estrategias, los planes y las acciones dirigidos a dar cumplimiento a los objetivos de las políticas de seguridad vial del Gobierno Nacional en todo el territorio nacional".* *El Decreto 787 de 2015 establece las funciones de la estructura interna de la ANSV y, en su artículo 12, consagra como funciones de la Secretaría General, entre otras, las siguientes:* *"(…) 11. Dirigir la identificación, el diseño y la implementación de soluciones tecnológicas acordes con las necesidades de la Agencia y velar por la operación, funcionalidad y seguridad de la información sistematizada. (…)".* *Así mismo, la Resolución 329 del 28 de junio de 2019, "Por la cual se establecen los Grupos Internos de Trabajo de la Secretaría General y se redistribuyen los mismos", señala en su artículo sexto, como funciones del Grupo de Tecnologías de la Información y de las Telecomunicaciones – GTIC, entre otras:* *1. Apoyar y prestar el soporte técnico que requieren las diferentes áreas de la ANSV para el procedimiento de la información, de acuerdo con las políticas establecidas en la materia.* *2. Proponer e implementar los mecanismos para el establecimiento de publicación y administración de la información.* *3. Apoyar los procesos informáticos de la ANSV y el mantenimiento de la base computacional y de telecomunicaciones.* *4.Implementar las políticas de seguridad informática y de telecomunicaciones de la ANSV.* *5. Verificar el adecuado cumplimiento de los requerimientos técnicos establecidos para el software, hardware y sistemas de comunicaciones, de forma que se ajusten a las necesidades de la ANSV y dentro de los estándares del mercado.* *6. Plantear a la Secretaría General planes, programas y proyectos en materia de tecnología de la información y comunicaciones que contribuyan a la gestión de la Entidad de conformidad con los lineamientos institucionales.* *En el marco de la estrategia de fortalecimiento tecnológico de la Agencia Nacional de Seguridad Vial (ANSV) y en cumplimiento de los lineamientos de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), el Marco de Referencia de Arquitectura Empresarial*

	(MRAE) y las políticas institucionales de gestión de tecnologías de la información y seguridad y privacidad de la información, la Entidad requiere adelantar la Fase II del proyecto de ciberseguridad institucional, orientada al fortalecimiento de las capacidades de prevención, detección, monitoreo, respuesta y gestión de incidentes de seguridad informática. *Actualmente, la ANSV cuenta con una infraestructura tecnológica y de seguridad basada en la arquitectura Fortinet Security Fabric como: Firewall, WAF, SIEM, SandBox, DDoS, NAC, entre otros y en un ecosistema de seguridad Microsoft de nivel empresarial, soportado bajo licenciamiento Microsoft 365 E5 en la totalidad de la entidad. Este licenciamiento habilita de forma nativa Microsoft Defender XDR con sus módulos de Defender for Endpoint Plan 2, Defender for Office 365 Plan 2, Defender for Cloud Apps y Defender for Identity, así como Microsoft Entra ID P2 con Conditional Access, Identity Protection y Privileged Identity Management (PIM), y Microsoft Purview con capacidades avanzadas de prevención de fuga de información (DLP), clasificación mediante etiquetas de sensibilidad, gestión del ciclo de vida documental, Insider Risk Management y eDiscovery. A esto se suma Microsoft Intune para la administración centralizada y el cumplimiento de más de 700 dispositivos corporativos. Este ecosistema, ampliamente utilizado por la entidad desde hace varios años, ha permitido consolidar una postura de seguridad robusta y alineada con los estándares de gobierno digital vigentes,* *Durante la vigencia 2025 la ANSV ejecutó la Fase I del fortalecimiento de ciberseguridad institucional, mediante la adquisición e implementación de controles orientados principalmente a la protección perimetral, administración centralizada de la infraestructura Fortinet, autenticación multifactor para accesos remotos, gestión de accesos privilegiados (PAM), análisis continuo de vulnerabilidades, protección de riesgos digitales externos (Digital Risk Protection) y fortalecimiento de las capacidades de correlación mediante FortiAnalyzer IoC. Dichas capacidades permitieron incrementar significativamente los controles preventivos de la entidad; sin embargo, el ecosistema tecnológico continúa presentando brechas relacionadas con la automatización de la respuesta, la detección avanzada basada en comportamiento, la protección de accesos bajo principios Zero Trust y la operación especializada de monitoreo 7x24.* *En este contexto, el proyecto contempla el suministro, implementación, integración, configuración, puesta en operación, soporte y mantenimiento de una solución integral de ciberseguridad compuesta por seis (6) componentes complementarios.* *El primer componente corresponde a una Plataforma de Orquestación, Automatización y Respuesta (SOAR), orientada a centralizar la gestión de incidentes de seguridad, automatizar flujos de atención y optimizar los tiempos de respuesta mediante procesos estandarizados e integrados con las herramientas de seguridad existentes. Actualmente la Agencia Nacional de Seguridad Vial dispone de una plataforma institucional para la correlación y monitoreo de eventos de seguridad basada en FortiSIEM, complementada con un servicio de monitoreo especializado que realiza la supervisión*

