PROPUESTA COMERCIAL

Versión: 1

DIRECCIÓN GENERAL MARÍTIMA

DIRIGIDA A:



Bogotá, 25 de Julio del 2025

Señores

DIRECCIÓN GENERAL MARÍTIMA

Referencia: Capacidades Cibernéticas– Versión 2

Cordial saludo,

Por medio de la presente hacemos entrega de nuestra oferta comercial, la cual tiene como objeto detallar la solución técnica y de servicios especializados para el cumplimiento de su requerimiento.

Quedamos a su entera disposición para revisar cualquier detalle que consideren relevante en aras del pleno entendimiento de esta propuesta y de nuestro interés por continuar siendo sus mejores aliados en los procesos que involucran la seguridad de su información.

Atentamente,

Alejandra Martínez.

Gerente de Cuenta
alejandra.martinez@wexler.com.co
Cel. 320 3031280

Tabla de Contenido

1. PROPIEDAD Y CONFIDENCIALIDAD 5
2. RESUMEN EJECUTIVO 6
3. REQUERIMIENTO DEL CLIENTE 7
4. PROPUESTA TÉCNICA 8
4.1. DESCRIPCIÓN DE LA SOLUCIÓN OFERTADA 8
4.1.1. SOLUCIÓN DE PROTECCION DE MARCA 8
4.1.2. ENTREGABLES 10
4.1.3. SERVICIO PARA IMPLEMENTAR EL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 10
4.1.4. SOLUCIÓN PARA LA PROTECION DE DATOS DLP 12
4.1.5. SOLUCIÓN PARA EL CONTROL DE ACCESO PAM 13
4.2. SERVICIOS PROFESIONALES 14
4.2.1. SERVICIOS DE PLANEACIÓN, DISEÑO Y DIAGNÓSTICO: 14
4.2.2. SERVICIO DE IMPLEMENTACIÓN: 15
4.2.2.1. DESPLIEGUE DE SERVICIOS DE SEGURIDAD 15
4.2.3. SERVICIO DE CONFIGURACIÓN Y PUESTA A PUNTO: 15
4.2.3.1. ENTREGA EN OPERACIÓN: 15
4.2.3.2. ENTREGABLES DEL PROYECTO: 16
4.2.4. TIEMPO DE IMPLEMENTACIÓN, CONFIGURACIÓN Y ENTREGA: 16
4.2.5. SERVICIO DE TRANSFERENCIA DE CONOCIMIENTO: 16
4.2.6. SERVICIO DE GESTIÓN DEL PROYECTO: 17
4.2.6.1. LÍDER DE PROYECTO DE PARTE DE WEXLER SAS: 17
4.2.6.2. LÍDER DE PROYECTO DE PARTE DEL CLIENTE: 18
4.2.7. SERVICIO DE SOPORTE TÉCNICO: 18
4.2.8. SERVICIO DE ADMINISTRACIÓN Y GESTIÓN: 19
4.3. PREMISAS Y/O SUPUESTOS 20
5. PROPUESTA COMERCIAL 22
4.4. OFERTA ECONÓMICA 22
4.5. CONDICIONES COMERCIALES 22
4.5.1. VIGENCIA DE LA OFERTA: 22
4.5.2. INTEGRIDAD DE LA OFERTA: 22
4.5.3. IMPUESTOS: 22
4.5.4. MONEDA: 22

4.5.5. TIEMPOS DE ENTREGA: 23
4.5.6. MODO DE FACTURACIÓN: 23
4.5.7. FORMA DE PAGO: 23

1. PROPIEDAD Y CONFIDENCIALIDAD

DIRECCIÓN GENERAL MARÍTIMA, se obliga a mantener la confidencialidad absoluta con respecto a la información contenida en la presente propuesta. Esta "Información", podrá ser utilizada exclusivamente para el desarrollo de la(s) actividad(es) descritas por **WEXLER SAS.**

Igualmente se compromete a tomar todas las medidas necesarias para que la información no llegue a manos de terceros en ninguna circunstancia y se obliga a no utilizarla para ningún objeto diferente al de adelantar las tareas que se deriven directamente del cumplimiento de las actividades que se desprendan del contenido de la propuesta.

Adicionalmente, DIRECCIÓN GENERAL MARÍTIMA se compromete a devolver toda información tan pronto como termine la labor de evaluación de la presente propuesta si **WEXLER SAS** así lo solicita, junto con la confirmación escrita de que la misma no ha sido copiada ni reproducida y que DIRECCIÓN GENERAL MARÍTIMA no tiene en su poder o ha entregado a terceros copia alguna de la misma.

