DIAN - DIRECCION DE IMPUESTOS Y ADUANAS NACIONALES

ANEXO CARACTERÍSTICAS TÉCNICAS MÍNIMAS (FICHA TÉCNICA)

Objeto: "Contratar la adquisición, instalación, configuración e implementación de un Centro de Operaciones de Seguridad - SOC, para la DIAN - Dirección de Impuestos y Aduanas Nacionales".

Ítem	Mínimo Exigido por la DIAN	CUMPLE/ NO CUMPLE
1	Descripción General y Requerimientos para la DIAN	
1.1	<p>La Dian requiere adquirir, instalar, configurar e implementar un Centro de Operaciones de Seguridad - SOC, el cual debe constar como mínimo de los siguientes componentes y servicios:</p> <ol style="list-style-type: none"> SIEM - Correlacionador de Eventos (Ver características en el ítem 2). FISICO 25000 SOAR - Orquestación, automatización y respuesta de seguridad) (Ver características en el ítem 3). VIRTUAL Herramienta de protección de bases de datos (Ver características en el ítem 4). Virtual SaaS Monitoreo a la Gestión de Vulnerabilidades (Ver características en el ítem 5). SaaS Caza de amenazas (Ver características en el ítem 6). FISICO NDR - Detección y respuesta en red e Inteligencia de amenazas (Ver características en el ítem 7). FISICO Solución de análisis de código estático y dinámico para aplicaciones (Ver características en el ítem 8). SaaS Protección de marca (Ver características en el ítem 9). SaaS Ethical hacking (Ver características en el ítem 10). Servicio Implementación de toda la plataforma y los dispositivos adquiridos (Ver características en el ítem 11). Servicios de Monitoreo (Ver características en el ítem 12). Garantía y Soporte técnico de tres (3) años (Ver características en el ítem 13). Capacitación (Ver características en el ítem 14). Transferencia de Conocimiento (Ver características en el ítem 15). Documentación (Ver características en el ítem 16). Equipo Mínimo de Trabajo (Ver características en el ítem 17). Certificaciones (Ver características en el ítem 18). Gestión de Incidentes (Ver características en el ítem 19). Devolución del servicio (Ver características en el ítem 20). <p>NOTA 1: Se entiende que es un contrato llave en mano. NOTA 2: Todos los elementos adquiridos y entregados producto del presente proceso contractual serán de propiedad de la DIAN. NOTA 3: Todos los elementos, plataformas, soluciones, servicios y demás capacidades requeridas por la Entidad en este anexo técnico deberán ser prestados por el contratista ganador.</p>	
1.2	<p>El futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, donde instalará todos los productos, capacidades, plataformas, soluciones y servicios, requeridos por la Entidad y que se encuentran en el anexo técnico y que le permitan realizar todas las actividades solicitadas en este por la DIAN. Entendiéndose que el contratista realizará toda la gestión, monitoreo, administración, acompañamiento, soporte y garantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados por el futuro SOC durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en este anexo técnico de obligatorio cumplimiento.</p>	
2	Especificaciones Técnicas SIEM	
2.1	Marca (Especificar la marca ofrecida)	
2.2	Referencia o Modelo (Especificar el modelo ofrecido)	
2.3	Cantidad (Especificar la cantidad ofrecida, debe ser físico, appliance de proposito específico)	
2.4	Se debe licenciar como mínimo para 2467 dispositivos (2056 que están estipulados en el inventario anexo más el 20% de incremento adicional).	
2.5	Debe tener la capacidad de manejar como mínimo 25000 EPS	
2.6	Debe realizar analítica en tiempo real.	
2.7	Debe manejar tasa de retención de tres (3) meses en línea y seis (6) meses fuera de línea.	
2.8	Debe tener autoaprendizaje de inventario de activos (CMDB)	
2.9	Debe tener correlación cruzada de analítica de SOC y NOC	
2.10	Debe tener asignaciones de reglas de TI e ICS (Industrial Control System) de MITRE ATT&CK y visibilidad de cobertura	
2.11	Debe tener monitoreo de transacciones sintéticas	
2.12	La solución debe estar en capacidad de instalarse en Azure, AWS, HyperV (en la versiones con que cuenta la entidad), Vmware (en la versiones con que cuenta la entidad). (Revisar archivo anexo inventarios), se aclara que la Entidad cuenta con Windows Server 2012R2, Windows Server 2022 y VMware ESXi, 7.0.3	

2.13	El contratista deberá realizar la correlación, monitoreo y casos de uso sobre la plataforma suministrada a la entidad, de tal forma que todo el know how y parametrizaciones queden para la entidad. Para la fase de implementación se deberán desarrollar y ejecutar 20 casos de uso, de manera, posterior durante la operación los que sean requeridos por la DIAN.	
2.14	Todas las labores de configuración de la herramienta de monitoreo y correlación de eventos y la generación de los casos de uso para el monitoreo SOC deberán ser ejecutadas por el personal asignado en el contrato.	
2.15	Dentro del plan de trabajo deberá especificar la metodología que utilizará para administrar, configurar, monitorear y gestionar el servicio de monitoreo objeto del presente contrato, especificando etapas, recursos, entregables, herramientas y técnicas a utilizar. Nota: La Entidad se reserva el derecho de ajustar aspectos de la metodología.	
2.16	Cuando un evento de seguridad ocurra o este en suceso, el servicio de monitoreo SOC deberá identificarlo y estar en la capacidad de relacionar de forma directa o indirecta con otros eventos de seguridad asociados, determinando el patrón de ataque.	
2.17	Debe tener métricas de base y detección de desviaciones (comportamientos anómalos).	
2.18	El contratista realizará la integración y monitoreo de los dispositivos y activos tecnológicos que conforman la infraestructura tecnológica de la entidad (Revisar archivo anexo inventarios)	
2.19	Una vez integrada toda la plataforma tecnológica, el contratista configurará y afinará la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos: <ul style="list-style-type: none"> • Actividades asociadas a la administración de cuentas de usuario final (UserID) • Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator). • Ejecución de comandos especiales sobre sistemas operativos • Ejecución de comandos especiales sobre bases de datos (dump,drop, delete, insert, update) • Cambios de parámetros técnicos, de configuración o de seguridad • Cambios de configuración horaria. • Cambios no autorizados en recursos tecnológicos críticos • Actividades de conexión de cuentas de usuario final o administradores. • Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs. • Actividades asociadas a conexión de acceso remoto. • Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional. 	
2.20	Contexto en tiempo real para análisis de seguridad que incluya: <ul style="list-style-type: none"> · Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución. · Análisis del rendimiento de aplicaciones y sistemas junto con datos del entorno para identificar rápidamente problemas de seguridad. · Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geo-localización. · Detección de dispositivos, aplicaciones de red y cambios de configuración no autorizados. 	
2.21	Contexto del dispositivo y de la aplicación <ul style="list-style-type: none"> · Dispositivos de red incluyendo switches, routers, WLAN. · Dispositivos de seguridad - Firewalls, IPS de red, gateways Web/Mail, protección contra malware, escáneres de vulnerabilidades. · Servidores, incluyendo Windows, Linux, AIX, HP UX. · Servicios de infraestructura incluyendo DNS, DHCP, DFS, AAA, controladores de dominio. · Aplicaciones orientadas al usuario, incluidos servidores Web, servidores de aplicaciones, correo, bases de datos. · Dispositivos de almacenamiento como (revisar contra inventario) · Cloud Apps, incluyendo AWS, Azure. · Infraestructura de la nube incluyendo AWS. · Dispositivos ambientales como UPS, HVAC, hardware del dispositivo. · Infraestructura de virtualización incluyendo VMware ESX, Microsoft HyperVScalable . 	
2.22	Informes de Cumplimiento Out-of-the-Box <ul style="list-style-type: none"> · Informes predefinidos listos para ser utilizados, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo, incluyendo: PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls. 	
2.23	Supervisión de rendimiento <ul style="list-style-type: none"> · Monitor de métricas de sistema (almacenamiento, rendimiento, memoria, etc). · Estado del sistema a través de SNMP, WMI, PowerShell. · Estado de aplicaciones a través de JMX, WMI, PowerShell. · Supervisión de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster. · Monitorización del rendimiento de aplicaciones a medida. · Microsoft Active Directory y Exchange a través de WMI y Powershell. · Posibilidad de agregar métricas personalizadas. 	
2.24	Supervisión del cambio de configuraciones en tiempo real <ul style="list-style-type: none"> · Recopilar archivos de configuración de red, almacenados en un repositorio versionado. · Recopilar las versiones de software instaladas, almacenadas en un repositorio versionado. · Detección automatizada de cambios en la configuración de la red y el software instalado. · Detección automatizada de cambios de archivos y carpetas. Windows/Linux, configuración 	

	<ul style="list-style-type: none"> · Detección automatizada de cambios de archivos y carpetas - Windows y Linux - quien y que. · Detección automatizada de cambios desde un archivo de configuración. · Posibilidad de detección automatizada de cambios en el registro de Windows a través de agente. 	
2.25	<p>Detección de anomalías</p> <ul style="list-style-type: none"> · Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. · Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. · Disparadores incorporados y personalizables sobre anomalías de comportamiento. 	
2.26	<p>Analítica</p> <ul style="list-style-type: none"> · Búsqueda de eventos en real - sin necesidad de indexación. · Búsquedas por palabras clave basadas en atributos de eventos analizados. · Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. · Match de patrones complejos en tiempo real. · Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas. · Programación de informes y entregas de resultados por correo electrónico a los principales interesados. · Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). · Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. · Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes. · Análisis escalable mediante la adición de nodos worker en caliente. · Posibilidad de priorización de los informes de incidentes. 	
2.27	<p>Recolección de logs escalable y flexible</p> <ul style="list-style-type: none"> · Soporte inmediato para una amplia variedad de sistemas de seguridad y APIs de proveedores - tanto locales como en la nube. · Los agentes de Windows proporcionarán una colección de eventos altamente escalable y rica, incluida la supervisión de integridad de archivos, los cambios de software instalados y la supervisión de cambios en el registro. · Agentes de Linux para la supervisión de integridad de archivos. · Capacidad de hash de ficheros vía File Integrity Monitoring utilizando SHA256. · Protección de la integridad de los logs almacenados en la plataforma utilizando SHA256. · Capacidad para modificar los analizadores directamente desde la interfaz gráfica de usuario y aplicarlos en el sistema en ejecución sin pérdida de tiempo de inactividad y de evento. · Creación de nuevos analizadores (plantillas XML) a través del entorno de desarrollo integrado y capacidad para compartir a través de la función de exportación / importación. · Recopilación segura y fiable de eventos para usuarios y dispositivos ubicados en cualquier lugar. 	
2.28	<p>Notificación y Gestión de Incidentes</p> <ul style="list-style-type: none"> · Framework de notificación de incidentes basado en políticas. · Posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico. · Integración basada en API a sistemas externos de ticketing - Aranda, ServiceNow, Salesforce, ConnectWise, Remedy y Jira. · Sistema incorporado de ticketing o integrarse al sistema de ticketing de la Entidad (Aranda). 	
2.29	<p>Paneles de control personalizados</p> <ul style="list-style-type: none"> · Dashboards configurables en tiempo real, con desplazamiento "Slide-Show" para mostrar KPIs. · Informes y análisis exportables entre organizaciones y usuarios. · Identificación rápida los problemas críticos, por ejemplo, a través de un código de colores. · Actualización rápida mediante el cálculo en memoria, sin acceso a disco. · Dashboards especializados para servicios empresariales, infraestructura virtualizada y aplicaciones especializadas. 	
2.30	<p>Integración con fuentes de Inteligencia Externas</p> <ul style="list-style-type: none"> · API para integrar inteligencia externa de amenazas - Dominios de malware, IPs, URL, hashes, nodos Tor, etc. · Integración para fuentes de inteligencia de amenazas populares - ThreatStream, CyberArk, SANS, Zeus, etc. · Tecnología para manejar grandes fuentes de información de amenazas - descarga incremental y compartición entre nodos, coincidencia de patrones en tiempo real. 	
2.31	<p>Integraciones de Tecnología Externa</p> <ul style="list-style-type: none"> · Integración con cualquier sitio web externo para la búsqueda de direcciones IP. · Integración basada en API para fuentes externas de inteligencia de amenazas. · Integración bidireccional basada en API con sistemas de help desk como ARANDA · Integración bidireccional basada en API con CMDB externas – directamente soportado. · Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop. · API para una fácil integración con sistemas de aprovisionamiento. · API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión. 	

2.32	Administración <ul style="list-style-type: none"> · GUI basada en web, a ser posible HTML5. · Control de acceso basada en roles para restringir el acceso a la GUI y a los datos. · Todas las comunicaciones entre módulos están protegidas por HTTPS. · Auditoría completa de la actividad del usuario. · Fácil actualización de software con un mínimo tiempo de inactividad y pérdida de eventos. · Actualización de la base de conocimientos (analizadores, reglas, informes) sencilla. · Archivado basado en políticas. · Hashing de registros a tiempo para no repudio y verificación de integridad. · Autenticación de usuario flexible – local, y externa a través de Microsoft AD y OpenLDAP, Cloud SSO/SAML a través de Okta. 	
2.33	Escalabilidad <ul style="list-style-type: none"> · Escalabilidad de recolección de datos mediante la implementación de máquinas virtuales con la función de recolección (colectores virtuales). · Los recolectores deben poder almacenar en búfer eventos cuando la conexión no esté disponible. · Escalado del análisis mediante la implementación de nuevas máquinas virtuales. · Arquitectura de balanceo integrada para recoger eventos desde sitios remotos usando recolectores 	
2.34	Supervisión de disponibilidad <ul style="list-style-type: none"> · Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento. · Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP. · Monitorización del hardware y del entorno. · Calendario para la programación de las ventanas de mantenimiento. · Cálculo de SLA – consideración de las horas normales de trabajo y fuera de horas. 	
2.35	Almacenamiento <ul style="list-style-type: none"> · Soporte de archivado de logs tanto para NFS como HDFS. · Creación de políticas de retención de logs tanto por espacio como por periodos de tiempo. 	
2.36	Licenciamiento <ul style="list-style-type: none"> · El fabricante ofertante deberá disponer de un método de licenciamiento escalable tanto por número de dispositivos como por EPS asociados. · Se deberá disponer de paquetes de licencia de agentes avanzados para monitorización de servidores críticos Windows y Linux, en ambientes híbridos (On-premise y Cloud). · Se deberá disponer de paquetes de licencia de agentes de UEBA para equipos Windows. Dichas licencias de UEBA no deberán conllevar consumo asociado ni de licencia de dispositivos ni de EPS. · Se deberá disponer de otras suscripciones como Indicadores de Compromiso (IoC). · Se deberá poder añadir EPS adicionales sin necesidad de contratar soporte asociado a los mismos. · Se podrán desplegar tantos colectores virtuales en ambientes híbridos como se quiera sin coste adicional. 	
2.37	En la solución SIEM entregada se debe integrar al SOAR, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración, para lo cual el oferente se apoyará en los inventarios incluidos en el archivo excel Anexo Técnico Proyecto SOC DIAN.	
3	Especificaciones Técnicas Plataforma SOAR	
3.1	Marca (Especificar la marca ofrecida)	
3.2	Referencia o Modelo (Especificar el modelo ofrecido)	
3.3	Cantidad (Especificar la cantidad ofrecida)	
3.4	La solución ofertada debe estar licenciada como mínimo para tres (3) analistas.	
3.5	En la solución SOAR entregada se debe integrar el SIEM, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración, para lo cual el oferente se apoyará en los inventarios incluidos en el archivo excel Anexo Técnico Proyecto SOC DIAN.	
3.6	Debe proporcionar varios paneles configurables que se integren con RBAC (Control de acceso basado en roles) para el control de acceso por función.	
3.7	La solución debe proporcionar un mecanismo para resaltar las alertas que se acercan al SLA configurado.	
3.8	El dashboard debe mostrar información específica del analista, como alertas y tareas asignadas al analista.	
3.9	Las alertas deben ordenarse por severidad.	
3.10	Los analistas deben poder configurar un dashboard específico del analista que muestre información relevante para ellos, y poder exportar las plantillas de dashboard, y deben autorefresharse.	
3.11	La solución debe proporcionar cuadros de mando centrados en funciones, como; analista de nivel 1, analista de nivel 2, gerente de SOC	
3.12	Debe medir las métricas de COS relevantes, como el tiempo medio para la identificación, confirmación, contención, erradicación y recuperación. Y mostrar estas métricas en un tablero.	
3.13	Mostrar un dashboard de monitoreo de estado de integraciones y también el estado del sistema del motor SOAR.	
3.14	La solución debe proporcionar un marco de desarrollo de tablero basado como mínimo en HTML / JSON / JS para permitir a los usuarios crear sus widgets de tablero personalizados e importarlos a la solución SOAR.	
3.15	El sistema debe proporcionar informes gráficos personalizados, y tener un sistema estructurado de manejo de incidentes que admita la clasificación de alertas manual y automática, y el manejo estructurado de incidentes.	