	permanente de los eventos de seguridad y genera las alertas correspondientes hacia el equipo de tecnología de la Entidad. *No obstante, una vez se genera una alerta de seguridad, las actividades de análisis inicial, apertura de incidentes, notificación, recopilación de evidencias, ejecución de acciones de contención y seguimiento continúan desarrollándose de manera manual, dependiendo de la intervención del personal técnico de la Entidad.* *Este modelo incrementa los tiempos de respuesta frente a incidentes de seguridad, aumenta la probabilidad de errores operativos y dificulta la aplicación homogénea de los procedimientos establecidos para la atención de incidentes, especialmente en eventos de alta criticidad o que requieren la ejecución coordinada de múltiples acciones sobre diferentes plataformas tecnológicas.* *Adicionalmente, la incorporación de nuevos componentes tecnológicos como Microsoft Defender XDR, NDR y Deception incrementará el volumen de eventos que deberán ser gestionados por la Entidad, haciendo necesario contar con mecanismos que permitan automatizar los procesos operativos asociados a la respuesta frente a incidentes.* *Por lo anterior, se requiere implementar una plataforma* ***Security Orchestration, Automation and Response (SOAR)*** *que permita integrar las diferentes soluciones de seguridad existentes en la ANSV, automatizar los flujos de respuesta mediante playbooks previamente definidos, enriquecer automáticamente los eventos de seguridad, gestionar casos de manera centralizada y ejecutar acciones de contención sobre las diferentes plataformas tecnológicas, reduciendo los tiempos de respuesta y fortaleciendo la capacidad operativa del proceso institucional de gestión de incidentes de seguridad de la información.* *Como segundo componente, se requiere una Plataforma SASE con capacidades ZTNA (Zero Trust Network Access), destinada a fortalecer el acceso seguro a aplicaciones y recursos institucionales bajo un modelo de confianza cero. La entidad actualmente utiliza mecanismos tradicionales de acceso remoto (VPN), los cuales fueron fortalecidos mediante MFA durante la Fase I; sin embargo, dichos mecanismos continúan otorgando acceso basado en red y no en identidad ni contexto.* *La implementación de ZTNA permitirá:* • *acceso por aplicación* • *mínimo privilegio* • *gestión de identidad* • *mejorar posturas de seguridad* • *controles a nivel de geolocalización* • *cumplimiento del modelo Zero Trust.* *El tercer componente corresponde a un Servicio Gestionado de Detección y Respuesta (MDR), enfocado en el monitoreo especializado, la identificación*

	temprana de amenazas y la atención de incidentes de seguridad de manera continua. La Agencia Nacional de Seguridad Vial cuenta actualmente con un servicio de monitoreo continuo de eventos de seguridad soportado sobre la plataforma FortiSIEM, mediante el cual se supervisan permanentemente los registros generados por la infraestructura tecnológica institucional y se notifican oportunamente las alertas identificadas. *Si bien este esquema permite disponer de monitoreo continuo y generación de alertas, la atención de incidentes continúa dependiendo de la capacidad operativa del personal técnico de la Entidad para realizar investigaciones especializadas, validar indicadores de compromiso, determinar el alcance real de los incidentes, efectuar actividades de búsqueda proactiva de amenazas (Threat Hunting), analizar campañas activas de ciberataques y apoyar técnicamente los procesos de contención y recuperación.* *Asimismo, el crecimiento del ecosistema tecnológico institucional, la incorporación de nuevas soluciones de seguridad, la integración de Microsoft Defender XDR y la evolución permanente de las amenazas cibernéticas hacen necesario fortalecer las capacidades especializadas de detección e investigación más allá del monitoreo tradicional de eventos.* *En este contexto, se requiere implementar un servicio de **Managed Detection and Response (MDR)** para toda la infraestructura tecnológica de la ANSV, que complemente las actividades actualmente desarrolladas por el servicio de monitoreo existente mediante capacidades avanzadas de investigación de incidentes, inteligencia de amenazas, búsqueda proactiva de actividades maliciosas, análisis especializado de indicadores de compromiso, acompañamiento técnico durante incidentes de alta criticidad y apoyo experto en la toma de decisiones para la contención y recuperación de los servicios institucionales.* *El servicio MDR deberá realizar el monitoreo, análisis, investigación y respuesta sobre los eventos e incidentes de seguridad generados por la totalidad de la infraestructura tecnológica de la ANSV, integrando la telemetría proveniente de Microsoft Defender XDR, FortiSIEM, FortiAnalyzer, FortiGate, la solución NDR, la plataforma Deception, Active Directory, Microsoft Entra ID, Microsoft 365, servicios en nube y demás fuentes de información definidas por la Entidad, evitando la duplicidad de funciones y fortaleciendo el modelo institucional de operación de ciberseguridad.* *La solución deberá incorporar capacidades de Threat Intelligence que permitan enriquecer los indicadores de compromiso (IOC), identificar campañas activas, actores de amenaza, TTP asociados al marco MITRE ATT&CK y generar recomendaciones de mitigación para la Entidad.* *El proveedor deberá realizar actividades periódicas de Threat Hunting proactivo sobre la información recolectada por las plataformas de seguridad, utilizando hipótesis de compromiso, indicadores de amenaza, comportamientos anómalos y técnicas basadas en MITRE ATT&CK.*