Las obligaciones señaladas en el presente acuerdo continuarán vigentes aún después de su vencimiento o terminación.

2. RESUMEN EJECUTIVO

Somos una compañía 100% colombiana, integradora de soluciones y servicios tecnológicos la cual cuenta con más de 10 años de experiencia en el mercado; contamos con un grupo de profesionales certificados en plataformas de seguridad informática, infraestructura tecnológica y servicios consultivos especializados.

Por requerimiento de **DIRECCIÓN GENERAL MARÍTIMA,** (en adelante, "el cliente"), nos permitimos presentar en este documento una propuesta comercial y técnica donde se plasmarán los objetivos y alcances para prestar el CAPACIDADES CIBERNÉTICAS.

El presente documento de oferta considera el suministro de CAPACIDADES CIBERNÉTICAS del fabricante VARIOS de acuerdo con la solicitud del cliente. Adicionalmente, se incluyen los servicios de instalación, configuración, despliegue, puesta a punto y servicio técnico de toda la solución, dando cumplimiento a los objetivos descritos, en los plazos y condiciones detalladas en el transcurso del presente documento de oferta.

La Presente Propuesta y sus anexos forman un acuerdo total entre las partes (**WEXLER SAS** y DIRECCIÓN GENERAL MARÍTIMA, y reemplazaran cualquier comunicación y/u oferta anterior, sea de forma oral o escrita.

3. REQUERIMIENTO DEL CLIENTE

La Dirección General Marítima (DIMAR) requiere una solución integral para fortalecer su postura en ciberseguridad, protección de marca y control de riesgos digitales, estructurada en cuatro componentes principales:

1. **Protección de Marca (x 1 año)**

Monitoreo de sitios falsos, redes sociales (incluye TikTok) y apps no autorizadas.

Inventario automatizado de activos (dominios, IPs, DNS, SSL).

Inteligencia sobre amenazas (APT), dark web y cadena de suministro (mín. 50 aliados).

Cobertura mínima: 15 ejecutivos, 7 perfiles sociales, 2 apps, 25 palabras clave.

Takedowns, tablero de incidentes, soporte 24x7, y cumplimiento con ISO 27001, FIRST, NIST SP 800-53.

2. PESI – Plan Estratégico de Seguridad de la Información

Diagnóstico técnico y normativo (AS-IS).

Evaluación de riesgos, definición del estado objetivo (TO-BE) y hoja de ruta.

Portafolio de proyectos, indicadores, talleres, capacitaciones y validación institucional.

Entregables editables con enfoque en mejora continua.

3. Prevención de Pérdida de Datos (DLP) – x 1 año

Clasificación automática de datos sensibles.

Control de fuga por correo, USB, nube, etc.

Políticas contextuales, reportes técnicos y cumplimiento con MSPI y MAE.

Integración con AD, SIEM, antivirus y herramientas existentes.

4. Gestión de Accesos Privilegiados (PAM) – x 1 año

Gestión segura de credenciales, grabación de sesiones y accesos just-in-time.

Auditoría, analítica de comportamiento, integración nativa y soporte 8x5 / 24x7.

Cumple con ISO 27001, FIRST, NIST y otros estándares clave.

4. PROPUESTA TÉCNICA

4.1. DESCRIPCIÓN DE LA SOLUCIÓN OFERTADA

En virtud de lo solicitado por el cliente se describe a continuación las soluciones propuestas:

4.1.1. SOLUCIÓN DE PROTECCION DE MARCA

El presente documento tiene como propósito presentar a DIMAR una propuesta técnica detallada de una solución integral de protección de marca, orientada a dar cumplimiento completo a los requerimientos establecidos en el pliego de condiciones. Esta solución está diseñada para salvaguardar la identidad digital institucional, mitigar riesgos reputacionales y operativos, y fortalecer la postura de seguridad digital de la Entidad.

Protección contra Fraude y Suplantación de Identidad
La solución ofertada permite detectar sitios web fraudulentos, aplicaciones móviles no autorizadas y perfiles falsos en redes sociales como Facebook, X (Twitter), Instagram, LinkedIn, TikTok, YouTube, entre otras. Incorpora mecanismos de respuesta inmediata mediante procesos automáticos de "takedown" y ofrece acompañamiento técnico, legal y de comunicación para la remoción de contenido suplantador.