3.16	Los reportes deben poderse exportar al menos en formatos PDF o CSV, y poderse enviar los reportes agendados, a un receptor de email.	
3.17	El acceso a la funcionalidad del informe debe ser controlado por RBAC (Control de acceso basado en roles), y tener auditoría que identifique la actividad de informes, incluida la descarga de informes.	
3.18	Debería ser posible incluir una variedad de gráficos y métricas en informes personalizados.	
3.19	Las alertas y los incidentes deben manejarse por separado, cada uno en su propio módulo de interfaz de usuario. Las interfaces de gestión de alertas e incidentes deben ser personalizables para permitir una visualización flexible de la información, incluida la visualización de información de la alerta en sí más información adicional devuelta por los playbook de investigación.	
3.20	Permitir la correlación de alertas, indicadores, activos, campañas e incidentes junto con cualquier módulo personalizado cuando varios registros comparten valores de campo similares.	
3.21	La solución debe proporcionar una pista de auditoría específica para cada alerta.	
3.22	Permitir definir las condiciones que se deben cumplir antes de que se pueda ejecutar un playbook y limitar los playbook que se muestran al analista a aquellos que son relevantes para la vista actual.	
3.23	La solución debe permitir que el analista vincule directamente indicadores y cree nuevos indicadores desde dentro de la alerta. El usuario debe poder agregar nuevos artefactos o IOC (Indicador de compromiso) al finalizar la investigación.	
3.24	Proporcionar una función de búsqueda global que permita al analista buscar palabras clave en todo el sistema.	
3.25	Debería ser posible enviar actualizaciones, notas o acciones de la investigación a una plataforma de tiquetes.	
3.26	El analista debe tener la capacidad de solicitar que se creen tickets en la plataforma de tiquetes con información relevante incluida	
3.27	Debería ser posible enriquecer automáticamente el ticket con datos como el host, la IP, la reputación del archivo, etc.	
3.28	El administrador del sistema debe tener la capacidad de administrar el campo de comentarios y los archivos adjuntos agregando, editando o eliminando comentarios y mensajes	
3.29	El ticket debe incluir metadatos como el propietario, el estado y la prioridad del ticket. Estos metadatos deberían estar disponibles para su uso en los playbook.	
3.30	Debería ser posible controlar el acceso a las funciones de gestión de casos de manera granular utilizando el control de acceso basado en roles impulsado por GUI.	
3.31	El escalamiento de tiquetes debe basarse en: prioridad, riesgo, impacto o edad	
3.32	El sistema debe permitir que el analista realice un análisis de causa raíz (RCA - relacionado con la causa de la interrupción)	
3.33	El sistema debe permitir al analista realizar un análisis posterior al incidente (PIA, relacionado con el manejo de incidentes)	
3.34	La solución debe poder realizar una búsqueda de texto completa en todos los incidentes para notas y descripción u otras palabras clave en los incidentes.	
3.35	El sistema debe admitir funciones de gestión del ciclo de vida de incidentes, incluidas funciones para ayudar con la ingestión, el enriquecimiento, la asignación, la investigación y la escalada de datos.	
3.36	El sistema debe admitir el mapeo de tickets para las fases de la cadena de muerte cibernética (cyber kill chain).	
3.37	El sistema debe admitir la asignación y el seguimiento flexibles del Acuerdo de nivel de servicio multinivel en varias fases, como: SLA de reconocimiento, SLA de resolución.	
3.38	Permitir agregar y eliminar archivos y pruebas directamente desde o hacia los tickets.	
3.39	El sistema debe proporcionar una pista de auditoría detallada para ayudar con el registro de la cadena de custodia de los eventos vistos y los datos recopilados.	
3.40	El sistema debe proporcionar funciones para ayudar con la búsqueda de amenazas y el seguimiento de campañas.	
3.41	Permitir al analista buscar indicadores en el SIEM o en la solución de gestión de registros directamente desde la GUI de SOAR y procesar los resultados de la consulta devueltos.	
3.42	La solución debe tener la capacidad de crear módulos personalizados desde dentro de la GUI web, un módulo es un subsistema como: Alertas, Incidentes, indicadores... etc.	
3.43	Debería ser posible almacenar las respuestas a las consultas de registro del SIEM directamente en el ticket correspondiente.	
3.44	La solución debe permitir la visualización de entidades vinculadas (análisis de enlaces) como la dependencia entre incidentes, alertas, indicador, activos, usuarios y vulnerabilidades en cada una de las interfaces de usuario de estas entidades.	
3.45	Ciertos campos deben ser visibles y / u obligatorios bajo condiciones específicas (ejemplo: las notas de cierre deben ser visibles y obligatorias solo cuando el estado de alerta está configurado como cerrado).	
3.46	La solución debe tener una función de gestión de colas personalizable que admita la asignación automatizada de alertas / incidentes / tareas a varios grupos de usuarios.	
3.47	La solución debe integrarse con el marco de MITRE ATT&CK proporcionando enriquecimiento táctico, análisis de amenazas, investigación de incidentes y sugerencias de remediación.	
3.48	La solución debe permitir que el analista edite campos en la interfaz de usuario.	
3.49	La solución debe permitir a los usuarios visualizar gráficamente las entidades correlacionadas y sus atributos como gravedad, nombre, ID... etc.	
3.50	Un código de colores debe ayudar al analista a identificar la gravedad de cada entidad.	
3.51	La correlación gráfica debe estar disponible para diferentes entidades como activos, vulnerabilidades, alertas e incidentes.	
3.52	La solución debe tener al menos 600 playbooks que incluyan casos de uso, muestras y conectores relacionados.	
3.53	El sistema debe proporcionar un registro de ejecución visual del playbook que identifique el estado de ejecución del libro de jugadas y ayude con la resolución de problemas al identificar visualmente los pasos fallidos del mismo.	
3.54	La ejecución del playbook debe registrarse y estar fácilmente disponible para auditoría y resolución de problemas.	
3.55	Los playbook deben almacenarse de manera estructurada, como en una carpeta o estructura de grupo.	
3.56	El sistema debe proporcionar un generador gráfico de playbook visual de arrastrar y soltar.	
3.57	Debería ser posible realizar acciones de corrección y del sistema desde los playbook. Los ejemplos de acciones de remediación incluyen bloquear al usuario, deshabilitar la cuenta, etc. Los ejemplos de acciones del sistema incluyen la actualización del ticket, la asignación del ticket, la actualización del indicador y la aprobación de la ejecución del playbook.	
3.58	El administrador debe tener la capacidad de exportar Playbook, incluidas todas sus versiones guardadas (similar a SVN / GIT).	
3.59	Debería ser posible ejecutar varios playbook al mismo tiempo. El sistema debe ser escalable y permitir que se ejecute una gran cantidad de playbook simultáneos con nodos o licencias adicionales.	

3.60	Las herramientas de depuración deben estar disponibles de fábrica con la herramienta.	
3.61	El editor de playbook debe admitir: <ul style="list-style-type: none"> · Acciones y tareas manuales. · Pasos de aprobación y toma de decisiones. · Playbooks anidados. · Condiciones lógicas y bucles. · Ejecución de Python para scripts personalizados. · Correos electrónicos de texto enriquecido. · Solución de problemas de playbook de manera visual. · Capacidad configurable para detener o continuar con el error en algún paso del playbook. · La capacidad de marcar los playbook como activos". 	
3.62	El sistema debe permitir que los playbooks se ejecuten de diversas formas, como; ejecución manual del libro de jugadas, ejecución en la creación o actualización de registros, ejecución en un horario o cuando se solicita un punto final de API específico.	
3.63	Los playbook deben admitir una arquitectura de etiquetas flexible que permita a los analistas etiquetar los libros de jugadas y otros objetos del sistema con un valor de etiqueta que se pueda buscar y procesar.	
3.64	El acceso al playbook debe ser controlado por RBAC.	
3.65	El editor de playbooks debe admitir versiones o instantáneas del playbook para permitir la reversión de un playbook a una versión anterior.	
3.66	La solución debe admitir el reinicio del playbook desde el paso del playbook fallido anteriormente.	
3.67	La solución debe permitir al usuario ejecutar el playbook desde el editor de playbook.	
3.68	El sistema debe tener un mecanismo de actualización de conectores en vida que permita actualizaciones de conectores de proveedores entre versiones de software.	
3.69	El sistema debe tener una selección de conectores proporcionados y validados por el proveedor para la integración con sistemas de terceros. La documentación de los conectores debe estar publicada e Internet.	
3.70	La solución debe tener al menos 300 conectores de integración.	
3.71	La solución debe contar con conectores de integración ya desarrollados para integración con las siguientes plataformas con las que cuenta la entidad: Firewall de Nueva generación, Sandbox, plataforma de logs y reportes (SIEM).	
3.72	La GUI debe proporcionar una indicación de que las actualizaciones del conector están disponibles y proporcionar el registro de cambios de cada versión.	
3.73	Debe haber disponible un SDK de conector.	
3.74	El sistema debe proporcionar un asistente de ingestión de datos fácil de usar para configurar la ingesta de datos desde sistemas de terceros.	
3.75	El sistema debe proporcionar un indicador gráfico (tablero) del estado de los conectores que indique si la conexión al sistema de terceros está en buen estado sin la interacción del usuario.	
3.76	El sistema debe incluir una base de datos de "indicadores" dedicada que proporcione un almacén central de indicadores observados únicos	
3.77	El sistema debe admitir la correlación de los indicadores observados en múltiples alertas.	
3.78	Debería ser posible importar y exportar de forma masiva varios indicadores.	
3.79	Debería ser posible asignar una reputación a los indicadores, ya sea de forma manual o automática desde fuentes de inteligencia de amenazas de terceros.	
3.80	Los indicadores deben poder agruparse por evento, campaña, atacante, vector.	
3.81	El analista debe poder vincular los indicadores a las fases de Cyber Kill Chain (etiqueta).	
3.82	El sistema debe proporcionar un control de acceso basado en roles (RBAC) granular y flexible. RBAC debería permitir a los administradores configurar a qué áreas de la GUI puede acceder un usuario y a qué conjuntos de datos (por ejemplo, qué alertas) pueden acceder.	
3.83	La configuración de usuario y RBAC debería ser posible a través de la GUI.	
3.84	RBAC debe ser granular, lo que permite a los administradores especificar los permisos Crear lectura, actualización y eliminación hasta el nivel de la función.	
3.85	La solución debe admitir la autenticación de usuarios internos, la autenticación de usuarios externos a través de LDAP, autenticación de 2 factores y SAML SSO.	
3.86	Debe permitir que la granularidad del control de acceso sea a nivel de módulo, registro o campo ("Alertas", "máquina A con IP 1.2.3.4 infectada", "1.2.3.4" son respectivamente ejemplos de módulo, registro y campo).	
4	Especificaciones Técnicas herramienta de protección de Bases de Datos	
4.1	Marca (Especificar la marca ofrecida)	
4.2	Referencia o Modelo (Especificar el modelo ofrecido)	
4.3	La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo esquemas, objetos, tablas, sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un comportamiento base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.	
4.4	La solución entregada deberá ser implementada, configurada y puesta en marcha para monitorear todas las bases de datos de la Entidad, de acuerdo con el inventario de bases de datos que se encuentra en este archivo en la hoja "Inventario Infraestructura IT".	
4.5	Proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.	
4.6	Generar reportes y tendencias en tiempo real, así como permitir la modificación de estos.	
4.7	Contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente.	
4.8	La solución no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.	

4.9	Funcionar independiente a la activación de la auditoría nativa de la base de datos.	
4.10	La solución deberá ser transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.	
4.11	La solución deberá ser capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.	
4.12	La solución deberá realizar una evaluación exhaustiva de los riesgos de la infraestructura objetivo a diferentes niveles/capas de la infraestructura de base de datos incluyendo: <ul style="list-style-type: none"> • Aspectos de configuración de la base de datos tales como nivel de parcheo, configuración de las cuentas de usuario, evaluación de la fortaleza de las contraseñas, vigencia de contraseñas. • Aspectos de configuración de la plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos. 	
4.13	Deberá de poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.	
4.14	Tener la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo con las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.	
4.15	Proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.	
4.16	Alertar en tiempo real modificaciones, cambios, reemplazo y borrado de registros, tablas, índices y archivos sin autorización de la base de datos, con el fin de proteger el principio de integridad de la seguridad de la información.	
4.17	Monitorear toda la actividad de las bases de datos, y almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.	
4.18	Monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.	
4.19	Hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior posterior y sin degradar el performance de la base de datos.	
4.20	Tener la capacidad de monitorear el tráfico cifrado hacia las Bases de Datos.	
4.21	Proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.	
4.22	Manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automática o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.	
4.23	Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación: <ul style="list-style-type: none"> • Número de registros a regresar por la consulta (SQL Query) • Número de registros afectados • Tipo de datos accedido (financiero, recursos humanos, inventarios, o cualquier definición personalizada) • Acceso a datos marcados como sensibles • Base de Datos, Esquema, Tabla y Columna accedida • Estado de autenticación de la sesión • Usuario y/o grupo de usuarios de Base de Datos conectado • Usuario conectado en la capa aplicativo, a diferencia del usuario conectado a la base de datos • Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares) • Autenticación (login, logout) y tareas (quering) • Direcciones IP origen y destino • Nombre de Host origen, usuario firmado en el host origen • Aplicación usada para la conexión a la base de datos • Tiempo de respuesta/procesamiento de las tareas • Errores en el manejador de SQL • Número de ocurrencias en intervalos de tiempo definidos • Por operaciones básicas (Select, Insert, Update, Delete) • Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export) • Por Stored Procedure o función utilizada • Si existe evento asignado de cambios (ticket) • Fecha y hora del evento 	
4.24	La solución deberá identificar individualmente a los usuarios finales que realicen actividades mediante aplicaciones, aún si utilizan mecanismos comunes de comunicación entre la aplicación y la base de datos, esta actividad no deberá implicar la modificación de la aplicación y/o de la base de datos.	
4.25	Debe posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.	
4.26	Asociar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad.	
4.27	Proteger contra ataques SQL y no-SQL (como buffer overflow)	
4.28	Verificación de violaciones de la información que incluyan: <ul style="list-style-type: none"> • Altos volúmenes de acceso a datos sensibles más allá de lo habitual. • Acceso a datos inusual para cierta hora del día. • Acceso a datos desde una ubicación desconocida. 	

	<ul style="list-style-type: none"> • Acceso a datos utilizando aplicaciones/herramientas no autorizadas. 	
4.29	Debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.	
4.30	Tener facilidades de archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)	
4.31	Contar con políticas, reportes, alertas y transacciones pre-identificadas y pre-configuradas para trabajar con plataformas empresariales.	
4.32	Tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y syslog.	
4.33	<p>La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios:</p> <ul style="list-style-type: none"> • Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos. • Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa. • Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos. • Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar APIs. • Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer autenticación a las bases de datos. 	
4.34	Permitir el manejo de alarmas y notificaciones en tiempo real para los eventos de correlación mencionados anteriormente.	
4.35	Contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de estas.	
4.36	<p>La solución deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo. El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:</p> <ul style="list-style-type: none"> • Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos. • Deberá incluir una lista pre-configurada y detallada de las firmas de ataque. • Deberá permitir la modificación o adición de firmas por el administrador. • Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes. • Deberá detectar ataques conocidos en múltiples niveles, incluyendo, la red, sistemas operativos, software del servidor web y ataques a nivel de aplicación. 	
4.37	<p>La solución deberá contar con una base de datos de vulnerabilidades predefinida para las siguientes regulaciones:</p> <ul style="list-style-type: none"> • CIS • DISA (STIG) • FISMA • HIPAA • PCI-DSS 	
4.38	<p>Contar con políticas de vulnerabilidades para bases de datos y descubrir vulnerabilidades conocidas para las siguientes bases de datos:</p> <ul style="list-style-type: none"> • DB/2 • Informix • MSSQL • MySQL • Oracle • Sybase 	
4.39	<p>Deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos:</p> <ul style="list-style-type: none"> • Oracle (Including NDE/ASO, SSL) • Oracle Exadata • Microsoft SQL Server • IBM DB2 para Linux, z/OS y DB2/400 • IBM IMS para z/OS • IBM Informix • IBM Netezza • SAP Sybase (ASE, IQ, SQL Anywhere) • SAP-HANA • Teradata • MySQL • PostgreSQL • Progress OpenEdge • Maria DB 	
4.40	Debe proporcionar un proceso de instalación, actualización y gestión de cambios centralizada, segura y ágil para los agentes; la cual debe proporcionar una visión completa de todas las actualizaciones disponibles para los componentes de la solución de protección de bases de datos.	