	El servicio MDR deberá administrar el ciclo de vida completo de los incidentes de seguridad mediante una plataforma de gestión de casos (Case Management), permitiendo la trazabilidad de las investigaciones, evidencias, actividades ejecutadas, tiempos de atención y generación de informes. *Con el fin de optimizar los procesos de monitoreo, investigación, análisis y respuesta ante incidentes de seguridad, el proveedor del servicio MDR deberá incorporar capacidades de Inteligencia Artificial Generativa y/o Machine Learning como apoyo a la operación del Centro de Operaciones de Seguridad (SOC).* *Las capacidades de Inteligencia Artificial deberán utilizarse como mecanismo de apoyo para los analistas del SOC y en ningún caso reemplazarán la validación técnica realizada por el personal especializado del proveedor.* *La solución propuesta deberá incluir, como mínimo, las siguientes capacidades:* • *Apoyar el análisis y priorización de alertas de seguridad, reduciendo falsos positivos y facilitando la identificación de incidentes reales.* • *Generar resúmenes ejecutivos y técnicos de los incidentes de seguridad investigados, utilizando lenguaje natural.* • *Asistir a los analistas durante las investigaciones mediante el análisis contextual de eventos, indicadores de compromiso (IOC), tácticas, técnicas y procedimientos (TTP) asociados al marco MITRE ATT&CK.* • *Proporcionar recomendaciones técnicas para la contención, erradicación y recuperación de incidentes, indicando las acciones sugeridas para reducir el impacto sobre la infraestructura tecnológica.* • *Facilitar consultas en lenguaje natural sobre eventos de seguridad, incidentes, activos comprometidos, usuarios involucrados e indicadores de compromiso, cuando la plataforma utilizada por el proveedor disponga de dicha funcionalidad.* • *Apoyar las actividades de Threat Hunting mediante la identificación de comportamientos anómalos, correlaciones no evidentes e indicadores asociados a amenazas emergentes.* • *Generar explicaciones técnicas de las cadenas de ataque detectadas, facilitando el análisis de causa raíz y la comprensión del incidente por parte de la ANSV.* • *Apoyar la elaboración de informes técnicos y ejecutivos derivados de las investigaciones realizadas por el servicio MDR.* • *Analizar la información proveniente de las diferentes fuentes de telemetría (SIEM, XDR, NDR, Deception, Firewall, Active Directory y demás soluciones de seguridad integradas), generando contexto adicional para la toma de decisiones.* *Incorporar capacidades de aprendizaje continuo basadas en inteligencia de amenazas y nuevas técnicas de ataque, contribuyendo al fortalecimiento permanente de la capacidad de detección.El proveedor deberá garantizar que la información procesada mediante las capacidades de Inteligencia*