Caza de Amenazas y Cadena de Suministro
Se provee un módulo de inteligencia que identifica grupos APT, sus tácticas y técnicas, así como amenazas dirigidas contra DIMAR o su cadena de suministro. Esta funcionalidad permite monitorear al menos 50 proveedores o aliados estratégicos, generando alertas oportunas desde fuentes de inteligencia en la web oscura.

Descubrimiento y Seguimiento de Activos
La solución realiza descubrimiento automatizado y continuo de activos digitales expuestos (dominios, subdominios, direcciones IP, certificados SSL y DNS). Además, clasifica, evalúa el riesgo y permite gestionar manualmente dichos activos desde una interfaz intuitiva. Incluye alertamiento sobre modificaciones no autorizadas en registros DNS y whois.

Inteligencia de Vulnerabilidades
Incluye monitoreo automático de certificados SSL, detección de vulnerabilidades en aplicaciones expuestas, verificación de protocolos SPF, DKIM y DMARC, análisis de bibliotecas externas, supervisión de servicios vulnerables, y escaneo bajo demanda para validar medidas de mitigación.

Monitoreo Web (superficial, profunda y oscura)
La solución analiza información sensible expuesta en la deep web, dark web y web superficial, incluyendo credenciales comprometidas y documentos institucionales.

Supervisa plataformas como GitHub y Bitbucket, e incluye capacidades de análisis de malware mediante sandboxing y herramientas tipo VirusTotal.

- **WEXLER SAS** prestará el servicio desde su centro de monitoreo ubicado en la ciudad de Bogotá, donde se garantizará las condiciones de seguridad mínimas en aspectos de acceso al espacio físico y acceso a las herramientas de software de monitoreo.
- **WEXLER SAS** prestará el servicio de correlación avanzada de eventos de seguridad de la información y ciberseguridad para proteger los activos TI del cliente que serán objeto de monitoreo.
- **WEXLER SAS** enfrentará y ayudará a prevenir las diferentes situaciones de riesgos de seguridad de la información y ciberseguridad, al contar con un monitoreo proactivo, que garantice, por parte del cliente, la debida gestión y optimización de las configuraciones de los activos TI que serán objeto de monitoreo.
- **WEXLER SAS** apoyará en la definición de estrategias de seguridad, que permitan fortalecer las políticas y controles de seguridad de la información del cliente.
- **WEXLER SAS**, cuando un evento de seguridad ocurre o está en suceso, identificará y estará en la capacidad de relacionar de forma directa o indirecta con otros eventos de seguridad asociados, determinando el patrón de ataque.
- **WEXLER SAS** alertará sobre eventos y/o comportamientos anormales que se presenten bajo la operación de los activos TI del cliente que serán objeto de monitoreo.
- **WEXLER SAS** informará al equipo de seguridad de la información del cliente, de manera inmediata, sobre cualquier evento o incidente real que se presenten en la infraestructura tecnológica objeto de monitoreo.
- **WEXLER SAS** permitirá la integración del envío de alarmas automáticas vía correo electrónico y/o vía telefónica.
- **WEXLER SAS** incluirá la personalización de hasta cinco (5) reportes que el cliente requiera durante la prestación del servicio.
- **WEXLER SAS** 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 respuesta oportuna a los riesgos y amenazas. Por lo anterior, el personal del servicio de **WEXLER SAS** deberá realizar el escalamiento y las comunicaciones por medio de correo electrónico y/o telefónico con el personal del cliente a fin de comunicar las incidencias presentadas y las acciones a seguir para solucionarlas. Adicionalmente realizará el seguimiento a los eventos hasta que estos sean cerrados adecuada y oportunamente.
- **WEXLER SAS** definirá la matriz de escalamiento de común acuerdo con los responsables de seguridad en el cliente, clarificando el nivel de escalamiento según el tipo y nivel de incidente.
- **WEXLER SAS** generará reportes de eventos y de análisis de tendencias, con el fin de recomendar las acciones preventivas para que sean ejecutadas por el cliente, 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 de acuerdo con las necesidades del cliente.