4.41	Notificar cuando se encuentre disponible una nueva versión del agente de monitoreo.	
4.42	El despliegue y la instalación centralizada de parches y actualizaciones a componentes solo deberá ser realizada por usuarios con los privilegios necesarios y administradores de la herramienta.	
4.43	Proporcionar información del tráfico enviado de los agentes a los dispositivos, identificando actividades de bases de datos que no son necesarias monitorear; permitiendo a los administradores de la solución generar reglas de exclusión para reducir el consumo de recursos en el servidor.	
4.44	Contar con la opción de reducir el tráfico entre la comunicación entre el agente y el dispositivo utilizando métodos de compresión de datos.	
4.45	Proporcionar la opción de enmascarar la información personal que se despliega a través de la interfaz de administración, además deberá contar con la opción de desenmascarar esta información dependiendo los privilegios de cada usuario.	
4.46	Monitorear datos y usuarios, identificar de manera inteligente, priorizar los riesgos y presentar una imagen clara y procesable de los riesgos descubiertos y detenidos.	
4.47	Contar con aprendizaje automático y análisis de grupos de personas para establecer una línea de base contextual completa del acceso típico de los usuarios a las tablas de la base de datos, detectar y prioriza la actividad anómala.	
4.48	Aprender dinámicamente los patrones de acceso a datos normales de los usuarios y luego identificar actividades de acceso inapropiadas o abusivas para alertar proactivamente a los equipos de TI sobre conductas peligrosas.	
4.49	La solución deberá contar con el aprendizaje para automatizar el procesamiento de grandes cantidades de registros de actividad de las bases de datos para resolver incidentes significativos.	
4.50	Contar con algoritmos pre-configurados desarrollados para detectar el acceso a datos abusivos o inapropiados específicos, como el abuso de la cuenta de servicio o el acceso excesivo a los registros de la base de datos.	
4.51	Deberá contar con un tablero intuitivo que proporcione un resumen ejecutivo de los riesgos de violación de datos en sus bases de datos y archivos compartidos.	
4.52	Incluir una consola de reportería basada en big data, que retenga los datos siempre en tiempo real y permita generar búsquedas y analítica forense, como mínimo debe manejar una retención de seis (6) meses.	
4.53	La solución ofrecida deberá ser de propósito específico.	
4.54	Consola de Administración de la Plataforma de Monitoreo de Bases de Datos	
4.54.1	Los diferentes componentes de seguridad de bases de datos distribuidos en red deberán de administrarse a través de una consola centralizada.	
4.54.2	La consola centralizada deberá de ser el único punto de contacto, administración, control, análisis y reporte para las diferentes soluciones e infraestructura de seguridad en bases de datos.	
4.54.3	En el modo monitoreo el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.	
4.54.4	En el modo de cumplimiento de políticas, la solución deberá bloquear ataques proactivamente.	
4.54.5	Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de tomar las acciones adecuadas. Las acciones deberán incluir la habilidad para terminar las solicitudes y respuestas, bloquear la sesión TCP, bloquear el usuario de la aplicación, o bloquear la dirección IP.	
4.54.6	Respecto de ataques particularmente destructivos, la solución deberá ser capaz de bloquear la dirección IP por un periodo de tiempo configurable.	
4.54.7	En modo analizador de paquetes, la solución deberá ser capaz de enviar un paquete TCP-RST a ambos extremos de la conexión. Alternativamente, si así se configura, la solución podrá reportar el comportamiento anómalo, pero no tomar acción alguna.	
4.54.8	La solución podrá ser desplegada dentro de ambientes virtuales VMWare como dispositivo virtual.	
4.54.9	La solución deberá ser capaz de poder desplegarse en nubes públicas como Amazon Web Services o Microsoft Azure	
4.54.10	La solución deberá soportar el volumen de tráfico y deberá tener una latencia menor a 5ms, para no impactar el desempeño de las aplicaciones.	
5	Especificaciones Técnicas Monitoreo Gestión de Vulnerabilidades.	
5.1	Marca (Especificar la marca ofrecida)	
5.2	Referencia o Modelo o Versión (Especificar el modelo ofrecido)	
5.3	Alcance del Requerimiento	
5.3.1	Debe ser en modalidad software como servicio. (SaaS), con capacidad de aprovisionamiento rapido y elasticidad automática de servicios. No se aceptan soluciones de código abierto o similares. debe integrarse con herramientas de vulnerabilidades tal como Trend Vision One, entre otras.	
5.3.2	Licenciamiento para 17726 activos que incluyen (15000 pc's, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web). Las licencias podrán ser reasignadas entre activos, sin generar costos adicionales para la Entidad, los tiempos para la reasignación de licencias serán acordados en su momento con el futuro contratista, normalmente estos tiempos oscilan entre uno y quince días dependiendo de la cantidad y el grado de complejidad de la actividad.	
5.4	Generalidades	
5.4.1	La solución tecnológica deberá traducir la información obtenida por medio de evaluación de vulnerabilidades, evaluación de líneas base de configuración y evaluación de cumplimiento regulatorio sobre todos los activos TI, recursos en la nube y aplicaciones web, con el fin de priorizar acciones y comunicar el riesgo cibernético.	
5.4.2	La solución ofertada deberá proveer una visibilidad completa sobre toda la superficie de ataque, sobre un único portal que proporcione una vista unificada.	
5.4.3	La solución ofertada permitirá anticipar las amenazas y priorizar los esfuerzos de mitigación con el fin de evitar ataques.	
5.4.4	La solución ofertada deberá contar con una vista de exposición, la cual permita enfocar los esfuerzos de seguridad brindando información clara y concisa de la exposición con respecto a la seguridad de la Entidad. De la misma forma deberá proporcionar una puntuación global unificada de la exposición obtenida a partir de diferentes fuentes de datos.	
5.4.5	La solución ofertada deberá contar con un Inventario de Activos centralizado, con el objetivo de proporcionar una visibilidad completa hacia todos los activos independientemente de la fuente de datos (Activos TI, Aplicaciones Web), permitiendo la agrupación por medio de etiquetas.	
5.4.6	La solución ofertada deberá realizar una gestión de vulnerabilidades basadas en el riesgo, permitiendo una priorización dinámica de las tareas de remediación en función de las amenazas.	
5.4.7	La solución ofertada deberá realizar una evaluación de vulnerabilidades en entornos web de manera automatizada de manera completa y precisa.	
5.4.8	La solución ofertada permitirá la protección de la infraestructura en la nube, permitiendo una visibilidad completa y de manera continua de exposiciones, vulnerabilidades y permisos de acceso; priorizando tareas de remediación.	

5.4.9	La solución ofertada permitirá proveer métricas de evaluación de los programas de evaluación y remediación de la Entidad.	
5.4.10	La solución ofertada deberá soportar funcionalidades de seguridad de doble factor de autenticación.	
5.4.11	La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	
5.4.12	La solución ofertada deberá tener capacidades que permitan análisis, visualización y priorización de rutas de ataques proporcionando una respuesta enfocada de forma preventiva con el fin de interrumpir las rutas que pueden ser utilizadas por un atacante. Dicho análisis deberá ser soportado bajo las criticidades expuestas en el marco MITRE ATT&CK.	
5.4.13	La solución ofertada permitirá gestionar la superficie de ataque externa, con el fin de identificar y reducir riesgo, brindando a la entidad la visión de un atacante.	
5.4.14	Debe tener cobertura de activos en la entidad los cuales podrán estar ubicados en el Datacenter principal, la red general, sus dependencias, el Datacenter Alternativo e infraestructura Cloud de la Entidad.	
5.4.15	Debe incluir una capacidad integrada de exploración activa y pasiva, incluyendo análisis continuo por medio de análisis de tráfico desde un puerto espejo o similar).	
5.4.16	La solución ofertada deberá poder ejecutar descubrimiento de activos y vulnerabilidades a través de: <ul style="list-style-type: none"> • Monitoreo pasivo mediante el análisis de red a través de un puerto espejo para el descubrimiento de activos, incluyendo el descubrimiento pasivo de objetivos utilizando IPv6. Dicha tecnología deberá estar patentada. • Sensores activos para el descubrimiento de activos y análisis de vulnerabilidades incluyendo el uso de IPv6. Estos sensores se pueden desplegar en forma de escáneres o agentes. 	
5.4.17	Consolidar todos los hallazgos, tanto para el módulos de gestión de vulnerabilidades en infraestructura como de aplicaciones web.	
5.4.18	La solución de gestión de vulnerabilidades debe incluir paneles gráficos personalizables que permitan ajustar la información presentada a las necesidades puntuales del usuario.	
5.4.19	Se debe ofrecer entrenamiento gratuito en línea como parte de la oferta para los integrantes de la DIAN por parte del fabricante de la solución. Esto durante la vigencia del contrato de soporte.	
5.4.20	Todos los módulos licenciados deberán ser parte de la misma solución permitiendo la exploración, administración, uso y configuración desde una misma consola WEB.	
5.4.21	La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de los activos TI de la Entidad y hacer parte de una plataforma de gestión de ciberexposición.	
5.4.22	La solución ofertada deberá estar en la capacidad de cubrir más de 82.000 CVEs IDs y 30.000 Bugtraq IDs, con una baja tasa de falsos positivos.	
5.5 Arquitectura de la Solución Ofertada		
5.5.1	La solución ofertada debe estar basada en cloud y tratarse de una solución (SaaS), la información adquirida deberá ser almacenada dentro de la aplicación evitando el uso de bases de datos o soluciones externas.	
5.5.2	Debe proporcionar una API integral o solución similar de iguales o superiores características para la automatización de procesos e integración con aplicaciones de terceros.	
5.5.3	El software debe incluir la opción de uso de agentes para aquellos dispositivos que no puedan ser analizados por otros medios de manera frecuente y ofrecer opciones de implementación, agentes, máquinas virtuales desplegadas localmente, o como una aplicación instalada en el sistema operativo a escanear, todas ellas avaladas por el fabricante.	
5.5.4	Debe permitir el uso de motores de análisis ubicados en la nube sin costo adicional y que permitan la recolección de datos sobre activos que se encuentren expuestos hacia internet, además debe permitir la instalación de sensores en soluciones de nube pública como Azure y AWS entre otras. Dichos sensores deben encontrarse disponibles en los catálogos de cada uno de estos proveedores o estar habilitados para este tipo de arquitecturas (Cloud). Los motores de análisis son suministrados por el fabricante de la solución y cubiertos por el licenciamiento adquirido.	
5.5.5	Debe soportar integración con Centro de Operaciones de Seguridad (SOC) mediante alertas automatizadas nativas en el producto. También deberá tener la capacidad de integrarse a soluciones tipo SIEM y de Orquestación de seguridad (SOAR), la solución deberá estar en capacidad de generar alertas cuando se detecten nuevas vulnerabilidades críticas en sistemas relevantes, nuevas vulnerabilidades asociadas a una amenaza conocida y otras reglas personalizables.	
5.5.6	La solución ofertada deberá hacer uso de sensores los cuales podrán desplegarse en una variedad de plataformas, incluyendo: Windows Workstations y Servers, Linux, Mac OS ya sea en dispositivos virtuales o físicos.	
5.5.7	La solución ofertada deberá poder desplegar el número de escáneres, monitores de red y agentes de escaneo donde sean necesarios sin que esto represente un incremento en costo.	
5.5.8	La solución ofertada deberá poder equilibrar cargas a través de múltiples escáneres de forma dinámica con base en la disponibilidad de cada escáner desplegado.	
5.6 Control de Acceso a la solución		
5.6.1	La solución ofertada deberá proporcionar control de acceso basado en roles (RBAC) para controlar el acceso de los usuarios a conjuntos de datos y funcionalidades específicas en el caso de que La DIAN así lo requiera.	
5.6.2	La solución debe ofrecer la capacidad de restringir los permisos de flujo de trabajo para incluir, aceptar y volver a ejecutar clasificaciones de riesgo para vulnerabilidades.	
5.6.3	Debe poder definir y administrar grupos de usuarios, incluida la limitación de las funciones de escaneo y el acceso a informes.	
5.6.4	Deberá permitir configurar permisos de acceso y visibilidad a los resultados y de control y configuración de los parámetros del escaneo.	
5.7 Exploración		
5.7.1	La solución debe permitir escaneos en plataformas Windows, Linux, Mac OS, así como máquinas virtuales.	
5.7.2	Debe incluir diversas alternativas para la recolección de información (escáner activo, pasivo, agente o similares), todo esto cubierto por el licenciamiento adquirido sin límite para su implementación, mas allá de las cantidades solicitadas ítem 5.3.2.	
5.7.3	La solución debe admitir múltiples motores de escaneo distribuidos geográficamente y administrados por una consola central. En el caso de que la DIAN requiera desplegar el servicio de escaneo de manera local para reducir el impacto a nivel de red, la solución debe permitir dicho despliegue mediante una máquina virtual o agentes que reporten a la consola central.	
5.7.4	La solución debe ser configurable para limitar la carga sobre la red ocasionada por el escaneo para evitar la generación de tráfico que podría interrumpir la operación normal de la red.	
5.7.5	Debe proporcionar la capacidad de admitir el escaneo sin conexión y la importación de resultados en la plataforma. (Análisis Off-Line)	
5.7.6	La solución debe permitir la entrada y el almacenamiento seguro de credenciales de usuario, incluidas las cuentas locales y de dominio de Windows, y Linux ,Unix su y sudo.	

5.7.7	La solución debe permitir escalar privilegios en los objetivos desde el acceso normal del usuario al acceso con roles de administración (root/ administrador).	
5.7.8	Debe permitir la programación de escaneos personalizados, incluida la capacidad de ejecutar escaneos en momentos designados, con una frecuencia predeterminada.	
5.7.9	La solución debe poder realizar búsquedas de datos confidenciales en los endpoint o equipos de usuario final. La aplicación deberá contar con una biblioteca o similar que permita la identificación y parametrización de los datos a identificar.	
5.8	Descubrimiento de Activos	
5.8.1	La solución debe ser capaz de detectar servicios que se ejecutan en puertos no estándar y detectar servicios configurados para no mostrar pancartas de conexión. En caso de detectar un nuevo servicio, el sistema deberá alertar en la consola central a través de un banner, pancarta o similar.	
5.8.2	Debe tener la capacidad de probar varias instancias del mismo servicio que se ejecuta en diferentes puertos y tener la funcionalidad de escanear hosts que no responden al ping	
5.8.3	La solución debe admitir el uso opcional de netstat para una enumeración rápida y precisa de los puertos abiertos en un sistema cuando se proporcionan las credenciales, además debe admitir el uso de SMB y WMI para escanear sistemas Windows.	
5.8.4	La solución debe ser capaz de iniciar automáticamente los servicios de registro remoto en los sistemas Windows al realizar una exploración con credenciales, y luego detener automáticamente el servicio una vez que se complete la exploración.	
5.8.5	El escáner debe admitir el protocolo Secure Shell (SSH) con la capacidad de escalar privilegios para escaneos de vulnerabilidades y auditorías de configuración en sistemas basados en Unix.	
5.8.6	La solución ofertada deberá permitir la clasificación de activos identificados de manera manual o dinámica, con diferentes atributos encontrados en el análisis con base en etiquetas o en grupos de trabajo, para poder usarse en escaneos posteriores.	
5.8.7	La solución debe proporcionar la capacidad de ajustar las políticas de escaneo para un impacto mínimo en las redes y los objetivos.	
5.8.8	El producto debe proporcionar un descubrimiento activo y pasivo de puntos de acceso inalámbrico (WAP), mediante una maquina virtual local en la red o agentes locales.	
5.9	Detección, Análisis y Evaluación de Vulnerabilidades	
5.9.1	La solución debe realizar el escaneo para la detección de vulnerabilidades locales y remotas sin la necesidad de un agente en el dispositivo de destino.	
5.9.2	Debe tener la funcionalidad de realizar pruebas con agentes para la detección de vulnerabilidad local sin costo adicional.	
5.9.3	Debe ser capaz de rastrear los cambios de DHCP al asociar los resultados de escaneo de un sistema así como con una dirección IP diferente a la inicial	
5.9.4	La solución debe ser compatible con el estándar de clasificación de vulnerabilidades CVE (Common Vulnerabilities and Exposures).	
5.9.5	La solución debe proporcionar auditorías de parches para los sistemas operativos Windows y aplicaciones Microsoft (Edge, Microsoft Office, IIS, Exchange, 365, entre otros)	
5.9.6	La solución debe proporcionar auditorías de parches para todos los principales sistemas operativos Unix, Mac OS, Linux, entre otros.	
5.9.7	La solución debe proporcionar cobertura para aplicaciones de terceros como Java, Python entre otras.	
5.9.8	Debe proporcionar integración con los sistemas de administración de parches: Microsoft WSUS / SCCM, entre otros, esto como herramienta adicional para la auditoría de actualización.	
5.9.9	Debe incluir la calificación de vulnerabilidad de acuerdo con el estándar aceptado por la industria, es decir, el Sistema de calificación de vulnerabilidad común Versión 4 (CVSS 4).	
5.9.10	El producto ofertado debe proporcionar información acerca de la capacidad de explotación de la vulnerabilidad por parte de terceros como Core, Metasploit y Canvas.	
5.9.11	La solución ofertada debe suministrar información de vulnerabilidades que pueden ser explotadas por malware.	
5.9.12	Seleccionar de forma inteligente las pruebas a realizar basándose en la información obtenida de los escaneos iniciales para intentar realizar pruebas adicionales basadas en la información obtenida previamente sobre un dispositivo o host.	
5.9.13	Permitir la habilitación o deshabilitación de pruebas durante los escaneos programados.	
5.9.14	Etiquetar los activos por grupos en función de las necesidades de la organización con la finalidad de categorizar los resultados y asignar las tareas correspondientes.	
5.9.15	La solución no debe depender de la capacidad del sistema operativo para programar tareas.	
5.9.16	La solución ofertada debería admitir el escaneo IPv6, con descubrimiento pasivo de objetivos IPv6.	
5.9.17	Debe rastrear con precisión los activos y sus vulnerabilidades, incluidos los activos de TI altamente dinámicos como dispositivos móviles, máquinas virtuales e instancias en la nube.	
5.9.18	Debe poseer un sistema de puntuación de vulnerabilidad que contemple la probabilidad de explotación de vulnerabilidades, considerando atributos como la existencia de un exploit, si se han presentado víctimas de dicha vulnerabilidad, entre otros.	
5.9.19	Debe poseer un sistema de puntuación de vulnerabilidad que contemple la probabilidad de explotación de vulnerabilidades, considerando atributos como la existencia de un exploit, si se han presentado víctimas de dicha vulnerabilidad, entre otros.	
5.9.20	La solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad. Dicha calificación deberá ser obtenida a partir de los siguientes factores: <ul style="list-style-type: none"> •Ea priorización deberá correlacionar información de vulnerabilidades con bases de inteligencia de amenazas para determinar la probabilidad de explotación. •El modelo de priorización deberá ser capaz de predecir si una vulnerabilidad tiene posibilidades de explotación en el futuro cercano. •Ea priorización deberá considerar elementos de evaluación diversos, como: edad de la vulnerabilidad, madurez del código de explotación, intensidad y fuentes de las amenazas, número de días desde que se conoció una actividad de amenaza sobre la vulnerabilidad. 	
5.9.21	La solución ofertada deberá proveer una vista de soluciones que permitan enfocar en las secciones más importantes primero. Dicha vista deberá proveer los siguientes datos: <ul style="list-style-type: none"> •Descripción de la solución. •Número de dispositivos asociados a la solución. •Número de instancias de vulnerabilidades asociadas a la solución. •Ea calificación dinámica de probabilidad de explotación más alta para las vulnerabilidades asociadas a la solución. 	
5.9.22	La solución ofertada deberá incluir la posibilidad de programar ventanas de escaneo.	
5.10	Escaneo de Aplicaciones Web (FQDN)	