	Artificial utilizadas durante la prestación del servicio MDR no será utilizada para el entrenamiento de modelos públicos, ni compartida con terceros diferentes a la ANSV, salvo autorización expresa de la Entidad. Asimismo, deberá implementar mecanismos que garanticen la confidencialidad, integridad y protección de la información institucional procesada por dichas capacidades. *De igual manera, el proyecto contempla como:* *cuarto componente una Plataforma de Decepción (Deception), diseñada para detectar de forma temprana comportamientos maliciosos mediante activos señuelo, Actualmente la ANSV dispone de controles preventivos y de detección basados en firmas, comportamiento, correlación de eventos y análisis de vulnerabilidades. Sin embargo, estas soluciones actúan principalmente sobre activos productivos y generan alertas cuando un comportamiento anómalo ya ha comenzado a afectar infraestructura o usuarios.* *La implementación de una plataforma de Deception incorpora una estrategia de defensa activa basada en activos señuelo (decoys), credenciales falsas y servicios simulados distribuidos estratégicamente dentro de la infraestructura tecnológica.* *Estos activos no son utilizados durante la operación normal de la entidad; por lo tanto, cualquier intento de acceso, reconocimiento, autenticación o interacción constituye un indicador de compromiso con una probabilidad extremadamente baja de falsos positivos.* *La solución permitirá:* • *detectar movimientos laterales* • *detectar reconocimiento interno* • *identificar uso indebido de credenciales comprometidas* • *detectar atacantes antes de que alcancen activos críticos* • *enriquecer automáticamente la investigación realizada por el SIEM y el SOAR* • *mejorar la capacidad de respuesta frente a amenazas persistentes (APT).* *Esta plataforma debe permitir la integración con:* • *FortiSIEM* • *SOAR* • *Active Directory* • *Defender XDR* *Como quinto componente, se requiere una Plataforma de Detección y Respuesta en Red (NDR), orientada a proporcionar visibilidad y análisis avanzado del tráfico de red para identificar amenazas y anomalías. Actualmente la ANSV cuenta con mecanismos de protección perimetral y correlación de eventos que permiten detectar incidentes basados en registros generados por dispositivos y aplicaciones.*

	No obstante, estas soluciones presentan limitaciones para identificar amenazas cuyo comportamiento únicamente puede observarse mediante el análisis continuo del tráfico de red, especialmente en escenarios donde el atacante realiza movimientos laterales, comunicaciones con servidores de comando y control (C2), técnicas de evasión o actividades de exfiltración utilizando protocolos legítimos. *La plataforma NDR permitirá incorporar capacidades avanzadas de análisis de comportamiento del tráfico de red mediante inteligencia artificial y modelos de comportamiento, fortaleciendo la detección temprana de amenazas avanzadas que actualmente pueden pasar inadvertidas.* *Esta plataforma debe integrarse con:* • *FortiGate* • *FortiAnalyzer* • *FortiSIEM* • *SOAR* • *Microsoft Defender* *Finalmente, como sexto componente, se contempla la habilitación de FortiAI sobre la plataforma FortiAnalyzer existente, incorporando capacidades de inteligencia artificial generativa para apoyar las actividades de monitoreo, investigación, correlación de eventos y generación de reportes de seguridad. Actualmente el análisis de incidentes de seguridad requiere que los analistas consulten múltiples fuentes de información, correlacionen eventos, interpreten registros técnicos y elaboren manualmente reportes e informes de investigación.* *La incorporación de capacidades de inteligencia artificial sobre la plataforma FortiAnalyzer permitirá asistir dichas actividades mediante mecanismos de análisis contextual, resumen automatizado de incidentes, explicación de eventos, priorización de alertas y generación asistida de reportes técnicos.* *La solución no reemplaza las funciones de los analistas de seguridad, sino que incrementa su productividad, reduce los tiempos de investigación y mejora la capacidad de respuesta frente a incidentes de seguridad.* ***Arquitectura objetivo e integración de la solución*** *Con el fin de garantizar el aprovechamiento de las inversiones previamente realizadas por la Agencia Nacional de Seguridad Vial, evitar la duplicidad de funcionalidades y consolidar una operación unificada de ciberseguridad, las soluciones objeto del presente proceso deberán integrarse con la arquitectura de seguridad actualmente implementada por la Entidad.* *La arquitectura objetivo estará basada en un modelo de defensa en profundidad, donde cada componente cumpla un rol específico dentro del ciclo de prevención, detección, correlación, orquestación y respuesta a incidentes de seguridad, evitando la coexistencia de plataformas con funciones redundantes o independientes.*