- **WEXLER SAS** entregará un informe preliminar de un incidente sucedido. Este debe ser remitido al cliente 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.
- **WEXLER SAS** permitirá visualizar la actividad de monitoreo a través de tableros de control que permitan ver métricas en línea de acuerdo a las necesidades del cliente, por ejemplo:
  - 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
- **WEXLER SAS** entregará las evidencias que sean recopiladas a través del monitoreo, las cuales se entiende son propiedad del cliente y podrán ser solicitadas en cualquier momento para la atención de requerimientos legales.
- **WEXLER SAS** certificará su operación bajo la norma ISO 27001:2013, lo que garantiza la aplicación de las mejores prácticas en cuanto a la seguridad de la información.

4.1.2. ENTREGABLES

Los servicios de elaboración de informes y reportes, consecuencia de las actividades de Monitoreo SOC, objeto de la actual propuesta, están considerados en el presente documento de oferta.

WEXLER SAS presentará mensualmente o cada vez que sea requerido por el cliente, los informes de servicio que contengan la siguiente información:

- 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.
- Incidentes de seguridad presentados.
- Estadísticas de la información procesada.
- Hallazgos realizados sobre la plataforma tecnológica.
- Análisis y recomendaciones sobre los resultados.

4.1.3. SERVICIO PARA IMPLEMENTAR EL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

Esta propuesta tiene como objetivo presentar el enfoque metodológico y operativo para la elaboración del Plan Estratégico de Seguridad de la Información (PESI) de la DIMAR, conforme a lo estipulado en los requerimientos del pliego. El objetivo principal es estructurar un modelo estratégico y sostenible que fortalezca la postura de seguridad de la entidad, alineado con marcos normativos nacionales e internacionales.

Diagnóstico Normativo y Técnico

1.1 Revisión del Marco Normativo y Estándares Internacionales
Se realiza un análisis comparativo del estado actual de cumplimiento frente a marcos como MSPI (Resolución 500/2021), MAE (Dominio Seguridad), Ley 1581/2012, Decreto 612/2018, ISO/IEC 27001, ISO/IEC 27005, NIST CSF, entre otros.

1.2 Análisis del Estado Actual (AS-IS)
Se levantará información institucional a través de entrevistas, encuestas, revisión documental y talleres, para identificar procesos, actores, herramientas y capacidades actuales en materia de seguridad.

1.3 Evaluación de Riesgos y Brechas
Se aplicará una metodología reconocida (ISO 27005, FAIR o similar) para identificar vulnerabilidades, amenazas y brechas, y estimar su impacto sobre los procesos misionales de la Entidad.

Planeación Estratégica del PESI

2.1 Definición del Estado Objetivo (TO-BE)
Se formulará el modelo deseado de seguridad de la información, alineado con el PED 2042, el PETI institucional y las prioridades del sector defensa.

2.2 Formulación de Objetivos Estratégicos y Tácticos
Se definirán metas medibles, líneas de acción, responsables y motivadores clave para alcanzar el estado objetivo.

2.3 Diseño del Modelo de Gobernanza
Se estructurará un esquema de roles, comités, funciones y mecanismos de seguimiento para gestionar la seguridad de forma efectiva y transversal.

2.4 Portafolio de Proyectos y Hoja de Ruta
Se identificarán los proyectos clave del PESI con su cronograma, responsables, costos estimados y análisis de sostenibilidad a 3 o 5 años.

Entregables y Transferencia de Conocimiento

3.1 Documento PESI Completo
Se entregará el documento estructurado con narrativa estratégica, análisis de brechas, riesgos, portafolio de proyectos, plan de implementación, indicadores (KPI/KRI) y anexos técnicos.

3.2 Artefactos Estratégicos y Matrices
Incluye matriz de riesgos, matriz de gobernanza, cronograma, catálogo de motivadores, objetivos estratégicos y plan de acción detallado.

3.3 Talleres Participativos y Validación
Se realizarán al menos 2 talleres con los líderes institucionales para validar el PESI y afinar su implementación con el equipo técnico de DIMAR.

3.4 Transferencia de Conocimiento
Incluye sesiones de capacitación funcional y estratégica al equipo de seguridad de la información de la entidad.

3.5 Acompañamiento en Aprobación Institucional
El equipo consultor acompañará las reuniones de presentación y ajuste, brindando soporte para la adopción interna del documento.

3.6 Garantía de Calidad
Todos los entregables se presentarán en formatos editables (Word, Excel, Visio) y se garantizará un enfoque de mejora continua y seguimiento a la ejecución.