5.10.1	La solución debe poder escanear aplicaciones web internas y externas (hasta copar el licenciamiento requerido para 260 aplicaciones) y debe permitir la definición de secciones críticas de la aplicación que sean seguras para escanear y de otras partes que nunca deberían escanearse, para evitar latencias de rendimiento e interrupciones.	
5.10.2	La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de las aplicaciones web de la Entidad; provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición.	
5.10.3	La solución deberá ver todas las vulnerabilidades de las aplicaciones web, internas y externas, en una vista unificada o a través de la misma interface WEB.	
5.10.4	La solución ofertada deberá poder escanear aplicaciones modernas desarrolladas en frameworks JavaScript, AJAX, HTML5 and Single Page Applications.	
5.10.5	La solución ofertada permitirá realizar escaneos sin degradación de performance en el sitio, por medio de escaneos seguros, permitiendo definir sitios que no deben ser escaneados a partir de la URL, o extensiones de archivos	
5.10.6	La solución ofertada deberá permitir el escaneo de terceros y componentes open source como CMS, sitios web y motores de lenguaje.	
5.10.7	Debe permitir la ejecución de análisis autenticados sobre portales o aplicaciones, soportando el formato como Selenium o similares para automatizar dichas pruebas.	
5.10.8	La solución debe permitir la ejecución de análisis autenticados sobre portales o aplicaciones, soportando el formato HTTP Server Authentication para automatizar dichas pruebas.	
5.10.9	La solución debe permitir la ejecución de análisis autenticados sobre portales o aplicaciones, soportando el formato de autenticación por formularios pre establecidos.	
5.10.10	La solución debe permitir la ejecución de análisis autenticados sobre portales o aplicaciones, soportando el uso de cookies o similar para automatizar dichas pruebas.	
5.10.11	Los reportes de vulnerabilidades deben poderse presentar de manera organizada de acuerdo a los grupos establecidos por el TOP 10 de OWASP.	
5.10.12	La solución debe permitir la carga de Scripts de pruebas como Selenium o equivalentes para definir la ruta de inspección dentro del portal/aplicación.	
5.10.13	La solución debe soportar la descomposición de ruta (path Decomposition) para ampliar la superficie de inspección sobre el portal/aplicación.	
5.10.14	La solución debe permitir la parametrización de los análisis para definir: <ul style="list-style-type: none"> o Número de URL a inspeccionar dentro del portal. o Profundidad a nivel de DOM y ruta de directorios. o Tiempo máximo de respuesta. o Límite de redirección. o Definición del "User Agent" o Parametrización de encabezados o Número máximo de conexiones HTTP. o Número máximo de requerimientos por segundo. 	
5.10.15	La solución debe permitir reducir la velocidad de análisis cuando se detecte congestión en la red.	
5.10.16	La solución debe estar en capacidad de analizar vulnerabilidades en API tipo REST. La solución debe estar en capacidad de detectar vulnerabilidades de las siguientes familias, entre otras:	
5.10.17	<ul style="list-style-type: none"> o Access Restriction Bypass via Origin Spoof o Basic Authentication without HTTPS o Password field with auto-complete o Session Fixation o Unencrypted Password Form o Code Injection o Code Injection (php://input wrapper) o Code Injection (timing attack) o Operating System Command Injection o Operating System Command Injection (timing attack) o Component Vulnerability: Angular, Apache, Apache Solr, Apache Struts, Apache Tomcat, Atlassian, Bootstrap, Drupal, Wordpress, Joomla, jQuery, Kentico, Kibana, Knockout.js, lighthouse, Magento, MediaElement.js, Modernizr, Moment.js, nginx, PHP, Sitefinity, vBulletin, Webmin, YUI. o Cross Site Request Forgery o Cross-Site Scripting (XSS): In event tag of HTML element, in HTML tag, in path, in script context, in script src, DOM based, Response Splitting. o Data Exposure: Backup file/directory, Credit Card number disclosure, CVS Entries Detected, CVS Repository Detected, CVS/SVN user disclosure, Disclosed US Social Security Number, E-mail address Disclosure, Error Message, Full Path Disclosure, Git Repository Detected, Gitignore File Detected, Private IP address Disclosure, Source Code Disclosure, Source Code Leakage, SVN Repository Detected, Web.config File Information Disclosure, WS_FTP.Log File Detected. o Local or Remote File Inclusion o SSL/TLS: SSL Insecure Protocols, Certificate Expired, Certificate Common Name Mismatch, Certificate RSA Keys less than 2048 bits, Weak Hashing Algorithm, Insecure/Null Cipher Suites Supported, HTTP to HTTPS redirect not enabled. o HTTP Security Header: Deprecated Content Security Policy, Disabled X-XXS-Protection Header, HTTP Header Information Disclosure, Insecure 'Access-control-allow-origin' Header, Insecure Cross-Origin Resource Sharing Configuration, Insecure Cross-Origin Resource Sharing Configuration, Missing Header (Cache-control, Content-type, Expect-CT, X-Content-Type-Options, X-Frame-Options, X-XSS-Protection), Missing Content Security Policy, Missing Feature Policy, Missing HTTP Strict Transport Security Policy, Missing Referrer Policy, Permissive Content Security Policy Detected, Permissive HTTP Strict Transport Security Policy Detected, Report Only Content Security Policy Detected. o Injection: Blind NoSQL Injection, Blind SQL Injection, Host Header Injection, LDAP Injection, NoSQL Injection, SQL Injection, XML External Entity, XPath Injection. o Web Servers: Apache .htaccess and .htpasswd Disclosure, Backdoor Detection, Common Directories Detection, Common Files Detection, Directory Listing, HTTP Trace Allowed, Misconfiguration in LIMIT directive of .htaccess file, Publicly writable directory, Robots.txt file detected, Sitemap.xml file detected 	
5.10.18	La solución Deberá contar con una plantilla que permita auditar la configuración de la aplicación.	
5.10.19	Deber la capacidad para ser desplegada como un contenedor de Docker, permitiendo el escaneo de sitios públicos y privados.	
	La solución ofertada deberá contar con las siguientes plantillas de escaneo, entre otras: <ul style="list-style-type: none"> •API •Config Audit •g4Shell 	

5.10.20	<ul style="list-style-type: none"> •Overview •PCI •Quick Scan •Scan •SSL/TLS 	
5.10.21	La solución ofertada permitirá conocer el estado y progreso de una tarea de escaneo; de la misma forma generar tareas de escaneo programadas y envío de resultados por medio de correo electrónico.	
5.10.22	La solución ofertada deberá contar con la capacidad de gestionar los hallazgos, donde se puedan observar todas las vulnerabilidades descubiertas en la infraestructura.	
5.10.23	La solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad.	
5.10.24	El fabricante de la solución deberá poner a disposición acceso a una API que permita crear conectores, importar/exportar datos y automatizar procesos.	
5.11 Postura de Seguridad infraestructura Cloud		
5.11.1	La solución ofertada deberá Gestionar las Vulnerabilidades de todas las cargas de trabajo (CWPP), Gobierno y Cumplimiento de la infraestructura nube (CSPM), Gobierno de Identidades (CIEM), Análisis e Identificación de Comportamiento Malicioso (CDR) y Gobierno de Infraestructura como Código (IaC / DevSecOps) de la entidad, bajo una arquitectura CNAPP; provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición	
5.11.2	La solución ofertada deberá soportar como mínimo las nubes de Azure, AWS entre otras.	
5.11.3	La solución ofertada deberá poseer capacidades de autoremediación.	
5.11.4	La solución ofertada deberá estar en la capacidad de evaluar y priorizar el riesgo de la infraestructura evaluada.	
5.11.5	La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de las cargas de trabajo; Ser provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición.	
5.12 Auditoría de Configuración		
5.12.1	La solución debe ser capaz de realizar auditorías de cumplimiento sin la necesidad de un agente instalado en el dispositivo de destino.	
5.12.2	La solución debe proporcionar puntos de referencia de auditoría de seguridad y configuración para estándares de cumplimiento normativo así como otros estándares de mejores prácticas de la industria.	
5.12.3	Debe proporcionar puntos de referencia de auditoría de seguridad y configuración conforme a las mejores prácticas del proveedor, como Microsoft, Linux, soluciones MDM, enrutadores y conmutadores, firewalls y VMware.	
5.12.4	La solución debe proporcionar una auditoría de los sistemas operativos de Microsoft y Linux a nivel de configuración.	
5.12.5	Debe suministrar una auditoría de las bases de datos a nivel de configuración y auditoría de la infraestructura de red a nivel de configuración.	
5.12.6	La solución debe proporcionar una auditoría de la administración de dispositivos móviles a nivel de configuración y auditorías de paquetes antivirus específicos.	
5.12.7	La solución debe estar en capacidad de auditar la presencia de información de identificación personal (PII) y otro contenido confidencial.	
5.12.8	La solución debe permitir que las políticas de auditoría sean personalizables para las necesidades específicas de la organización.	
5.12.9	Debe suministrar puntos de referencia para dar cumplimiento a las recomendaciones del CIS.	
5.12.10	La solución debería ofrecer soporte SCAP (Security Content Automation Protocol)	
5.12.11	Debe contar con plantillas de auditoría asociadas a las mejores prácticas de la industria.	
5.13 Flujo de Trabajo		
5.13.1	La solución debe agregar los resultados de los escaneos individuales en vistas de vulnerabilidad acumulativa con capacidades de filtrado y análisis para permitir la obtención de detalles.	
5.14 Integración e Informes		
5.14.1	La solución debe proporcionar la capacidad de automatizar la generación de informes. La solución debe estar en capacidad de producir informes ad hoc.	
5.14.2	Debe admitir la capacidad de producir informes en pdf y pdf cifrado de manera programada o por demanda.	
5.14.3	La solución debe proporcionar una biblioteca de plantillas para los paneles de presentación de datos.	
5.14.4	La solución ofertada deberá tener la capacidad de integrarse con soluciones tipo Privileged Access Management (PAM)	
5.14.5	Debe permitir la exportación de los tableros de datos presentados en formato CSV, PDF y HTML.	
5.14.6	La solución deberá poderse integrar a las tecnologías de Monitoreo de Seguridad (SIEM de cualquier fabricante).	
6 Especificaciones Técnicas Caza de Amenazas		
6.1	Marca (Especificar la marca ofrecida) SE LICENCIA POR VLANS APPLIANCE DE PROPOSITO ESPECIFICO	
6.2	Referencia o Modelo (Especificar el modelo ofrecido)	
6.3 Alcance		
6.3.1	<p>Para el monitoreo y alertamiento temprano sobre nuevas vulnerabilidades, ataques, amenazas externas y del ciberespacio que puedan afectar a la infraestructura interna de la entidad el contratista debe adelantar el despliegue, configuración y afinamiento de herramientas para cacería de amenazas, las cuales permitan tener una visual horizontal y vertical en el caso de incidentes de seguridad de la información.</p> <p>Debe tener por lo menos las siguientes componentes:</p> <p>Herramientas de caza de amenazas: herramienta para buscar e interceptar ataques ocultos de una manera proactiva. Se puede desplegar una sola herramienta siempre y cuando tanto la inteligencia como la caza sean completamente identificables y a nivel de mercado sea aceptada como tal.</p> <p>Hay que tener en cuenta que el despliegue de herramientas que no tengan las capacidades de cacería de amenazas completas, no serán evaluadas.</p> <p>Parametrizar y/o configurar la herramienta adquirida, a partir de las mejores prácticas definidas por el fabricante y las exigencias de la entidad.</p>	
6.4 Aspectos Generales		

6.4.1	Debe permitir la creación de trampas de alta interacción, con capacidad de clonar activos existentes.	
6.4.2	El appliance de decepción debe estar en capacidad de crear al menos 400 señuelos, en hasta 20 máquinas virtuales y desplegarse en mínimo 128 VLANs.	
6.4.3	El licenciamiento de la solución debe ser como mínimo ciento veinte (120) vlangs.	
6.4.4	Debe permitir la creación de trampas activas con un flujo de tráfico de red falso entre las trampas implementadas para confundir y desviar a los atacantes que monitorean el tráfico, asegurando que interactúen con las trampas implementadas.	
6.4.5	Debe realizar ejecución de investigaciones proactivas de los eventos correlacionados para detectar amenazas avanzadas desconocidas.	
6.4.6	Debe permitir hacer visualización completa del ataque	
6.4.7	La solución ofertada debe incorporar paquetes de tokens para las máquinas señuelo o VM decoy.	
6.4.8	La solución ofertada debe soportar las siguientes acciones mediante integración con la solución Perimetral . - Bloqueo. - Cuarentena. - Exportación de IOCs.	
6.4.9	La solución deberá proporcionar reportes que caractericen tanto la identificación de incidentes como ataques detectados en la red de la entidad. Estos reportes deben incluir: - Severidad. - Última Actividad. - Tipo del evento. - Información de direccionamiento del atacante. - Información de credenciales de uso del atacante. - Información de direccionamiento de la Víctima. - Tiempo de iniciación del ataque - Puertos de ejecución del ataque - Tipo de Ataque - Información de passwords usados por el atacante. - Línea del tiempo. - PCAP del tráfico capturado por el Decoy.	
6.4.10	Debe estar en capacidad de hacer detección de reconocimientos de red que usen ping (ICMP)	
6.4.11	Debe contar con señuelos que simulen conectores a base de datos que usen ODBC	
6.4.12	Debe integrarse con el Firewall de Nueva Generación, de manera que se pueda tener en este último un dashboard centralizado con la información general del dispositivo y los señuelos desplegados.	
6.4.13	Debe permitir exportar indicadores de compromiso (IOC) al menos en formato CSV para su uso por parte de plataformas externas.	
6.4.14	Debe permitir el despliegue de señuelos en activos reales para que dirijan al atacante a la solución de Decepción de amenazas.	
6.4.15	Debe tener la capacidad de emular activos del tipo Gateway de VPN SSL.	
6.4.16	Debe tener la capacidad de emular activos con servicios SAMBA, SMB, SSH y HTTP/S habilitados.	
6.4.17	Debe tener la capacidad de definir una lista de Ips legítimas de la red para que no generen alertas cuando interactúen con los señuelos.	
6.4.18	Debe permitir visualizar en un mapa los señuelos desplegados.	
6.5	Aspectos Adicionales	
6.5.1	Debe tener al menos 4 capas de decepción, con la capacidad de crear los siguientes elementos falsos:	
6.5.2	Señuelos de infraestructura (Sistemas operativos, cámaras, impresoras, bases de datos, etc), de acuerdo a la cantidad de vlangs (120).	
6.5.3	Carnadas o servicios falsos que se ejecuten sobre los señuelos (servidores web, aplicaciones, etc), de acuerdo a la cantidad de vlangs (120).	
6.5.4	Tráfico de red falso para detectar ataques de tipo MitM o app spoofing, entre otros.	
6.5.5	Tokens o recursos falsos desplegados sobre los señuelos (Credenciales, archivos, recursos compartidos, conexiones RDP, etc).	
6.5.6	Los tokens falsos creados no deben ser visibles para los usuarios de la entidad, únicamente para el atacante.	
6.5.7	Todos los elementos falsos se deben desplegar sin requerir instalar agentes sobre la infraestructura real de la entidad	
6.5.8	La solución se debe poder instalar como appliance virtual y cubrir los siguientes Hipervisores: VmWare KVM Hyper-V	
6.5.9	Debe poder instalarse en infraestructura de nube pública, como mínimo en: Azure AWS Google Cloud	
6.5.10	Debe escanear automáticamente la red haciendo uso de técnicas de escaneo pasivo y sugerir los elementos de decepción que se deben desplegar.	
6.5.11	La solución debe poder crear señuelos para ambientes OT (Tecnología Operacional) y para redes SCADA (PLC, HMI, Sensores IoT, entre otros).	
6.5.12	La solución, al desplegar un señuelo, debe permitir una interacción completa sobre el mismo. Esto con el fin de evitar que el atacante detecte que se trata de un señuelo.	
6.5.13	La solución debe ofrecer diferentes tipos de señuelos para desplegar y adicionalmente, debe permitir la creación de señuelos personalizados.	