	La arquitectura objetivo deberá soportar un modelo de operación basado en capacidades de Managed Detection and Response (MDR), donde el proveedor adjudicatario realice el monitoreo continuo, la detección avanzada, la investigación, la cacería de amenazas (Threat Hunting), la priorización de alertas, la respuesta coordinada a incidentes y la generación de inteligencia de amenazas, aprovechando las capacidades tecnológicas existentes en la ANSV. *En este modelo, FortiSIEM continuará desempeñando el rol de plataforma institucional de gestión y correlación de eventos de seguridad (SIEM), consolidando la telemetría proveniente de las diferentes soluciones tecnológicas. El servicio MDR deberá consumir esta información para realizar los procesos de análisis especializado, investigación y gestión de incidentes.* *La plataforma SOAR constituirá el componente central de orquestación y automatización de la respuesta ante incidentes de seguridad, integrando la información generada por FortiSIEM y por las demás soluciones tecnológicas implementadas, ejecutando flujos automatizados de atención, enriquecimiento de eventos, apertura de casos, generación de evidencias y coordinación de actividades de respuesta.* *El servicio MDR constituirá el componente central de monitoreo, investigación y operación de ciberseguridad de la ANSV, integrando las capacidades de monitoreo continuo 24x7, análisis especializado, correlación avanzada, threat hunting, inteligencia de amenazas, investigación de incidentes, clasificación de alertas y coordinación de las acciones de respuesta.* *El proveedor MDR deberá consumir la información proveniente de FortiSIEM, Microsoft Defender XDR, NDR, Deception, FortiAnalyzer, Active Directory y demás fuentes de telemetría definidas por la Entidad. Microsoft Defender XDR continuará proporcionando las capacidades de protección de endpoints, identidades, correo electrónico, aplicaciones y Microsoft 365. El servicio MDR deberá consumir las alertas e incidentes generados por Defender XDR y, cuando la Entidad lo autorice, ejecutar acciones de contención y respuesta utilizando sus capacidades nativas.* *El servicio MDR deberá realizar actividades de ingeniería de detecciones (Detection Engineering), ajustando y optimizando permanentemente las reglas de detección, casos de uso y mecanismos de correlación sobre FortiSIEM y Microsoft Defender XDR, con el fin de reducir falsos positivos y mejorar la capacidad de identificación temprana de amenazas.* *El servicio MDR deberá validar, investigar y priorizar las alertas antes de escalar incidentes a la ANSV, disminuyendo falsos positivos y garantizando tiempos de respuesta acordes con los SLA establecidos con una disponibilidad 24*7*365.*

	La solución NDR deberá integrarse con la infraestructura de red institucional para proporcionar capacidades avanzadas de análisis del tráfico, detección de movimientos laterales, comunicaciones con infraestructura maliciosa, actividades de comando y control, exfiltración de información y demás comportamientos anómalos que no puedan ser identificados únicamente mediante registros de eventos. Los eventos generados por la plataforma NDR deberán ser enviados hacia FortiSIEM y posteriormente consumidos por la plataforma SOAR para su correlación, priorización y automatización de la respuesta. *La plataforma de Deception deberá integrarse con Active Directory, segmentos de red y demás componentes tecnológicos definidos por la Entidad, generando alertas de alta confiabilidad cuando se detecten intentos de reconocimiento, autenticación o interacción sobre activos señuelo. Dichas alertas deberán ser enviadas a FortiSIEM para su correlación y posteriormente gestionadas mediante la plataforma SOAR.* *Las capacidades de FortiAI deberán operar sobre la plataforma FortiAnalyzer existente, apoyando los procesos de análisis de incidentes, investigación, correlación de eventos y generación de reportes técnicos, sin reemplazar las funciones propias del SIEM ni de la plataforma SOAR.* *Todas las soluciones deberán integrarse mediante interfaces, API o mecanismos soportados por los fabricantes, evitando procesos manuales de intercambio de información y garantizando la interoperabilidad entre las diferentes plataformas de seguridad implementadas por la Entidad.* *La siguiente es una imagen de la arquitectura establecida por la ANSV, sin embargo, esta puede ser modificada según requerimientos:*

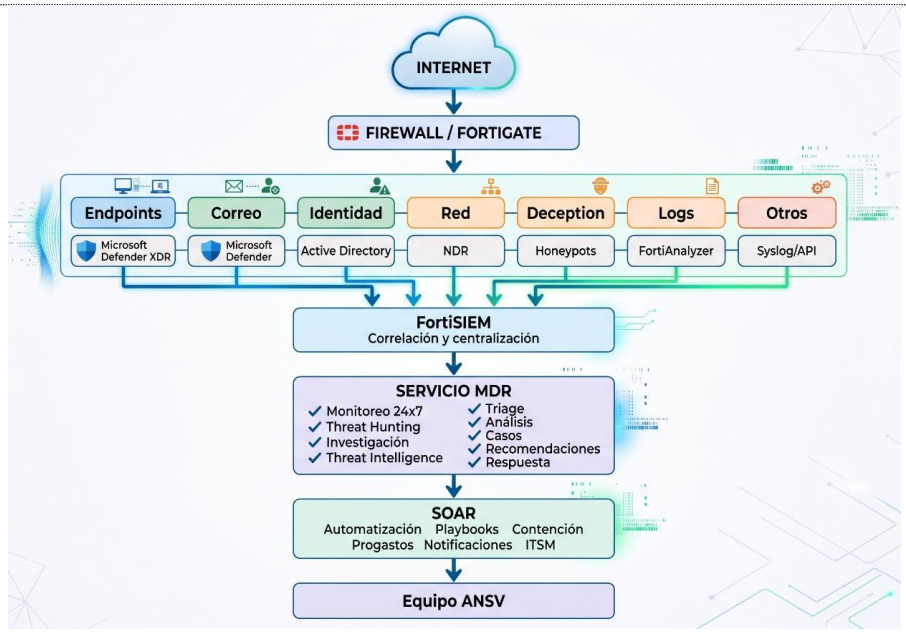


Ilustración 1 - Propuesta de Arquitectura

Requerimientos específicos de integración

Integración con FortiSIEM

El contratista deberá garantizar que las soluciones ofertadas permitan el envío de eventos, alertas y metadatos hacia la plataforma FortiSIEM actualmente implementada por la ANSV, utilizando conectores soportados por el fabricante, Syslog, API REST, STIX/TAXII u otros mecanismos estándares de integración.