4.1.4. SOLUCIÓN PARA LA PROTECION DE DATOS DLP

El presente documento tiene como objetivo presentar a DIMAR una propuesta técnica detallada de una solución gestionada de Prevención de Pérdida de Datos (DLP). Esta propuesta responde a los requerimientos del pliego con un enfoque integral en la protección de información sensible, cumplimiento normativo, y visibilidad completa sobre riesgos de fuga de datos en tránsito, en reposo y en uso.

Protección de Información Sensible
La solución propuesta permite la identificación y clasificación automatizada de datos sensibles como información confidencial, reservada o personal, de acuerdo con las políticas definidas por DIMAR. Utiliza motores de detección avanzados para inspeccionar datos en múltiples ubicaciones (correo, USB, impresión, almacenamiento en nube, navegación web, etc.), aplicando políticas contextuales que consideran el tipo de usuario, el dispositivo, la ubicación y el riesgo asociado.

Control de Canales de Fuga de Datos
El sistema detecta, alerta y puede bloquear actividades que impliquen la exfiltración de datos a través de medios como correo electrónico, dispositivos de almacenamiento, herramientas de mensajería o servicios en la nube. Esta visibilidad y control permiten gestionar las acciones en tiempo real y aplicar medidas preventivas antes de que ocurra una fuga.

Aplicación de Políticas Contextuales
Las políticas pueden adaptarse de forma dinámica según el contexto del usuario, dispositivo, aplicación utilizada, ubicación geográfica y clasificación del dato. Esto permite escenarios de control granular que se alinean con los procesos de la Entidad.

Gestión del Riesgo y Reportes
La solución ofrece monitoreo constante de incidentes relacionados con la seguridad de la información, prioriza alertas según su criticidad, y proporciona análisis forense básico. Se entregan reportes técnicos y ejecutivos mensuales, con métricas de incidentes, tendencias, acciones tomadas y recomendaciones específicas.

Cumplimiento Normativo
La solución está diseñada para apoyar a DIMAR en el cumplimiento de normativas como la Ley 1581, el Modelo de Seguridad y Privacidad de la Información (MSPI), los dominios MAE de ciberseguridad, e ISO 27001. Integra mecanismos de control y trazabilidad alineados con estos marcos regulatorios.

Administración y Operación del Servicio
El servicio incluye administración operativa gestionada por el proveedor, abarcando configuración inicial, gestión de políticas, manejo de incidentes, soporte a usuarios y mantenimiento del sistema durante todo el periodo de contratación.

Interfaz de Gestión y Auditoría
La plataforma incluye una consola de administración con dashboards personalizables, trazabilidad de eventos, auditoría, y acceso histórico de mínimo 6 meses para incidentes y configuraciones.

Integración e Infraestructura
La solución es compatible con Active Directory (AD), SIEMs como FortiAnalyzer o plataformas vía Syslog/API, antivirus EDR, herramientas NAC, sistemas de ticketing (ServiceNow, Remedy), CASB y entornos cloud. Esta integración facilita una gestión centralizada del riesgo.

4.1.5. SOLUCIÓN PARA EL CONTROL DE ACCESO PAM

El presente documento tiene como objetivo presentar a DIMAR una propuesta técnica detallada de una solución gestionada de Gestión de Accesos Privilegiados (PAM). Esta solución busca fortalecer el control de accesos, proteger credenciales críticas, mitigar riesgos asociados al uso indebido de privilegios y cumplir con las exigencias del pliego en materia de seguridad de la información.

Gestión Segura de Cuentas Privilegiadas
La solución propuesta permite almacenar, rotar, auditar y proteger credenciales privilegiadas utilizadas por administradores, servicios, APIs, bases de datos y otros componentes críticos del entorno institucional. Todas las credenciales se gestionan de forma segura mediante bóvedas cifradas y controles de acceso robustos.

Grabación y Auditoría de Sesiones
Cada sesión privilegiada puede ser grabada en su totalidad, firmada digitalmente y almacenada para su posterior análisis. Estas grabaciones permiten realizar auditoría

detallada de las actividades realizadas, facilitando la detección de acciones no autorizadas o desviaciones de políticas.

Accesos Just-in-Time y Zero Standing Privileges
La solución elimina el acceso permanente a recursos críticos, habilitando el acceso de forma temporal y controlada bajo aprobación previa. Esto minimiza la superficie de ataque y fortalece el principio de privilegio mínimo.