6.5.14	La solución debe soportar el marco de referencia MITRE para Sistemas de Control Industrial (MITRE ICS).	
6.5.15	Debe estar en la capacidad de crear señuelos falsos de los tipos presentes en la DIAN:	
6.5.16	La solución debe tener un motor de inteligencia que emplee técnicas Anti-Reconocimiento y Anti-Exploit para hacer rastreo de atacantes y correlación de campañas en tiempo real.	
6.5.17	Los indicadores de compromiso generados por la solución se deben poder compartir con diferentes herramientas de seguridad de la entidad. Incluido el formato STIX/TAXII	
6.5.18	La solución se debe integrar como mínimos con los siguientes elementos: Sistema de control de acceso a la red (NAC) Herramienta de Sandbox Solución SIEM Solución de respuesta automática (SOAR) BitDefender Solución de detección y respuesta en el endpoint (EDR)	
6.5.19	Debe ofrecer una representación visual tipo mapa que muestre en tiempo real los ataques o señuelos que han sido tocados por el atacante.	
6.5.20	Debe poder desplegarse en un entorno fuera de línea, sin acceso a internet.	
6.5.21	La solución debe contar con soporte de fábrica 7x24X365, garantía y actualizaciones de inteligencia de amenazas por un período de 3 años.	
7	Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas	
7.1	Marca (Especificar la marca de la herramienta del servicio ofrecido)	
7.2	Referencia o Modelo (Especificar el modelo de la herramienta del servicio ofrecido)	
7.3	Se debe licenciar como mínimo para 17727 activos que incluyen (15000 pc's, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web).	
7.4	Se debe suministrar una solución para Monitoreo de Red con Inteligencia Artificial con el objetivo de revisar el tráfico de red y alertar Cyberamenazas que existan en la red de la entidad.	
7.5	La solución debe ser centralizada, es decir, debe contar con una única interfaz de administración y visualización, desde la cual se pueda gobernar toda la solución y monitorear todo el entorno.	
7.6	El análisis del tráfico mediante los algoritmos de Machine Learning e Inteligencia Artificial debe realizarse de manera centralizada.	
7.7	El equipo que conforma el servicio debe ser instalado fuera de línea, es decir, la recepción del tráfico de red debe hacerse a través de puertos pasivos (spam port), de tal manera de no causar retardos en el desempeño de la red.	
7.8	La solución debe realizar un análisis completo del tráfico.	
7.9	La herramienta debe soportar los siguientes modos de implementación: Port mirror (SPAN PORT)	
7.10	La herramienta debe utilizar modelos matemáticos probabilísticos de estimación, analizando y correlacionando múltiples dimensiones distintas dentro del paquete, con el fin de validar los comportamientos anómalos en la red.	
7.11	El servicio debe proporcionar visibilidad completa de la red, incluidas las tecnologías tradicionales y no tradicionales (SD-WAN).	
7.12	El servicio debe poder identificar cualquier comportamiento anómalo en el entorno y alertar sobre estos comportamientos en tiempo real	
7.13	El servicio debe ser capaz de identificar cualquier dispositivo nuevo en la red	
7.14	Capacidad de realizar consultas a los datos capturados y almacenados en el hardware de uso específico (appliance) sin conectarse a la nube, como mínimo se debe tener un tiempo de retención de seis (6) meses.	
7.15	La solución debe poder realizar una captura de paquetes en tiempo real que permita un monitoreo de incidentes en el momento de su ocurrencia, así como ofrecer la opción de análisis exhaustivo de paquetes tanto en Wireshark como dentro de su propia interfaz de usuario.	
7.16	La solución debe permitir la personalización y adaptación del aprendizaje automático a condiciones y características específicas de la red.	
7.17	Capacidad para identificar cualquier amenaza anómala en la red en tiempo real a través del aprendizaje automático e inteligencia artificial.	
7.18	El oferente y/o contratista deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años.	
7.19	El servicio debe basarse en un sistema de seguridad que reciba todo el tráfico de la red desde uno o varios switches, lo analice e identifique las amenazas o incidentes que están ocurriendo en la red	
7.20	Después del período de aprendizaje inicial, la tecnología debe proporcionar automáticamente un seguimiento de auditoría completo de todos los dispositivos en el entorno, clasificando previamente al menos el tipo de dispositivo, el nombre de host, la dirección MAC, la primera y la última vez que se detectó el dispositivo en la red	
7.21	El servicio debe basarse en el análisis de comportamiento y correlación inteligente pudiendo detectar: o Toda conectividad inusual en la red. o Todas las actividades anómalas en la red. o Ser capaz de hacer un seguimiento detallado del dispositivo, indicando incluso su historial de dirección IP, uso del protocolo DHCP, etc. o Tener la capacidad de hacer un seguimiento detallado del usuario indicando incluso todos los nombres de host asociados a unas determinadas credenciales. o Identificar un volumen de conexiones significativamente inusual. o Identificar el nivel de rareza de un dispositivo en la red, así como el nivel de rareza de un acceso a un sitio externo	
7.22	La solución debe tener capacidad de detectar como mínimo los siguientes tipos de brechas de seguridad: o Ataques de tipo botnet o Propagación de gusanos o Ataques de ransomware o Infiltración y exfiltración de datos o Troyanos bancarios	

	<ul style="list-style-type: none"> o Credenciales comprometidas o Minería de bitcoins o Malware o Ataques de DDoS a través de dispositivos IoT o Amenazas avanzadas persistentes (APT) 	
7.23	<p>La tecnología deberá proporcionar la capacidad de realizar procedimientos automatizados por parte del proveedor del servicio para la cacería de amenazas basados en inteligencia artificial con al menos las siguientes capacidades:</p> <ul style="list-style-type: none"> o Procesos de Threat Hunting basados en anomalías de comportamiento detectadas por la inteligencia artificial. o Los procesos de Threat Hunting deberán indicar las fases del ciberataque en lo que se hayan visto la/las anomalías detectadas en el comportamiento. o El proceso de Threat Hunting deberá poder correlacionar anomalías detectadas dentro de la misma plataforma de IA e identificar si pertenecen o no a un ataque más complejo. Se deben validar con otras fuentes de información que lleguen al correlacionador para dar mayor contexto a los hallazgos identificados por la inteligencia Artificial. o Se deberá poder integrar el proceso de Threat Hunting automatizado para que otros servicios vía API puedan solicitar informes de cacería de amenazas de manera automatizada. o Se deben poder solicitar investigaciones autónomas y a demanda a la inteligencia artificial, donde el disparador pueda ser una anomalía ya detectada o una simple investigación a demanda. o El proceso de Threat Hunting deberá proporcionar un informe base entregado por la inteligencia artificial y uno adicional con la información de contexto y otras investigaciones adicionales realizadas por los analistas humanos. o El proceso deberá tener la capacidad de realizar investigaciones continuas 24/7 y en tiempo real de las anomalías detectadas por la inteligencia artificial o Se deberán realizar procesos de Threat Hunting manuales basados en TTP's mitre de manera recurrente, identificando qué anomalías detectadas por la plataforma de Inteligencia Artificial hacen parte de las técnicas buscadas para cada ejercicio de Treath Hunting propuesto. 	
7.24	<p>Debe poder realizar investigaciones autónomas basadas en inteligencia artificial, sea por demanda a través de la interfaz gráfica y/o a través de la integración vía API, esta investigación debe incluso poder realizarse sin intervención humana y generar un reporte donde se evidencia al menos un resumen ejecutivo del incidente, las alertas que fueron investigadas que hacen parte de incidente e información técnica de cada uno de los eventos identificados, asociándolos a la fase del Cyber Kill Chain y a una posible TTP de framework ATT&CK Mitre.</p>	
7.25	<ul style="list-style-type: none"> • El servicio debe alertar automáticamente sobre todas las actividades inusuales y anómalas en la red 	
7.26	<p>La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así:</p> <ul style="list-style-type: none"> o La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno o Debe funcionar completamente en función del comportamiento, donde no se permitan las tecnologías que hacen uso de reglas y / o firmas 	
7.27	<p>La Investigación basada en Inteligencia Artificial debe generar un reporte como resultado del proceso investigativo que contenga como mínimo:</p> <ol style="list-style-type: none"> i. Una reconstrucción cronológica de los eventos que hacen parte del Incidente. ii. Un resumen del incidente con una narrativa basada en procesamiento de lenguaje natural que describa a alto nivel los comportamientos evidenciados durante el incidente. iii. Detalles técnicos relevantes a la investigación realizada como direcciones Ips, Hostnames, cuentas de usuario involucradas, saltos de conexión, cantidad de transferencia de datos, destinos externos, rareza de los destinos, rareza de las conexiones y resúmenes de conexiones. 	
7.28	<p>La solución debe ser OPEN API O API RESTFULL , que admita integraciones con otros elementos de seguridad al menos en los formatos, CEF, LEEF, JSON, SYSLOG, entre otros.</p>	
7.29	<p>La solución debe utilizar varios algoritmos de inteligencia artificial, así como varias técnicas de Machine Learning como: Deep Learning, Machine Learning supervisado y Machine Learning no supervisado</p>	
7.30	<p>La tecnología debe ser auto-configurable, es decir, debe tener capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real.</p>	
7.31	<p>La solución debe poder reconocer nuevas amenazas que no hayan sido advertidas previamente (Zero Day)</p>	
7.32	<p>La solución debe tener la capacidad de modelar el comportamiento normal a nivel de usuario, dispositivos y red y a partir de estos identificar de forma autónoma las anomalías que corresponden a brechas de seguridad.</p>	
8	Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones	
8.1	<p>Marca (Especificar la marca ofrecida)</p>	
8.2	<p>Referencia o Modelo (Especificar el modelo ofrecido)</p>	
8.3	<p>La entidad requiere de una herramienta de software como servicio (SaaS), para el análisis de código estático tipo SATS y análisis de código dinámico tipo DAST para un total de cincuenta (50) aplicaciones.</p>	
8.4	<p>Dentro del servicio del SOC el contratista debe realizar análisis de vulnerabilidades y análisis automático y manual del código fuente de las aplicaciones de la entidad cada vez que se requiera validar La aplicación de las prácticas de SDLC sobre los desarrollos de la DIAN de acuerdo con el procedimiento de desarrollo seguro vigente referenciado por DIGIT (Dirección de Gestión de Información y Tecnología) de la DIAN.</p>	
8.5	<p>Dentro de los servicios del SOC se debe administrar y configurar los componentes de una solución de análisis de vulnerabilidades para Código fuente con módulos como son SCA, SCC, WEB Inspect, Runtime y sensores cuando sea requerido, y escalar a DIGIT y/o fabricas los eventos presentados para su solución.</p>	
8.6	<p>Debe dar soporte a las fábricas de desarrollo y pruebas en el proceso de Desarrollo Seguro 3 El contratista debe renovar y mantener el licenciamiento durante La ejecución del contrato, actualizar políticas, firmas y componentes de la herramienta utilizada cuando sean Liberadas por el fabricante.</p>	
8.7	<p>El contratista debe estar en la capacidad de dar transferencia de conocimiento para la correcta ejecución de pruebas y del uso de la herramienta.</p>	

8.8	El contratista debe crear los soportes requeridos en las auditorias.	
8.9	Documentar los cambios que se realicen sobre la herramienta y gestionarlos.	
8.10	Apoyar las acciones de remediación para el manejo de bugs o fallos de codificación en el software analizado	
8.11	Identificar deficiencias en la programación de funciones de autenticación, registro, cifrado, manejo de errores y procesamiento de datos	
8.12	Garantizar el correcto funcionamiento y la disponibilidad de la herramienta de análisis de código.	
8.13	Se deben ejecutar análisis estáticos, dinámicos e híbridos de los diferentes aplicativos concertados previamente con la DIGIT, cumpliendo con los requerimientos que la solución escogida establezca, Lo anterior, siguiendo el procedimiento de desarrollo seguro definido por la DIAN.	
8.14	Se deben generar los respectivos informes donde se presenta un resumen ejecutivo de las vulnerabilidades de desarrollo encontradas.	
8.15	Se deben generar los respectivos informes de desarrollo donde se describen las vulnerabilidades encontradas, junto con las recomendaciones de la solución asociados a las buenas prácticas de desarrollo de código seguro establecidas por el fabricante y según los lineamientos de la DIAN.	
8.16	Se deben generar los respectivos sets de pruebas para análisis estático y análisis dinámico ejecutado y debidamente firmado entre las partes.	
8.17	Apoyar con los recursos necesarios (personal idóneo) constantemente a la Dian realizando el respectivo acompañamiento, apoyo, experticia, experiencia, conocimiento en la resolución y remediación de todas y cada una de las vulnerabilidades encontradas durante la ejecución del contrato, se aclara que el personal de la Dian estará al frente de dichas actividades.	
8.18	El contratista debe utilizar también herramientas para SCA (Software Composition Analysis), utilizada para revisar todos los componentes open source y las librerías incorporadas en los proyectos de desarrollo.	
8.19	Dicha herramienta puede tener en cuenta SBOM (Software Bill Of Materials), detallando el inventario de componentes de software libre y contenedores, Open Source Vulnerability Management que permite hacer referencias cruzadas con bases de datos de vulnerabilidades para las componentes detectadas y Open Source Management Licenses, dada que algunas componentes no son del todo de uso libre.	
8.20	En el ciclo de desarrollo las herramientas del contratista deben utilizar SASE (Secure Access Services Edge), buscando seguridad en dispositivos móviles, Internet de las cosas y migración de aplicaciones on-premise hacia Cloud.	
8.21	El contratista debe tener el servicio de gestión y remediación según lo reportado en la herramienta, de modo que sirva de apoyo al área de DIGIT, para resolver todos los casos a remediar según los informes y dashboards que muestre la respectiva herramienta. El contratista debe poner a disposición el recurso humano para generar planes de acción sobre la información reportada en la herramienta.	
8.22	El Fabricante y/o canal Autorizado deberán tener la experiencia para prestar y dar soporte al Servicio de Escaneo de Aplicaciones contratado. Además del fabricante, el canal autorizado debe tener la capacidad de proporcionar servicios de Gestión de Programas de Seguridad en las Aplicaciones, Asesoría en Remediación y Pruebas de Penetración	
8.23	Debe permitir detectar vulnerabilidades en código fuente de forma estática	
8.24	Debe soportar lenguajes como: <ul style="list-style-type: none"> •Java •JavaScript •Python •Php •Ruby •C++ •C •C# 	
8.25	Debe permitir detectar vulnerabilidades en bibliotecas de terceros.	
8.26	Debe permitir la ejecución de pruebas dinámicas dirigidas a URL de aplicaciones Web.	
8.27	Debe integrar pruebas de seguridad en los principales entornos de integración continua (CI).	
8.28	Debe integrar pruebas de seguridad en los principales entornos de despliegue continuo (CD).	
8.29	Debe detectar automáticamente el lenguaje del código fuente a analizar.	
8.30	Determinar automáticamente los scanner de código a utilizar en función del lenguaje, atributos y configuración de la aplicación.	
8.31	Debe permitir integración nativa con las principales plataformas de CI/CD tales como: <ul style="list-style-type: none"> •GitHub Actions •GitLab •Jenkins •Travis •Azure DevOps •Bamboo •CircleCI 	
8.32	Debe permitir ejecutar análisis de seguridad manuales al código fuente de las aplicaciones.	
8.33	Debe permitir ejecutar análisis de seguridad automáticos al código fuente de las aplicaciones.	
8.34	Debe tener la capacidad de ejecutar análisis tipo SCA/OSS.	
8.35	Debe tener la capacidad de ejecutar análisis orientados a detección de secretos.	
8.36	Debe contar con la capacidad de definir puntuación general del riesgo de la aplicación.	
8.37	Debe determinar la gravedad de la vulnerabilidad basada en la clasificación del riesgo.	
8.38	Debe contar con la capacidad de correlacionar y priorizar automáticamente los riesgos más críticos a remediar.	
8.39	Debe integrar un panel que permita la visualización consolidada con detalles básicos en el cual se enumeren todas las aplicaciones escaneadas.	
8.40	El panel debe consolidar y clasificar integralmente los resultados generados en función de los escáneres utilizados (SAST, DAST, SCA/OSS y detección de secretos).	
8.41	El panel de visualización debe enumerar las vulnerabilidades encontradas por cada tipo de escáner.	

8.42	El panel de visualización debe categorizar los hallazgos por gravedad.	
8.43	El panel de visualización debe categorizar los hallazgos por la calificación de riesgo asignada.	
8.44	La solución debe permitir visualizar: <ul style="list-style-type: none"> • Número de archivos escaneados o Los tipos de escáner utilizados o UUID • ID de la organización • La hora en que se agregó la aplicación y se escaneó por última vez 	
8.45	Debe tener la funcionalidad de visualizar en detalle las vulnerabilidades de una aplicación, en el cual se muestre: <ul style="list-style-type: none"> • Archivo asociado • Número de líneas (SAST) o URL(DAST) • Severidad de la vulnerabilidad • Descripción • CVE asociado, si existe. • El número de instancias en las que se encuentra • Historia de la vulnerabilidad que incluye el tiempo de su primera y última aparición. • Estado de la Vulnerabilidad (Activa o Cerrada). 	
8.46	Debe permitir la modificación manual del estatus de la vulnerabilidad utilizando criterios como mínimo: <ul style="list-style-type: none"> • Nuevo: Esta es una nueva vulnerabilidad detectada por el escaneo. • Confirmado: esta es una vulnerabilidad real y requiere una solución. • En revisión: esta vulnerabilidad se encuentra actualmente en revisión o se está analizando para tomar medidas adicionales. • Revisado: la revisión de vulnerabilidad está completa. • Reabierto: la vulnerabilidad reparada es detectada nuevamente en el nuevo análisis y requiere ser abordada. • Resuelto: esta vulnerabilidad está reparada y no aparece en el siguiente resultado del análisis. • Riesgo aceptado: esta vulnerabilidad es un riesgo aceptado y continúa existiendo sin ningún daño potencial. • Falso positivo: esta vulnerabilidad es una falla potencial en el escáner o es indicativa de una característica única de la aplicación. • Eliminado: esta vulnerabilidad se pasa por alto en los escáneres. 	
8.47	Debe permitir filtrar los resultados según: <p>Clasificación de riesgo calculada: filtrado en función de la clasificación de riesgo asignada.</p> <p>Estado: filtrado según el estado.</p> <p>Categoría: filtrada en función de la aplicación específica. o Archivos: filtrado en función de los archivos específicos.</p>	
8.48	Debe permitir filtrado en función de los directorios específicos.	
8.49	La solución debe contar con documentación on-line para configurarla, administrarla y hacer uso de ella.	
9 Especificaciones Técnicas Protección de Marca (Deep&Dark Web)		
9.1	Marca (Especificar la marca ofrecida)	
9.2	Referencia o Modelo (Especificar el modelo ofrecido)	
9.3	Se debe licenciar para 260 activos públicos	
9.4	La herramienta/servicio debe rastrear y monitorear continuamente la presencia en línea de la marca en sitios web, redes sociales, foros, blogs y otros espacios digitales relevantes para identificar cualquier uso no autorizado o infracción de la marca.	
9.5	La herramienta/servicio debe identificar automáticamente posibles infracciones de marca, como el uso no autorizado del logotipo, el nombre de la marca.	
9.6	La herramienta/servicio debe enviar notificaciones inmediatas o alertas en tiempo real cuando se detecten infracciones de marca para que puedan abordarse de manera rápida y efectiva.	
9.7	La herramienta/servicio debe realizar la creación y gestión de casos para seguir el progreso de las acciones tomadas contra infractores, incluidas las comunicaciones legales, las medidas de cumplimiento y las soluciones	
9.8	La herramienta/servicio debe cumplir con los estándares de seguridad de datos para proteger la información confidencial relacionada con la marca y sus actividades de protección.	
9.9	Generar informes detallados mensualmente o bajo demanda cuando la Entidad así lo requiera, sobre actividades de protección de marca, incluidas estadísticas de monitoreo, acciones tomadas y resultados obtenidos.	
9.10	Realizar análisis retrospectivos y comparativos para evaluar la efectividad de las estrategias de protección de marca y ajustarlas según sea necesario	
9.11	Incluir capacidades de análisis de percepción para evaluar cómo se percibe la marca en línea y detectar cualquier tendencia negativa o potencial crisis de reputación.	
10 Especificaciones Técnicas Ethical Hacking		
10.1	Se deben realizar como mínimo dos (2) ejercicios de ethical hacking por año durante la vigencia del contrato del Centro de Operaciones de Seguridad de la Entidad, para lo cual el contratista deberá entregar el respectivo cronograma el cual debe incluir como mínimo las etapas de preparación, ejecución de pruebas, análisis y elaboración de informes.	
10.2	El alcance de los ejercicios de ethical hacking no se limita únicamente a los activos críticos de la entidad sino también a los que hacen parte del anexo de inventarios de éste proyecto. Aunque se priorizarán activos de relevancia en cada ejercicio, la selección de activos incluirá aquellos que la DIAN considere esenciales para evaluar la postura de seguridad de la infraestructura tecnológica en general. La determinación específica de los activos a incluir se hará en la fase de planeación de cada ejercicio, en conjunto con el contratista, de acuerdo con las necesidades de seguridad identificadas (como mínimo cien (100) activos).	