Integración con FortiAnalyzer

Las soluciones deberán aprovechar la información disponible en FortiAnalyzer para enriquecer los procesos de investigación y correlación de eventos, evitando la duplicidad de repositorios de registros de auditoría.

Integración con Microsoft Defender XDR

La solución deberá consumir y/o intercambiar eventos, alertas e indicadores de compromiso provenientes de Microsoft Defender XDR, permitiendo la ejecución automatizada de acciones de respuesta cuando estas sean autorizadas por la Entidad.

Integración con Active Directory

	La solución deberá integrarse con Microsoft Active Directory para enriquecer la información asociada a usuarios, grupos, equipos y credenciales durante la investigación de incidentes. ***Integración con el sistema de gestión de incidentes*** *La plataforma SOAR deberá permitir la integración con la herramienta institucional de gestión de incidentes (mesa de servicios o ITSM) para la creación automática de casos, seguimiento, cierre y trazabilidad de las actividades ejecutadas.* *El proponente deberá presentar dentro de su oferta la arquitectura detallada de integración de la solución, identificando los componentes existentes de la ANSV, los mecanismos de interoperabilidad, los conectores utilizados, el flujo de eventos entre plataformas y las acciones automatizadas que serán ejecutadas por la plataforma SOAR. La solución deberá garantizar la interoperabilidad con la infraestructura Fortinet existente (FortiSIEM, FortiAnalyzer, FortiGate y demás componentes), así como con Microsoft Defender XDR, evitando la duplicidad de funcionalidades y preservando a FortiSIEM como la plataforma institucional de correlación de eventos de seguridad.* *Todas las soluciones objeto del presente proceso deberán integrarse con la infraestructura de seguridad actualmente implementada por la ANSV, preservando la arquitectura institucional basada en FortiSIEM como plataforma central de correlación de eventos. Ningún componente podrá operar de manera independiente o generar islas de información. Los eventos, indicadores de compromiso, casos de seguridad y acciones de respuesta deberán intercambiarse mediante mecanismos de integración soportados por los fabricantes (API, Syslog, STIX/TAXII u otros estándares), garantizando la interoperabilidad entre FortiSIEM, FortiAnalyzer, Microsoft Defender XDR, FortiGate, Active Directory, Microsoft 365, NDR, Deception, SOAR y el servicio MDR.* *La arquitectura propuesta deberá preservar las inversiones existentes realizadas por la ANSV, garantizando la interoperabilidad con FortiSIEM, FortiAnalyzer, Microsoft Defender XDR, FortiGate, Active Directory y demás componentes de seguridad existentes, evitando la duplicidad de funcionalidades y permitiendo que el servicio MDR consolide la operación de monitoreo, investigación, threat hunting, inteligencia y respuesta ante incidentes sobre una arquitectura integrada.* ***SERVICIOS ESPECIALIZADOS*** ***Servicio de Soporte Técnico Especializado*** *El contratista deberá prestar soporte técnico especializado para todos los componentes suministrados e implementados dentro de la solución integral de ciberseguridad, incluyendo como mínimo las plataformas SOAR, SASE*

con capacidades ZTNA, NDR, Deception, FortiAI y demás elementos asociados, durante toda la vigencia contractual.
*El servicio deberá prestarse bajo un esquema de atención **24x7x365**, contemplando atención remota y, cuando sea requerido por la ANSV, atención en sitio para la solución de incidentes o actividades de soporte especializado.*
La gestión de incidentes deberá realizarse mediante herramientas formales de atención de casos, garantizando la trazabilidad completa de cada solicitud por medio de un número de radicado o ticket.