Analítica y Visibilidad
Incluye funciones de analítica del comportamiento del usuario (UBA), que identifican patrones anómalos en las sesiones administradas. Se generan alertas en tiempo real ante acciones atípicas o potencialmente maliciosas, permitiendo una respuesta proactiva.

Reportes Ejecutivos y Técnicos
Se entregan informes mensuales que documentan las sesiones registradas, riesgos detectados, métricas de cumplimiento, acciones tomadas y recomendaciones específicas. Estos reportes fortalecen la gobernanza y el control institucional sobre los accesos privilegiados.

Administración del Servicio
El proveedor asume la administración integral del servicio durante todo el contrato, incluyendo onboarding, definición de roles y políticas, rotación de credenciales, monitoreo de sesiones, análisis de riesgo y respuesta ante incidentes.

4.2. SERVICIOS PROFESIONALES

4.2.1. SERVICIOS DE PLANEACIÓN, DISEÑO Y DIAGNÓSTICO:

WEXLER SAS basado en la información otorgada por el cliente, realizará (en conjunto con el cliente) el levantamiento de información necesaria que describa una imagen detallada de la situación inicial, identificando riesgos, amenazas y requerimientos que presente la plataforma del cliente con el objetivo de lograr la consecución efectiva del proyecto.

Adicionalmente, **WEXLER SAS** y el cliente desarrollarán un plan de acción que defina los procesos y tiempos, así como personas responsables para cada una de las etapas del proyecto. En esta etapa también se definirán los entregables específicos que el cliente requiera y los criterios bajo los cuales se evaluarán y entregarán cada una de las etapas del proyecto.

Para dar cumplimiento al alcance general de la presente propuesta, durante esta fase se tiene previsto la ejecución de un conjunto de actividades, según se detalla a continuación:

- **WEXLER SAS** identificará los prerrequisitos técnicos para la implementación correcta de toda la(s) solución(es) ofertada(s). Será responsabilidad del cliente confirmar el cumplimiento de estos prerrequisitos antes de iniciar las actividades de implementación.
- **WEXLER SAS** confirmará la Arquitectura de toda la(s) solución(es) ofertada(s), de acuerdo con los requerimientos iniciales del cliente y los componentes de

hardware y software ofertados. Será responsabilidad del cliente confirmar esta Arquitectura para ser desplegada en las actividades de implementación.

- **WEXLER SAS** identificará los parámetros básicos de administración de toda la(s) solución(s) ofertada(s). Será responsabilidad del cliente confirmar la aprobación de los parámetros básicos de administración para ser desplegados en las actividades de implementación.
- **WEXLER SAS** informará las funcionalidades que se van a desplegar de toda la(s) solución(es) ofertada(s), de acuerdo con los requerimientos iniciales del cliente y los componentes de hardware y software ofertados. Será responsabilidad del cliente confirmar la aprobación de las funcionalidades para ser desplegadas en las actividades de implementación.
- **WEXLER SAS** identificará las actividades de integración con otras plataformas de toda la(s) solución(es) ofertada(s). Será responsabilidad del cliente confirmar la aprobación de las actividades de integración con otras plataformas para ser desarrolladas en las actividades de implementación.

Por último, **WEXLER SAS** elaborará un documento de entrega donde se listarán todos los prerrequisitos, condiciones y alcances técnicos identificados y establecidos en la fase de Planeación y Diagnóstico.

4.2.2. SERVICIO DE IMPLEMENTACIÓN:

4.2.2.1. Despliegue de Servicios de Seguridad

Los servicios de despliegue de Servicios de Seguridad correspondiente a las soluciones objeto de la actual propuesta están considerados en el presente documento de oferta.

WEXLER SAS aprovisionará y pondrá en producción los Servicios de Seguridad en la correspondiente a las soluciones objeto de la actual propuesta por el termino de 12 meses.

4.2.3. SERVICIO DE CONFIGURACIÓN Y PUESTA A PUNTO:

Los servicios de configuración y puesta a punto de la(s) solución(es) objeto de la actual propuesta están considerados en el presente documento de oferta.

WEXLER SAS realizará las labores de configuración de los equipos basado en las condiciones y alcances técnicos identificados y establecidos en la fase de Planeación y Diagnóstico.

WEXLER SAS habilitará los parámetros básicos de gestión y administración de los equipos basado en las condiciones y alcances técnicos identificados y establecidos en la fase de Planeación y Diagnóstico.