10.3	Los ejercicios a realizar deben ser de caja gris.	
10.4	La cantidad mínima de activos tecnológicos de información por ejercicio de ethical hacking sera de cien (100) activos, de acuerdo a los inventarios de activos entregado en este mismo archivo en sus hojas adyacentes.	
10.5	El contratista deberá establecer protocolos claros para la comunicación durante el proyecto, incluyendo puntos de contacto, actualizaciones regulares y manejo de hallazgos críticos.	
10.6	El contratista debara preparar un plan de respuesta a incidentes en caso de que se descubran vulnerabilidades graves.	
10.7	Para realizar los ejercicios de Ethical Hacking el contratista debe disponer de un equipo como mínimo de tres (3) ingenieros con conocimientos en programación, sistemas operativos y estar certificados en hackin ético.	
10.8	El personal destinado por el contratista para realizar estos ejercicios debe ser completamente diferente al personal destinado por el contratista para la implementación y operación del SOC.	
11	Especificaciones Implementación de todas las Plataformas Entregadas	
11.1	El contratista deberá realizar la Instalación, Implementación, configuración y puesta en marcha de todas las soluciones ofertadas, así como los equipos ofertados tanto físicos como virtuales con personal profesional e idóneo para realizar las labores pertinentes.	
11.2	Planeación de cada una de las actividades, validadas en conjunto con la entidad.	
11.3	Implementación de todas las soluciones y servicios entregados de acuerdo a las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura.	
11.4	Todos los elementos necesarios para la implementación de cualquiera de las capacidades requeridas por la Entidad en este proyecto, debe ser provista por el futuro oferente, entendiéndose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.	
11.5	Pruebas de Servicio de las plataformas ofertadas.	
11.6	El contratista deberá garantizar soporte y garantía para las plataformas ofertadas en un esquema 7 x 24 x 365 por tres (3) años.	
11.7	Realizar levantamiento de información previo a la instalación de todas las soluciones y las plataformas entregadas. La entidad dispondrá de los recursos humanos suficientes y necesarios para apoyar las labores propias de esta contratación, previo acuerdo entre las partes.	
11.8	Ubicaciones para implementación y configuración: El oferente contará con un Centro de Operaciones de Seguridad SOC en la ciudad de Bogotá, donde se implementarán todos y cada uno de los servicios, dispositivos, plataformas, soluciones y demás productos que hagan parte de los requerimientos de la Entidad en este proyecto.	
11.9	El contratista deberá guardar estricta reserva sobre cualquier información interna de la DIAN obtenida durante la prestación de los servicios tecnológicos contratados, esto mediante firma de cláusulas de confidencialidad de la información.	
11.10	El contratista deberá reportar a la DIAN, las sugerencias que contribuyan a la obtención de las mejores prácticas de operación de las plataformas y soluciones tecnológicas adquiridas.	
11.11	Todo el cableado eléctrico, lógico, patchs cords, conectores, patch panels y demás elementos y accesorios necesarios para la instalación deben ser provistos por el oferente o contratista. Se debe entender que es un contrato llave en mano, donde todos los componentes de las soluciones deben estar a cargo del oferente o contratista.	
11.12	Presentar Plan de trabajo y cronograma de trabajo dentro de los cinco (5) días calendario siguientes a la suscripción del acta de inicio, para aprobación del supervisor y realizar los ajustes a que haya lugar.	
11.13	El contratista deberá ejecutar la configuración de todos los ítems del presente Anexo de Características Técnicas Mínimas	
11.14	La implementación deberá comprender los siguientes puntos: <ul style="list-style-type: none"> • Diseño y planeación de cada una de las actividades minimizando la afectación del servicio. • Configuración y alistamiento de todas las plataformas o soluciones ofertadas a la última versión estable aprobada por los fabricantes. • Implementación de la soluciones y plataformas de acuerdo a las mejores prácticas de los fabricantes, teniendo en cuenta una arquitectura de red segura, alineada a los requerimientos actuales de la DIAN. • Pruebas de Servicio. • Puesta en Producción. • Estabilización de las plataformas. • Mantenimiento y mejora continua. 	
11.15	Será de la autonomía y responsabilidad del contratista la vinculación, organización, orientación y control del personal a su cargo, comprometiéndose a cumplir con las normas de seguridad existentes en la DIAN. Se aclara que, la DIAN no adquiere ninguna relación contractual, civil o laboral con los trabajadores de el Oferente.	
11.16	Todos los recursos tecnológicos, logísticos, de infraestructura, humanos y demás que se requieran para la implementación de los servicios incluidos en este documento, serán por cuenta del contratista, modalidad "llave en mano".	
11.17	Todas las plataformas y soluciones entregadas deberán ser de propósito específico, no se aceptan soluciones genéricas.	
11.18	Para los servicios o soluciones de tipo SaaS (Software como servicio) solicitados por la DIAN, el contratista deberá realizar el despliegue y entrega de la plataforma de gestión plenamente configurada de acuerdo al plan de trabajo, informando las funcionalidades que fueron desplegados o puestos al servicio de a Entidad, de acuerdo con los características ofertadas.	
11.19	Implementar las diferentes fases del proyecto bajo los estándares del PMBOK o metodologías ágiles, con el objeto, de garantizar la aplicación de conocimientos, habilidades, herramientas y técnicas estandarizadas en todas las actividades que se van a desarrollar durante el proyecto.	
11.20	Con su oferta el proponente deberá incluir datasheets o documentación pública del fabricante para validar su respectivo cumplimiento de cada uno de los requerimientos técnicos de la herramienta.	
12	Especificaciones Técnicas Servicios de Monitoreo	
12.1	La Entidad requiere servicios de un Centro de Operaciones de Seguridad - SOC, el servicio de SOC será realizado con las plataformas, soluciones y servicios adquiridos, así también con las plataformas y servicios prestados por parte del oferente. Se aclara que toda la infraestructura tecnológica de la Entidad cuenta con soporte y garantía por parte de los fabricantes con vigencias entre 2026 y 2028.	

12.2	Los servicios de monitoreo, correlación, administración, gestión, automatización y los demás que hagan parte del centro de operaciones de seguridad - SOC, deberán hacerse sobre toda la infraestructura tecnológica (appliance, plataformas, pc's, endpoints, aplicaciones, bases de datos, servidores, entre otros) estipulada en el archivo de inventarios que hace parte de este anexo técnico, y hasta copar las capacidades de licenciamiento solicitadas en este proyecto, con una disponibilidad de 7x24x365,	
12.3	La administración, operación, gestión de los servicios y demás actividades de las plataformas, soluciones, software, hardware, entre otros, que hacen parte de las capacidades requeridas por la Entidad en este proyecto, deben ser realizadas por el futuro oferente, por el tiempo de duración del proyecto.	
12.4	Dispositivos Adicionales: La Entidad solicitará incluir la cantidad de dispositivos adicionales que requiera hasta ocupar todo el licenciamiento de la herramientas y servicios adquiridos (SIEM, SOAR, NDR, Gestión de Vulnerabilidades, protección de bases de datos, entre otras).	
12.5	<p>Controles: El servicio de SOC ofrecido debe contemplar también el monitoreo de los siguientes controles tecnológicos pertenecientes al SGSI de la Entidad:</p> <ul style="list-style-type: none"> Dispositivos de punto final de usuario Derechos de acceso privilegiado Restricción de acceso a la información Acceso al código fuente Autenticación segura Gestión de la capacidad Protección contra malware Gestión de vulnerabilidades técnicas Gestión de la configuración Eliminación de datos Enmascaramiento de datos Prevención de la fuga de datos Copia de seguridad de la información Redundancia de las instalaciones de procesamiento de información Inicio de sesión Actividades de seguimiento Sincronización del reloj Uso de programas de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de redes Seguridad de los servicios de red Segregación de redes Filtrado web Uso de criptografía Ciclo de vida de desarrollo seguro Requisitos de seguridad de la aplicación Arquitectura del sistema seguro y principios de ingeniería Codificación segura Pruebas de seguridad en desarrollo y aceptación Desarrollo subcontratado Separación de los entornos de desarrollo, prueba y producción Gestión de cambios Información de prueba Protección de los sistemas de información durante las pruebas de auditoría 	
12.6	El contratista deberá realizar la integración de la herramienta GRC de NOVASEC propiedad de la DIAN con la plataforma SOAR, cuya función sea alimentar los riesgos de los controles tecnológicos de la ISO 270001 de modo tal que ante cualquier cambio en las herramientas que soportan estos controles sea informado al sistema GRC.	
12.7	El servicio debe permitir la integración del envío de alarmas automáticas vía correo electrónico.	
12.8	Los procesos de gestión y operación deben estar basados en las mejores prácticas establecidas por los modelos de procesos ITIL, CSIRT, ISO 27001:2022, NIST (CSF) o CERT.	
12.9	El SOC del contratista mediante el cual se prestarán los servicios debe estar certificado en ISO 27001, ser miembro FIRST™	
12.10	El servicio ofrecido deberá alinearse a las políticas, procesos, procedimientos y requerimientos de seguridad definidos por la Entidad.	
12.11	El servicio debe garantizar la disponibilidad, confidencialidad, integridad, no repudio, auditoría y privacidad de los datos y servicios soportados.	
12.12	El servicio debe incluir apoyo en la definición de estrategias de seguridad, que permitan fortalecer las políticas y controles de seguridad de la información.	
12.13	El servicio debe detectar actividades, técnicas inusuales y recolectar evidencias necesarias para determinar si se trata de un evento o incidente de seguridad, de acuerdo a los niveles de servicio.	
12.14	El contratista deberá realizar la correlación, monitoreo y casos de uso sobre las plataformas de la Entidad, de tal forma que todo el know how y parametrizaciones queden para la Entidad.	
12.15	Todas las labores de configuración de la herramienta de monitoreo y correlación de eventos y la generación de los casos de uso para el monitoreo SOC deberán ser ejecutadas por el personal del contratista asignado al proyecto SOC.	
12.16	El plan de trabajo entregado por el contratista deberá contener las etapas, resultados esperados, estrategias para asegurar el logro de los productos en los tiempos establecidos y describir los procesos/procedimientos, las técnicas y herramientas que utilizará en la ejecución del contrato	

12.17	Dentro del plan de trabajo deberá especificar la metodología que utilizará para administrar, configurar, monitorear y gestionar el servicio de monitoreo objeto del presente contrato, especificando etapas, recursos, entregables, herramientas y técnicas a utilizar. Nota: La Entidad se reserva el derecho de ajustar aspectos de la metodología.	
12.18	Cuando un evento de seguridad ocurre o está en suceso, el servicio de monitoreo SOC deberá identificarlo y estar en la capacidad de relacionar de forma directa o indirecta con otros eventos de seguridad asociados, determinando el patrón de ataque.	
12.19	El servicio debe incluir la personalización de reportes que la Entidad requiera durante la prestación del servicio.	
12.20	El servicio debe permitir la integración del envío de alarmas automáticas vía correo electrónico.	
12.21	Para la ejecución del contrato y el cumplimiento de los niveles de servicio solicitados, el contratista dispondrá del talento humano que él considere necesario.	
12.22	Proporcionar durante el período de la operación de los servicios un esquema de escalamiento interno a la herramienta.	
12.23	Los procesos de gestión y operación deben estar basados en las mejores prácticas establecidas por los modelos de procesos ITIL, CSIRT, ISO 27001:2013 o 27001:2022, NIST (CSF) o CERT. Nota: El contratista debe estar certificado en estas mejores prácticas de ISO 27001 en las versiones mencionadas, para su proceso de SOC.	
12.24	El servicio ofrecido deberá alinearse a las políticas, procesos, procedimientos y requerimientos de seguridad definidos por la Entidad.	
12.25	El servicio debe garantizar la disponibilidad, confidencialidad, integridad, no repudio, auditoría y privacidad de los datos y servicios soportados.	
12.26	El servicio debe incluir apoyo en la definición de estrategias de seguridad, que permitan fortalecer las políticas y controles de seguridad de la información.	
12.27	Mantener el inventario actualizado de dispositivos monitoreados de la solución.	
12.28	La actividad del servicio de monitoreo SOC, se centrará en el tratamiento de eventos, identificación de incidentes, los cuales contarán con un conjunto de metodologías y atención de procesos que permitirá brindar el alertamiento oportuno a los riesgos y amenazas. Por lo anterior, el personal del servicio deberá realizar el escalamiento y las comunicaciones por medio de correo electrónico y/o telefónico con el personal de la Entidad a fin de comunicar las incidencias presentadas. Adicionalmente realizará el seguimiento a los eventos hasta que estos sean cerrados adecuada y oportunamente.	
12.29	De forma permanente el servicio de monitoreo SOC realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo a la Entidad, resumiendo los resultados en Boletines o Informes extraordinarios de SOC. Los servicios de gestión de SOC realizarán seguimiento 7x24 a los ataques originados desde Internet al igual que los originados al interior de la Entidad. El SOC, debe definir la matriz de escalamiento de común acuerdo con los responsables de seguridad en la Entidad, clarificando el nivel de escalamiento según el tipo y nivel de incidente.	
12.30	El contratista realizará la integración y monitoreo de los dispositivos y activos tecnológicos que conforman la infraestructura tecnológica de la Entidad, según lo relacionado en el alcance del ÍTEM No. 2 "Infraestructura a ser monitoreada", del presente Anexo técnico.	
12.31	Una vez integrada toda la plataforma tecnológica, el contratista configurará y afinará la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos: * Actividades asociadas a la administración de cuentas de usuario final (UserID). * Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator). * Ejecución de comandos especiales sobre sistemas operativos. * Ejecución de comandos especiales sobre bases de datos (dump, drop, delete, insert, update). * Cambios de parámetros técnicos, de configuración o de seguridad. * Cambios de configuración horaria. * Cambios no autorizados en recursos tecnológicos críticos. * Actividades de conexión de cuentas de usuario final o administradores. * Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs. * Actividades asociadas a conexión de acceso remoto. * Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional.	
12.32	El proponente deberá tener un SOC Propietario.	
12.33	El oferente debe tener al menos tres (3) años, prestando el servicio, con SOC propietario, dentro del territorio nacional.	
12.34	El proveedor debe estar en la capacidad de prestar el servicio en el idioma español, para la interacción de las áreas de operación y tener al menos uno de sus centros de datos en Latinoamérica	
12.35	El SOC debe estar concentrado en un espacio físico. Indicar el área en m2	
12.36	El servicio debe incluir Threat Intelligence o Inteligencia Global, que permita usar un servicio mundial de amenazas identificadas.	
12.37	El Proponente debe demostrar algún reconocimiento del centro de gestión de seguridad propuesto (SOC), acompañado de una carta por el representante legal que consta que el SOC que propone cumple con los estándares requeridos por la DIAN (cumplimiento de todos y cada uno de los ítems solicitados en el anexo técnico, además de ser reconocido como un prestador de servicios SOC, tener capacidad instalada en Bogotá y contar con la respectiva experiencia).	
12.38	El servicio de SOC debe permitir gestionar el ciclo completo de un incidente desde su detección, análisis, escalamiento, cierre y documentación (con archivos de evidencias adjuntas) con la finalidad de generar una base de conocimiento.	
12.39	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 y debe alinearse a la metodología existente en la Entidad para la gestión de incidentes.	
12.40	El SOC deberá contar con procesos definidos para la detección, categorización y alertamiento temprano y oportuno de incidentes de seguridad.	
12.41	El SOC debe disponer de procesos para la gestión de cambio sobre la plataforma que soporta el servicio.	
12.42	El SOC debe disponer de herramientas colaborativas internas para el intercambio de información entre los funcionarios. Se deberá aportar una carta firmada por el representante legal del oferente evidenciando las herramientas colaborativas que se utilizan para la prestación del servicio.	
12.43	Tener los roles y responsabilidades del grupo de operaciones del SOC, está claramente definido, en lo que respecta al monitoreo, atención, manejo y contención de incidentes de seguridad.	
12.44	El SOC debe permitir a la DIAN realizar auditorías sobre los procesos, tecnologías, logs y personas que operan en el SOC, en caso de ser requerido.	