Los tiempos máximos de atención deberán ser:

Severidad	***Tiempo máximo de atención***
Crítico	*30 minutos*
Alto	*1 hora*
Medio	*6 horas*
Bajo	*12 horas*

Clasificación de severidad

Nivel	***Descripción***
Crítico	*Interrupción total de una o varias capacidades de ciberseguridad que afecten la detección, monitoreo, respuesta a incidentes o el acceso seguro a recursos institucionales.*
Alto	*Afectación significativa de funcionalidades críticas sin generar indisponibilidad total de la solución.*
Medio	*Problemas funcionales o de configuración que no comprometen la operación principal de los servicios.*
Bajo	*Consultas técnicas, actividades preventivas, requerimientos menores o solicitudes de información.*

El soporte incluirá:

- *Diagnóstico y solución de incidentes.*
- *Escalamiento hacia fabricante cuando sea requerido.*
- *Gestión de garantías y reemplazo de componentes defectuosos sin costo adicional para la Entidad.*
- *Acompañamiento técnico para actividades de actualización, ajustes y optimización de la solución.*
- *Soporte sobre integraciones con FortiSIEM, FortiAnalyzer, Microsoft Defender XDR, Active Directory, Microsoft 365 y demás componentes tecnológicos definidos por la ANSV.*

Transferencia de Conocimiento

	Con el fin de fortalecer las capacidades técnicas del Grupo TIC de la ANSV y garantizar la sostenibilidad operativa de la solución implementada, el contratista deberá realizar actividades de transferencia de conocimiento dirigidas al personal técnico de la Entidad. *La transferencia deberá contemplar como mínimo:* • *Participación de cinco (5) funcionarios o contratistas designados por la ANSV.* • *Duración mínima de cuarenta (40) horas.* • *Modalidad teórico-práctica.* • *Entrega de material técnico de consulta.* *Los contenidos deberán cubrir, como mínimo:* • *Administración y operación de la plataforma SOAR.* • *Operación y gestión del servicio MDR.* • *Administración de la solución SASE-ZTNA.* • *Gestión de la plataforma NDR.* • *Administración y monitoreo de la solución Deception.* • *Capacidades de FortiAI y FortiAnalyzer.* • *Procesos de gestión de incidentes e integración con FortiSIEM y Microsoft Defender XDR.* • *Mejores prácticas de operación y respuesta a incidentes basadas en marcos de referencia como MITRE ATT&CK, NIST e ISO/IEC 27001.*
	Bolsa de Horas de Especialista en Ciberseguridad *El contratista deberá suministrar una bolsa de hasta veinte (20) horas anuales de servicios especializados en ciberseguridad, independientes de las actividades de soporte, MDR, implementación y transferencia de conocimiento.* *Estas horas podrán ser utilizadas por la ANSV para:* • *Consultoría técnica especializada.* • *Definición y optimización de casos de uso de seguridad.* • *Ajuste de reglas de correlación y detección.* • *Apoyo en actividades de threat hunting.* • *Revisión de arquitecturas de seguridad.* • *Optimización de integraciones entre plataformas.* • *Recomendaciones para fortalecimiento de controles de seguridad.* • *Asesoría relacionada con marcos de referencia NIST, ISO/IEC 27001, Zero Trust y MITRE ATT&CK.* *El propósito de esta bolsa de horas será apoyar el fortalecimiento continuo de la postura de ciberseguridad institucional y optimizar la operación de las plataformas adquiridas.*
	Servicios de Implementación e Integración

	El contratista deberá ejecutar las actividades necesarias para el suministro, instalación, configuración, integración, parametrización, pruebas, puesta en operación y estabilización de todos los componentes de la solución de ciberseguridad adquirida. ***Implementación Plataforma SOAR*** • *Instalación y configuración de la plataforma.* • *Creación y parametrización de playbooks de respuesta.* • *Integración con FortiSIEM, FortiAnalyzer, Microsoft Defender XDR, Active Directory y demás plataformas definidas por la ANSV.* • *Configuración de gestión centralizada de casos.* • *Pruebas funcionales y de integración.* • *Documentación técnica y transferencia de conocimiento.* ***Implementación Plataforma SASE con capacidades ZTNA*** • *Configuración de acceso seguro basado en identidad y contexto.* • *Integración con Microsoft Entra ID y mecanismos de autenticación de la Entidad.* • *Configuración de políticas Zero Trust.* • *Pruebas de acceso y validación funcional.* • *Documentación y puesta en operación.* ***Implementación Servicio MDR*** • *Configuración de fuentes de telemetría.* • *Integración con FortiSIEM, Microsoft Defender XDR, NDR, Deception, FortiAnalyzer y demás componentes definidos por la Entidad.* • *Parametrización de casos de uso de detección.* • *Habilitación de procesos de threat hunting e inteligencia de amenazas.* • *Definición de procedimientos de escalamiento y respuesta.* ***Implementación Plataforma Deception*** • *Diseño de la arquitectura de activos señuelo.* • *Despliegue de decoys, credenciales señuelo y servicios simulados.* • *Integración con FortiSIEM y plataforma SOAR.* • *Validación de escenarios de detección.* ***Implementación Plataforma NDR*** • *Despliegue y configuración de sensores.* • *Integración con infraestructura de red institucional.* • *Configuración de modelos de detección.* • *Integración con FortiSIEM y SOAR.*

	• *Validación de capacidades de detección de amenazas.* ***Habilitación FortiAI sobre FortiAnalyzer*** • *Activación y configuración de capacidades de inteligencia artificial.* • *Integración con los procesos de análisis e investigación de incidentes.* • *Validación de generación de reportes y análisis asistido.* • *Capacitación orientada a administradores y analistas de seguridad.* ***Entregables mínimos*** • *Documento de arquitectura implementada.* • *Documento de integración entre plataformas.* • *Planes y resultados de pruebas.* • *Manuales de administración y operación.* • *Informe final de implementación.* • *Acta de puesta en operación y estabilización.*
OBJETO (Alcance si aplica)	*Contratar la implementación, fortalecimiento y operación de la estrategia de ciberseguridad para la protección de la infraestructura crítica y datos de la agencia.stg-110* ***Alcance General*** *Contratar el suministro, implementación, integración, configuración, puesta en operación, soporte y mantenimiento de una solución integral de ciberseguridad para la Agencia Nacional de Seguridad Vial (ANSV), orientada a fortalecer las capacidades de prevención, detección, monitoreo y respuesta ante incidentes de seguridad de la información. La solución comprende la implementación de una plataforma SOAR, una plataforma SASE con capacidades ZTNA, servicios MDR con capacidades de Inteligencia Artificial Generativa para apoyar las actividades de monitoreo, investigación, análisis y respuesta ante incidentes., una plataforma de Deception, una plataforma NDR y capacidades de inteligencia artificial FortiAI sobre FortiAnalyzer,. Asimismo, incluye las actividades de diseño, instalación, integración, pruebas, documentación, transferencia de conocimiento y acompañamiento técnico necesarias para su correcta operación e integración con la arquitectura tecnológica actual de la entidad.*
PLAZO DE EJECUCIÓN	*El plazo de ejecución del contrato será de hasta veinticuatro (24) meses, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución contractual y de la suscripción del acta de inicio. Durante este período, el contratista deberá ejecutar todas las actividades requeridas para el cumplimiento del objeto contractual, incluyendo el suministro, implementación, integración, configuración, parametrización, pruebas, puesta en operación, estabilización, soporte técnico especializado, mantenimiento, transferencia de conocimiento y acompañamiento técnico de las soluciones de ciberseguridad adquiridas.*

	Asimismo, deberá garantizar la correcta operación e integración de los componentes de la solución con la infraestructura tecnológica existente de la Agencia Nacional de Seguridad Vial (ANSV), así como la prestación de los servicios asociados, la renovación de licenciamiento y la disponibilidad de soporte del fabricante durante la vigencia contractual, de conformidad con las condiciones técnicas definidas en la ficha técnica y los demás documentos que hacen parte integral del proceso.
GARANTÍA (si aplica)	*El plazo de ejecución del contrato será de dos (2) años, contado a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento y ejecución.* *Para garantizar el cumplimiento del CONTRATO por parte del CONTRATISTA, deberá constituir una garantía la cual avalará el cumplimiento de las obligaciones surgidas del contrato, a favor del PATRIMONIO AUTONOMO- FONDO DE SEGURIDAD VIAL, identificado con NIT. 830.053.630-9, expedida por una compañía de seguros o entidad bancaria legalmente autorizada para ello, con el finde respaldar todas las obligaciones que surjan del mismo, con los siguientes amparos:* **15.2. Garantía de Cumplimiento a favor de las Entidades Compradoras** Los Proveedores deben constituir una garantía de cumplimiento dentro de los **tres (3) días hábiles** siguientes a la colocación de la Orden de Compra a favor de la Entidad Compradora, por el valor, amparos y vigencia establecidos en la siguiente tabla:

AMPARO	SUFICIENCIA	VIGENCIA
Cumplimiento del contrato	10 % de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.
Calidad y correcto funcionamiento de los bienes	10 % de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.
Calidad del servicio	10 % de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5% del Valor de la Orden de Compra	Duración de la Orden de Compra y (3) tres años más

ALCANCE TÉCNICO	*Ver: Documento Condiciones técnicas básicas obligatorias VF*

Cordialmente,

JUAN ANDRES COLLAZOS L. Firmado digitalmente por JUAN ANDRES COLLAZOS L.

JUAN ANDRES COLLAZOS LAMILLA
ASESOR CÓDIGO 1020 GRADO 16 DEL GRUPO DE TIC

Proyectó: Diego Armando Narvaez Buchely - **contratista del Grupo Tics**
Diana Lorena Sánchez- contratista del Grupo Tics