12.45	El SOC debe estar protegido al menos con tres anillos de seguridad física. Indicar cuantos anillos de seguridad utilizan para la protección física, describa cada uno de ellos, y quien provee el servicio de protección (Propio, condominio, administración, etc).	
12.46	El SOC debe tener protección física contra los siguientes posibles daños: Incendio, terremoto, manifestación social.	
12.47	El acceso al área donde se encuentran los analistas de gestión de eventos e incidentes de seguridad del SOC debe contar con doble factor de autenticación.	
12.48	El proponente deberá estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por falla en los servicios de suministro.	
12.49	El proponente deberá estar protegido para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado.	
12.50	Las instalaciones del SOC deben tener controles para los puntos de acceso por donde pueda ingresar personal no autorizado a las instalaciones del SOC	
12.51	El proponente deberá garantizar controles de acceso a cualquier repositorio de información que se requiera para los Clientes Gestionados para evitar el acceso no autorizado	
12.52	El proponente deberá contar con las herramientas necesarias para protección de Cualquier información para su visualización, procesamiento y/o almacenamiento.	
12.53	El servicio deberá contemplar los siguientes entregables: <ul style="list-style-type: none"> • Incidentes documentados. • Reportes periódicos de incidentes y a demanda. • Mitigación de incidentes de seguridad. 	
12.54	El monitoreo se realizará en horario 7x24x365 durante toda la duración del contrato.	
12.55	El servicio debe detectar actividades, técnicas inusuales y recolectar evidencias necesarias para determinar si se trata de un evento o incidente de seguridad, de acuerdo a los niveles de servicio.	
12.56	Las evidencias que sean recopiladas por el servicio de monitoreo SOC son propiedad de la Entidad y podrán ser solicitadas en cualquier momento para atención de requerimientos legales.	
12.57	El servicio de monitoreo SOC deberá analizar las diferentes alertas detectadas para descartar falsos positivos, antes de crear el caso/ticket en la herramienta institucional dispuesta para ello.	
12.58	Prestar el servicio desde un centro de operaciones de seguridad (SOC) ubicado en la ciudad de Bogotá D.C. (Colombia), cuya comunicación con la infraestructura de la Dian, se hará utilizando los canales de la Entidad.	
12.59	El servicio de monitoreo SOC se debe poder realizar en forma remota y disponer un personal en sitio solo cuando sea necesario.	
12.60	La herramienta SIEM que será adquirida por la Entidad, será administrada y operada por el contratista, con personal con experiencia en servicios de monitoreo de logs. La actividad de monitoreo y alertamiento se debe hacer en las instalaciones del contratista.	
12.61	Las herramientas adicionales que deba utilizar el contratista, tales como hardware, software, firmware, utilitarios o appliances, deben cumplir con la regulación de derechos de autor y propiedad intelectual. Así mismo, deben contar con soporte, mantenimientos y actualizaciones del fabricante o proveedor.	
12.62	Las herramientas adicionales que deba utilizar el contratista deben ser compatibles con la herramienta SIEM de la Entidad.	
12.63	Se deben generar alertas de otras amenazas que puedan impactar la infraestructura de la Entidad, como las identificadas en los reportes de análisis de tendencia de centros CSIRT/CERT o en las bases de datos de conocimiento del contratista.	
12.64	El centro de operación del contratista debe garantizar condiciones de seguridad mínimas en aspectos de acceso al espacio físico y acceso a las herramientas de software.	
12.65	El servicio de monitoreo SOC deberá mantener sincronizados todos los relojes de la herramienta SIEM con la hora legal colombiana, suministrada por el Instituto Nacional de Metrología de Colombia (https://inm.gov.co/web/servicios/hora-legal/).	
12.66	El servicio de monitoreo SOC debe ejecutar actividades permanentes para garantizar el descubrimiento y monitoreo de nuevos dispositivos en la red.	
12.67	El tiempo de custodia de los reportes, estadísticas, análisis de tendencia, métricas e indicadores será por la duración del contrato. Una vez terminado el vínculo contractual, el contratista deberá destruir toda la información a la que tuvo acceso de la Entidad.	
12.68	El contratista debe informar al equipo de seguridad de la información de la Entidad de manera inmediata, sobre cualquier evento o incidente real que se presenten en la infraestructura tecnológica.	
12.69	El contratista deberá presentar mensualmente o cada que sea requerido, los siguientes informes de: <ul style="list-style-type: none"> • Estado y resultados del servicio en el periodo de valoración, de tipo gerencial. • Eventos de actividad sospechosa atendidos durante el periodo. • Alertas, ataques, incidentes y tendencias. • Comportamientos más relevantes según la correlación realizada por el contratista. • Incidentes de seguridad presentados. • Estadísticas de la información procesada. • Hallazgos realizados sobre la plataforma tecnológica. • Análisis y recomendaciones sobre los resultados. 	
12.70	La Entidad podrá solicitar los informes que considere pertinentes, en la medida en que se vayan integrando nuevas herramientas.	
12.71	El contratista deberá generar reportes de eventos y de análisis de tendencias, para tomar las acciones preventivas, tales como: instalación de parches, actualización de versiones, modificación de políticas y configuraciones. Además, debe quedar registros de cuándo, dónde y cómo se presentan los incidentes, así como definir nuevos reportes acorde a las necesidades de la Entidad.	
12.72	El contratista deberá entregar un informe preliminar de un incidente sucedido. Este debe ser remitido a la Entidad posterior a la declaración del evento o incidente y después de la investigación de la actividad sospechosa o incidentes de seguridad se entregará el informe final detallado del mismo.	

12.73	<p>Los servicios ofrecidos deberán poder ser visualizados a través de tableros de control que permitan ver métricas en línea de acuerdo a las necesidades de la Entidad, por ejemplo:</p> <ul style="list-style-type: none"> • Alertas/Incidentes por tipo • Alertas/Incidentes nuevos y resuelto • Tiempo medio de creación de alertas/incidentes • Tiempo medio de solución • Tendencias y top de alertas/incidentes • Cumplimiento de acuerdos de servicio • Nivel de disponibilidad del servicio 	
12.74	Categorías de eventos de seguridad, mínimos para monitorear	
12.74.1	Cuentas Privilegiadas	
	Autenticación fallida	
	Autenticación exitosa	
	Usuario agregado a grupo especial local (cambio de privilegios)	
	Usuario eliminado de grupo especial local (cambio de privilegios)	
	Usuario agregado a grupo especial global (cambio de privilegios)	
	Usuario eliminado de grupo especial global (cambio de privilegios)	
	Cuenta bloqueada	
	Cuenta desbloqueada	
	Contraseña cambiada	
	Cambios de perfiles y permisos de cuentas privilegiadas	
12.74.2	Actividades de administración de cuentas (creación, eliminación, cambio de perfiles)	
	Elevación de privilegios a usuarios	
	Bases de datos	
	Autenticación exitosa - cuenta ordinaria	
	Autenticación fallida - cuenta ordinaria	
	Autenticación exitosa - SA	
	Autenticación fallida - SA	
	Cuenta bloqueada	
	Cuenta desbloqueada	
	Usuario agregado al grupo de SA	
	Ejecución de instrucciones DML (Insert, Update y Delete) sobre tablas en producción por usuarios no autorizados	
Ejecución de instrucciones DDL (Copia, (dump), Create, Drop, Alter) sobre tablas en producción por usuarios no autorizados		
Acceso de desarrolladores		
Actualización de cuentas		
12.74.3	Cambios sobre plataformas - Windows	
	Software instalado en Servidor Windows	
	Software desinstalado en Servidor Windows	
	Archivo crítico modificado (control de integridad)	
	Cambio en políticas del Directorio Activo	
Eliminación de logs de auditoría		
12.74.4	Cambios sobre plataformas - Linux	
	Software instalado en Servidor Linux	
	Software desinstalado en Servidor Linux	
	Archivo crítico modificado (control de integridad)	
Eliminación de logs de auditoría		
12.74.5	Conexiones	
	Acceso remoto	
	Cantidad inusual de conexión a los dispositivos, equipos, servidores y base de datos.	
12.74.6	Comportamiento sospechoso	
	Ataques de fuerza bruta.	
	Instalación o descarga de software no autorizado.	
	Acceso no autorizado a carpetas restringidas.	
	Patrones de virus informáticos o códigos maliciosos.	
	Ejecución de secuencia de operaciones y/o transacciones sobre los sistemas de información que pueden implicar fraudes	
12.74.7	Auditoría	
	Cambios de parámetros de seguridad	
	Archivos críticos del sistema operativo modificados	
	Cambios de políticas en Directorios Activos	

	Eliminación de logs de auditoría Modificación de winlogon.exe	
12.74.8	Tiempos de alertamiento y escalamiento al equipo de respuesta a incidentes de seguridad de la Entidad: <ul style="list-style-type: none"> • De impacto crítico: alertamiento dentro de los primeros 30 minutos y escalamiento en máximo 1 hora. • De impacto alto: alertamiento dentro de los primeros 60 minutos y escalamiento en máximo 2 horas • De impacto moderado: alertamiento dentro de las primeras 2 horas y escalamiento en máximo 12 horas • De impacto bajo: alertamiento dentro de las primeras 12 horas y escalamiento en máximo 24 horas. 	
12.75	Los informes de servicio deberán ser enviados los cinco (5) primeros días hábiles del mes. Los documentos entregables e informes que el contratista presente, deben contar con un formato de presentación estándar, redacción clara, buena ortografía y en idioma español.	
12.76	El servicio deberá estar enmarcado en el cumplimiento de la norma ISO 27001 del 2013 (SGSI) en su anexo A numeral 16: <ul style="list-style-type: none"> • A.16.1.1 Responsabilidades y procedimientos • A.16.1.2 Reporte de eventos de seguridad de la información • A.16.1.3 Reporte de debilidades de seguridad de la información • A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Nota: El contratista debe ser certificado ISO 27001 DEL 2013 o superior (SGSI) para su proceso de SOC, en caso de uniones temporales los integrantes de dicha unión deben ser certificados en ISO 27001 y ser miembros avalados de FIRST cada uno.	
12.77	Los incidentes deben ser gestionados de acuerdo con: <ol style="list-style-type: none"> 1. Planificar y preparar: establecer una política de gestión de incidentes de seguridad de la información y formar un Incident Respuesta Team (Grupo de respuesta de incidentes). 2. Detección e informes: El contratista deberá detectar e informar "eventos" que pueden ser o convertirse en incidentes. 3. Evaluación y decisión: El contratista deberá evaluar la situación para determinar si de hecho se trata de un incidente. 4. Respuestas: El contratista deberá reportar de manera oportuna al equipo de seguridad de la Entidad para que pueda contener, erradicar y remediar. 5. Lecciones aprendidas: El contratista deberá documentar la gestión de los riesgos de la información como consecuencia de las incidencias experimentadas. 	
12.78	ISO27001: El oferente debe presentar junto con su propuesta el certificado ISO 27001 DE 2013 (SGSI) O Spara su proceso de SOC.	
12.79	ISO22301: El oferente debe presentar junto con su propuesta el certificado ISO 22301 (Continuidad del Negocio).	
12.8	La DIAN realizará una visita presencial a las instalaciones del SOC, donde el oferente deberá cumplir con las garantías de las normativas en ISO 27001. Esta visita deberá ser coordinada con el gerente del proyecto.	
12.81	El servicio del SOC deberá contar con mínimos dos (2) centros de datos geográficamente ubicados en diferentes lugares dentro de Bogotá D.C o uno de estos puede estar fuera de Bogotá, siendo este para contingencia o alta disponibilidad, aclarando que el datacenter principal de donde se prestará el servicio de SOC y las capacidades contratadas, debe encontrarse en la ciudad de Bogotá. El proponente debe especificar la cantidad de Centro de Datos de los que dispone para el SOC, su ubicación y el rol de cada uno de ellos.	
12.82	El contratista deberá prestar el servicio de acompañamiento, asesoramiento, generación de planes de remediación entre otros para la solución de todas las vulnerabilidades e incidentes encontrados durante el tiempo que dure el contrato, para lo cual deberá contar con personal en sitio (mínimo un Ingeniero) en el horario laboral entre semana (8x5) y si por alguna circunstancia fortuita o de acuerdo a la necesidad de la DIAN (bajo demanda de la Entidad), se podrán coordinar sesiones en horario no hábil.	
13	Garantía y Soporte Técnico por tres (3) años.	
13.1	Los appliances, plataformas, dispositivos y componentes ofertados deben ser nuevos de fábrica, no re-manufacturados, ni reparados, ni reacondicionados en ninguna de sus partes.	
13.2	Las actualizaciones de software, firmware y parches/fixes de toda la plataforma y dispositivos entregados, deben ser realizadas por el contratista periódicamente en forma integrada y considerando todos los componentes. Una vez el fabricante o fabricantes de los dispositivos entregados, libera las nuevas versiones. De común acuerdo la Entidad programará dichas actividades para que el contratista proceda a realizarlas y probarlas. Por lo tanto, su periodicidad depende exclusivamente de la liberación de las actualizaciones de los fabricantes y deberá hacerse por los tres (3) años del soporte y garantía.	
13.3	El soporte requerido para la soluciones ofertadas deberá ser provisto por el contratista durante el tiempo de garantía ofrecido.	
13.4	El contratista deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 7x24X365 (telefónico, e-mail, acceso remoto o presencial en caso de que la DIAN así lo requiera, este soporte deberá ser suministrado por personal especializado en las plataformas entregadas. <p>La atención se debe prestar dentro de las dos (2) horas siguientes al reporte de incidente, la solución en un tiempo máximo de ocho (8) horas calendario. En el caso específico que se requiera de soporte de tercer nivel (fabricante), toda estas labores y demás labores propias del soporte y garantía serán gestionadas por el contratista, quien deberá escalar, gestionar y realizar todos los procedimientos que el fabricante solicite, en cuyo caso se establece un tiempo máximo de dos (2) días calendario para la solución definitiva</p>	
13.5	Para la prestación del servicio de soporte, el contratista deberá contar con el personal idóneo, el cual le permita solucionar los requerimientos de soporte durante la vigencia del contrato.	
13.6	En caso de requerirse una reconfiguración parcial o total de todas las plataformas entregadas en cualquiera de sus componentes, por fallas en su funcionamiento, la misma deberá ser realizada por el Contratista sin incurrir en costos para la Entidad.	

13.7	Realizar visitas de seguimiento técnico para mantenimiento preventivo a la plataformas ofertadas e implementadas, de manera cuatrimestral, durante el tiempo de garantía, soporte y la duración del presente proceso contractual, para lo cual el contratista deberá realizar y documentar entre otras, las siguientes actividades como parte del mantenimiento, previa coordinación con el supervisor del contrato en desarrollo: Revisar, diagnosticar y afinar todas las plataformas y dispositivos entregados, así como el desempeño de sus capacidades.	
13.8	Durante el tiempo de garantía ofrecido, se deberá garantizar soporte de la solución con ingenieros certificados en cada unos de los elementos y componentes de la plataforma implementada.	
13.9	El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil. (En el esquema de soporte definido para la solución implementada para la DIAN)	
13.10	El contratista deberá incluir la garantía de reemplazo de unidades completas, componentes, tarjetas, cables, accesorios o partes en la modalidad 7x24x365 durante un periodo que dure el presente contrato, para todos y cada uno de los componentes de la solución implementada.	
13.11	Al finalizar cada visita correctiva y/o preventiva el contratista generará un informe de servicio en la que constará el resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones, así como las evidencias de estas actividades. De igual forma, quedará constancia en el mismo acta o informe de servicio si hubo cambio de software, hardware y/o en alguna configuración.	
13.12	Se debe ofrecer todos los mecanismos, herramientas y procedimientos necesarios para mantener los niveles de disponibilidad requeridos y exigidos por la DIAN.	
13.13	El contratista deberá registrar, gestionar y hacer seguimiento a cualquier incidente reportado por la DIAN, además durante la atención inicial del caso se determinará su criticidad y la metodología para su resolución.	
13.14	Niveles de Atención que debe prestar el contratista: -Un primer nivel de atención con Agente Nivel I de la Mesa de Ayuda a través de la ejecución de un checklist, en conjunto con la Entidad, y la validación del respectivo problema. -Si la incidencia no es resuelto se deberá asignar un Ingeniero de Soporte de Nivel II para proceder con la atención remota o en sitio del incidente. -Si la incidencia persiste, el Ingeniero de Soporte de Nivel II procederá a gestionar la apertura de un ticket con el TAC del fabricante para dar pronta solución al incidente.	
13.15	Tiempos de Atención Se detallan los tiempos de atención requeridos por la Entidad para la atención de incidentes de seguridad u operación, este tiempo se define como el transcurrido entre el registro del incidente y el inicio de la atención de este por parte de un asesor de soporte y servicio Prioridad Crítica: Situación que se presenta y genera pérdida total del servicio en el ambiente de producción por indisponibilidad de todas las componentes críticas del mismo. La afectación genera un impacto catastrófico para el negocio. Prioridad Alta: Situación que se presenta y genera impacto mayor para el negocio sobre el servicio por indisponibilidad de algunas componentes críticas del mismo. Prioridad Media: Situación que se presenta y genera un impacto moderado para el negocio por degradación de algunas componentes del servicio. Prioridad Baja: Situación que se presenta pero que no genera afectación del servicio. Se trata de un evento que no impide en forma alguna la operación y el impacto para el negocio es menor.	
13.16	El contratista deberá entregar de forma trimestral un informe de la gestión de vulnerabilidades en el cual se refleje: - Las recomendaciones de mejores prácticas de manejo y atención de las vulnerabilidades críticas identificadas por la solución. - Estado general de los activos y FQDN monitoreados. - Avance en la resolución de hallazgos. - Informe de las auditorías realizadas. - Puntos de atención.	
13.17	Para la plataforma de gestión de vulnerabilidades, el contratista debe tener el servicio de gestion y remediacion segun lo reportado en la herramienta , de modo que sirva de apoyo al area de DIGIT, para resolver todos los casos a remediar segun los informes y dashboards que muestre la respectiva herramienta. El contratista debe poner a disposicion el recurso humano para generar planes de accion sobre la informacion reportada en la herramienta, y realizar el apoyo, soporte y acompañamiento durante la remediación de todas las vulnerabilidades encontradas en la prestación del servicio y la ejecución del contrato.	
14	Capacitación	
14.1	El oferente deberá ofrecer cinco (5) capacitaciones para cinco (5) ingenieros cada una, designados por la DIAN, con sus respectivos vouchers de certificación, dictadas en un centro de capacitación certificado por el fabricante de las soluciones, con una intensidad mínima de cuarenta (40) horas, en temas de SIEM, SOAR, y las demás soluciones, tecnologías y servicios adquiridos.	
14.2	Se debe ofrecer entrenamiento gratuito en línea como parte de la oferta para los integrantes del área de tecnología y la Oficina de Seguridad (OSI) de la DIAN para mínimo cincuenta (50) integrantes, por parte del fabricante de las soluciones y plataformas entregadas, durante la vigencia del contrato de soporte y garantía.	
15	Transferencia de Conocimiento	
15.1	Debe ser mínima de cuarenta (40) horas para veinte (20) personas, cuyo contenido debe contemplar uso y administración, además de conocer la instalación, configuración, monitoreo, administración y resolución de problemas de todas la plataformas, soluciones, servicios y dispositivos entregados, entre otros	
15.2	A cada asistente, el oferente debe entregar un certificado de asistencia, especificando su duración en horas, las fechas en las que fue realizado y debe ser firmado por el instructor.	

16	Documentación	<p>Manuales, procedimientos, instructivos y protocolos de todas las plataformas, soluciones, servicios y dispositivos implementados, entre otros.</p> <ul style="list-style-type: none"> - Documentación as built, que registre el estado de configuración e implementación al momento de la recepción formal de las soluciones entregadas (Informe definitivo de la Implementación) - Diagramas, planos y modelos de la Arquitectura de las plataformas y dispositivos implementados. - Documentos de garantía - Manuales de administración. - Manuales de operación. - Manuales de usuario. - Documentación de licenciamiento. - Catálogos de cada uno de los componentes de las plataformas y dispositivos implementados.
17	Equipo Mínimo de Trabajo	
17.1	<p>Un (01) Gerente de Proyecto</p>	<p>Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Tarjeta Profesional con expedición mínimo de cinco (5) años</p> <p>Posgrado en la modalidad de maestría en Gerencia de Proyectos y Certificación PMP.</p> <p>Certificación Itil Foundation v3 o superior</p> <p>Experiencia general de cinco (5) años en gerencia de proyectos de TI, de los cuales mínimo tres (3) años de experiencia específica gerenciando y/o coordinando proyectos de seguridad informática.</p> <p>La experiencia se cuenta a partir de la expedición de la tarjeta profesional.</p>
17.2	<p>Un (01) Gerente de Servicio SOC:</p>	<p>Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 5 años a partir de la emisión de la Tarjeta Profesional.</p> <ul style="list-style-type: none"> - Cédula de Ciudadanía - Tarjeta Profesional - Postgrado en Seguridad de la Información. - Certificación en SCRUM Foundations o superior - Certificación AUDITOR INTERNO <p>- Certificación vigente como arquitecto de seguridad de redes o analista de seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR o Protección de Marca) emitida por el fabricante.</p> <p>Certificaciones de experiencia mínima 5 años en implementación y/o soporte y/o administración de soluciones de seguridad.</p> <p>La experiencia se cuenta a partir de la expedición de la tarjeta profesional.</p>
17.3	<p>Un (01) Analista SOC Nivel III</p>	<p>Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 5 años a partir de la emisión de la Tarjeta Profesional:</p> <ul style="list-style-type: none"> - Cédula de Ciudadanía - Tarjeta Profesional - Postgrado o especialista en seguridad informática. - Certificación vigente como profesional, analista y/o arquitecto de seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR o Protección de Marca) emitida por el fabricante. - Certificación en gestión o administración de plataformas de seguridad informática. <p>Certificaciones de experiencia mínima de 5 años en implementación y/o soporte y/o administración de soluciones de seguridad.</p> <p>La experiencia se cuenta a partir de la expedición de la tarjeta profesional.</p>
17.4	<p>Un (01) Analista SOC Nivel II</p>	<p>Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 3 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986:</p> <ul style="list-style-type: none"> - Cédula de Ciudadanía - Tarjeta Profesional - Certificación vigente como profesional, analista, especialista y arquitecto de seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR o Protección de Marca) emitida por el fabricante. - Certificación en Plataformas Gestión de la Superficie de Ataque.

	- Certificaciones de experiencia mínima de tres (3) años en implementación y/o soporte y/o administración de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.	
17.5	<p>Tres (03) Analistas SOC Nivel I</p> <p>Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 3 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986:</p> <ul style="list-style-type: none"> -Cédula de Ciudadanía -Tarjeta Profesional -Certificación vigente como profesional, analista, especialista y arquitecto de seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR o Protección de Marca) emitida por el fabricante. - Certificación en Plataformas Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional. <p>NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365.</p>	
17.6	Cada uno de los anteriores perfiles deberá presentarse por separado donde ninguno podrá repetir rol o perfil o cargo, para lo cual se deberá aportar la hoja de vida actualizada a fecha del proceso, y las respectivas evidencias para el cumplimiento de cada uno de los requerimientos solicitados.	
17.7	Todo el personal del SOC requerido para la implementación, operación, gestión, monitoreo, soporte, garantía, entre otros, deberá ser propio del canal o contratista evitando figuras de tercerización, sin embargo se aclara que el contratista se podrá apoyar con recursos (personal) directamente del fabricante para la etapa de implementación.	
17.8	Dentro de este personal, el contratista debe contar con un Ingeniero en SITIO (en horario laboral de 8x5), en la sede principal de la DIAN Bogotá, para realizar el acompañamiento y asesoramiento frente al tema de las remediaciones a las posibles vulnerabilidades encontradas en el monitoreo y las demás halladas en las actividades correspondientes a las capacidades solicitadas por la Entidad en este anexo técnico.	
18	Certificaciones	
18.1	Se deben presentar las siguientes certificaciones expedidas y firmadas por el fabricante de la solución, plataformas, servicios y dispositivos entregados, entre otros:	
18.2	Una certificación emitida directamente de los fabricantes de las soluciones ofertadas donde se evidencie que los equipos suministrados no se encuentran en fin de venta y contaran con soporte por mínimo 5 años, estas cartas deben ser dirigidas a la Entidad.	
	Certificación de fabricante indicando que esta en alguno de los tres niveles de membresía mas altos ante el fabricante de las soluciones y plataformas ofertadas, exceptuando las capacidades de NDR y protección de bases de datos.	
	Certificación expedida por el fabricante, donde se indique el compromiso del suministro de piezas y partes de repuestos por un periodo mínimo de cinco (5) años posteriores a la declaración de obsolescencia de los equipos ofrecidos la cual debe quedar consignada en la respectiva garantía entregada a la entidad.	
	Certificación expedida por el fabricante en donde avalen la garantía y soporte técnico de tres (3) años ofrecida por el proponente para la plataformas, soluciones y dispositivos ofertados.	
18.3	Se debe allegar como máximo cinco (5) certificaciones de experiencia en la que conste que la empresa está prestando (en ejecución) o prestó los servicios de centro de operaciones de seguridad (SOC) o suministro de plataformas o dispositivos o tecnologías de información y comunicaciones como (Seguridad Informática, Firewalls, SANDBOX, SIEM), y/o implementó soluciones de (Seguridad informática), y/o en servicios de soporte técnico o tecnológico de soluciones o dispositivos de seguridad informática.	
	NOTA: Este requerimiento puede cambiar y solo se tendrá en cuenta en el proceso contractual y adjudicación del contrato.	
19	Gestión de Incidentes	
19.1	Análisis y detección	
19.1.1	Realizar la evaluación de los eventos y detectar aquellos que sean potencialmente un incidente evaluando su impacto después de la detección en el menor tiempo posible	
19.1.2	Gestionar los tiempos de notificación del incidente después de la evaluación del impacto, según propuesta realizada por el PROPONENTE y deberá alinearse con lo definido en el SGSPI en relación con los tiempos de atención del incidente	
19.1.3	Generar propuesta de solución del incidente después de la evaluación del impacto.	
19.1.4	En caso de ser necesario, realizar el escalamiento del o los incidentes de seguridad de la información a un nivel de servicio de soporte especializado, nivel 3 o 4 que pueda realizar el análisis y solución del incidente.	
19.1.5	Realizar el análisis Forense para incidentes críticos, y determinar el origen y el vector de inicio del incidente.	
19.1.6	Detectar si en los sistemas de información existen eventos anómalos que deban ser reportados, bloqueados y/o escalados a incidentes, e integrarlos a casos de uso si necesario.	
19.1.7	Gestionar los eventos e identificar los incidentes de seguridad de la información.	
19.1.8	El servicio deberá contar con los mecanismos necesarios para realizar el reporte de eventos sospechosos que puedan generar un incidente de seguridad.	
19.1.9	Detectar de manera temprana los incidentes de seguridad de la información, basado en la inteligencia y cacería de amenazas que permita a la DIAN la contención de posibles incidentes.	
19.2	Escalamiento y seguimiento	
19.2.1	Gestionar y canalizar las alertas a los diferentes grupos de interés y partes interesadas.	
19.2.2	Definir los casos de uso (eventos externos), sobre posibles ataques de ciberseguridad que se lleguen a presentar.	
19.2.3	Definir los casos de uso (eventos internos), generados por los usuarios al interior de la DIAN.	

19.2.4	Escalamiento a terceros internos y/o externos de ser necesario para la toma de acciones.																	
19.2.5	Registrar, realizar seguimiento y cerrar los incidentes de seguridad de la información en la plataforma SOAR.																	
19.2.6	Los incidentes de seguridad de la información se deberán trabajar de la mano con el personal de la DIAN, en cada fase del incidente hasta su resolución.																	
19.2.7	<p>El contratista debe Gestionar y canalizar las alertas a los diferentes grupos de interés y partes interesadas. Definir los casos de uso (eventos externos), sobre posibles ataques de ciberseguridad que se lleguen a presentar, estos casos de uso se deberán realizar entre el CONSULTOR y la DIAN. Definir los casos de uso (eventos internos), generados por los usuarios al interior de la DIAN.</p> <p>En el caso de un Incidente de seguridad se debe seguir el Modelo de Operación requerido para el SOC DIAN, y por lo tanto el procedimiento de escalamiento de incidentes sea de la siguiente manera:</p> <p>Nivel del Incidente: Es una herramienta estratégica la respuesta a incidentes dada la criticidad de la información y sus activos, el SOC debe estar en capacidad de dar respuesta efectiva y oportuna a los incidentes de seguridad, así mismo detectar, evaluar, gestionar vulnerabilidades y disparar la remediación al área de TI encargada, en todos los activos de información y en los sistemas de información de la DIAN.</p> <p>Severidad del incidente: Alto Impacto: Es un incidente de Seguridad que afecta a activos de información que tengan asociados los impactos catastrófico y mayor, que además de esto se relacionan directamente a los objetivos misionales y el Core de los sistemas de la DIAN, así como también son la reputación, el buen nombre y que involucren aspectos legales. Tipo de respuesta: Inmediata.</p> <p>Medio Impacto: Es un incidente de seguridad que afecta a activos de información que tengan asociados los impactos moderados que influyen directamente a los objetivos de un proceso. Tipo de respuesta: Media.</p> <p>Bajo Impacto: Es un incidente de seguridad afecta a activos de información que tengan asociados los impactos menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto. Tipo de respuesta: Baja.</p> <p>Tiempos de Atención / Solución para Incidentes</p> <table border="1"> <thead> <tr> <th>Prioridad</th> <th>Nivel máximo de atención</th> <th>Tiempo máximo para solución temporal. Se cuenta desde el vencimiento del Nivel máximo de atención.</th> <th>Tiempo máximo para solución definitiva. Se cuenta desde el vencimiento del Nivel máximo de atención</th> </tr> </thead> <tbody> <tr> <td>Alta</td> <td>1a hora</td> <td>1 hora</td> <td>2 horas</td> </tr> <tr> <td>Medio</td> <td>1/2 hora</td> <td>2 horas</td> <td>4 horas</td> </tr> <tr> <td>Baja</td> <td>1 hora</td> <td>4 horas</td> <td>8 horas</td> </tr> </tbody> </table>	Prioridad	Nivel máximo de atención	Tiempo máximo para solución temporal. Se cuenta desde el vencimiento del Nivel máximo de atención.	Tiempo máximo para solución definitiva. Se cuenta desde el vencimiento del Nivel máximo de atención	Alta	1a hora	1 hora	2 horas	Medio	1/2 hora	2 horas	4 horas	Baja	1 hora	4 horas	8 horas	
Prioridad	Nivel máximo de atención	Tiempo máximo para solución temporal. Se cuenta desde el vencimiento del Nivel máximo de atención.	Tiempo máximo para solución definitiva. Se cuenta desde el vencimiento del Nivel máximo de atención															
Alta	1a hora	1 hora	2 horas															
Medio	1/2 hora	2 horas	4 horas															
Baja	1 hora	4 horas	8 horas															
19.3	Lecciones aprendidas																	
19.3.1	Generar el reporte del incidente, acciones realizadas, sistemas afectados, nivel de afectación, controles afectados o inexistentes, hallazgos, recomendaciones, acciones a realizar, valoración total del incidente y/o reporte a terceras partes si es necesario.																	
19.3.2	El contratista deba entregar una base de conocimiento sobre las lecciones aprendidas en los diferentes procesos que se tenga en SOC, pensando en la transferencia de conocimiento al equipo interno de la DIAN y enmarcado en las mejores practicas del mejoramiento continuo, estas lecciones aprendidas deba ser revisadas al menos una vez al mes en el transcurso del contrato, Generando los respectivos reportes y artefactos para la el entendimiento de la DIAN.																	
19.4	Relacionamiento con terceros nacionales e internacionales (CSIRT – FIRST)																	
19.4.1	Efectuar reporte y relacionamiento con terceros en caso de realizar escalamiento de incidentes.																	
19.4.2	Tener una vinculación directa y activa con foros internacionales o nacionales de cert/csirt (grupos de respuesta a incidentes de seguridad informática) como referencia se puede tomar FIRST (Forum Incident Response and Security Teams) o equivalente.																	
19.4.3	Realizar con los entes de control en Colombia tales como el CSIRT, COLCERT, Centro Cibernético Policial, Fiscalía, entre otros, el escalamiento, retroalimentación e implementación de las recomendaciones dadas por un tercero. Si no es posible realizar la implementación deberá realizar el escalamiento a las áreas responsables, de igual forma será el responsable de tomar y aportar las evidencias necesarias.																	
19.4.4	Realizar monitoreo, reporte y/o relacionamiento con terceros nacionales e internacionales.																	
19.4.5	Reportar incidentes de seguridad a los entes externos: En caso de presentarse un incidente de seguridad de la información es el único autorizado para reportarlos de ser necesario. Se pueden reportar incidentes de seguridad de la información a través de los siguientes canales: - ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897. - CSIRT Gobierno reportar al correo csirtgob@mintic.gov.co - Centro cibernético Policial reportar en la siguiente ruta: https://caivirtual.policia.gov.co/																	
20	Devolución del servicio (licenciamiento posterior a la terminación del contrato)																	
20.1	Realizar y entregar el plan de trabajo detallado para la devolución del servicio, por lo menos cinco meses antes de la finalización del servicio.																	

20.2	Entregar las licencias a perpetuidad de las herramientas o recursos tecnologicos para los casos donde aplique, utilizados en la operacion del SOC , a nombre de la DIAN implementadas y configuradas durante el proyecto con las capacidades en las que se encuentren en operaci3n en el momento de la devoluci3n del servicio con soporte actualizado por m3nimo un a3o.	
20.3	Entregar la estrategia a seguir para la devoluci3n del servicio, este proceso se debe iniciar con un tiempo m3nimo de cuatro meses antes de la fecha de finalizaci3n y deber3 incluir como m3nimo: las copias de las configuraciones actuales, dise3os f3sicos y l3gicos de la prestaci3n de los servicios, procedimientos, instructivos, manuales y de m3s documentos de estrategia, copia en formato standard de la configuraci3n de los logs de las herramientas utilizadas durante el servicio prestado, evidencias o registros de las licencias a nombre de la DIAN y dem3s informaci3n administrativa asociada al servicio prestado.	
20.4	Realizar los procesos administrativos de cierre de contrato que haya lugar.	

PROPONENTE:	
NIT:	
REPRESENTANTE LEGAL:	
IDENTIFICACI3N:	
FIRMA DEL REPRESENTANTE LEGAL:	