4.2.3.1. Entrega en Operación:

Los servicios de entrega en operación de la(s) solución(es) objeto de la actual propuesta están considerados en el presente documento de oferta.

WEXLER SAS ejecutará un listado de pruebas funcionales previamente definidas con el cliente, con el objetivo de garantizar el correcto funcionamiento de la solución basado en las condiciones y alcances técnicos identificados y establecidos en la fase de Planeación y Diagnóstico.

WEXLER SAS y el cliente evaluarán el resultado del proyecto para luego dar paso al cierre y entrega de la documentación final del mismo.

4.2.3.2. Entregables del Proyecto:

Los servicios de elaboración de documentación de la(s) solución(es) objeto de la actual propuesta están considerados en el presente documento de oferta.

WEXLER SAS elaborará y remitirá al cliente durante el transcurso del proyecto los siguientes entregables:

- Documento de **Cronograma de Actividades del Proyecto** entregado en el KickOff del Proyecto.
- Documento de **Definición de Alcance** donde se listarán todos los prerrequisitos, condiciones y alcances técnicos identificados y establecidos en la fase de Planeación y Diagnóstico.
- Documento de **Diseño de Alto Nivel** de la solución. (Si es solicitado por el cliente en la fase de Planeación y Diagnóstico).
- Documento con el **Plan de Implementación**. (Si es solicitado por el cliente en la fase de Planeación y Diagnóstico).
- Documento con el **Plan de Migración** (Si es solicitado por el cliente en la fase de Planeación y Diagnóstico).
- Documento de **Entrega de la Solución.**
- Demás **Documentos Técnicos de la Solución** requeridos por el cliente (Hojas de datos de fábrica, Guías de usuario de fábrica, Guías de administración de fábrica, etc.)

4.2.4. TIEMPO DE IMPLEMENTACIÓN, CONFIGURACIÓN Y ENTREGA:

El tiempo para las labores de planeación, diagnóstico, implementación, configuración, puesta a punto y entrega propuesto para todas la(s) solución(es) que son objeto en el presente documento de oferta será de 30 días calendario.

Este tiempo comienza a correr desde el momento que se hayan entregado todos los appliances físicos y virtuales, las licencias, suscripciones y demás soluciones que son objeto en el presente documento de oferta.

De igual manera, el tiempo de duración de las labores descritas en el presente documento dependerán también de la coordinación que se tenga entre **WEXLER SAS** y el cliente.

4.2.5. SERVICIO DE TRANSFERENCIA DE CONOCIMIENTO:

Los servicios de transferencia de conocimiento de la(s) solución(es) objeto de la actual

propuesta están considerados en el presente documento de oferta.

WEXLER SAS realizará una transferencia de conocimiento funcional de la solución desplegada con duración de 24 horas hábiles, donde se informará a máximo cinco (5) integrantes del personal técnico del cliente sobre la arquitectura y las funcionalidades de la solución desplegada; además, se dará instrucción sobre la administración básica de la plataforma y el despliegue de los casos de uso de las funcionalidades configuradas en la solución.

En ningún momento esta transferencia de conocimiento equivaldrá a un curso oficial del fabricante, debido a que estos cursos oficiales son impartidos únicamente por learning partners oficiales del fabricante.

4.2.6. SERVICIO DE GESTIÓN DEL PROYECTO:

Los servicios de gestión del proyecto de la(s) solución(es) objeto de la actual propuesta están considerados en el presente documento de oferta.

WEXLER SAS implementará las diferentes fases del proyecto bajo los estándares del **PMBOK**, 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.

Para garantizar el cumplimiento de los requerimientos solicitados, se establece dentro de este documento de oferta las diferentes responsabilidades de los Líderes de Proyecto, en ambas partes (**WEXLER SAS** y el cliente), como se describe a continuación.

4.2.6.1. Líder de proyecto de parte de WEXLER SAS:

WEXLER SAS dispondrá de un líder de proyecto asignado al cliente y trabajará en la ejecución de las actividades del proyecto. Las responsabilidades principales son:

- Planeación y diseño del proyecto.
- Convocar y ejecutar el KickOff del proyecto.
- Monitorear y controlar el avance del proyecto.
- Monitorear y administrar los grupos de trabajo de **WEXLER SAS.**
- Realizar el seguimiento del proyecto y participar en los comités para realizar de la toma de decisiones que ayuden al curso del proyecto.
- Verificar el cumplimiento de los lineamientos de diseño y arquitectura definidos.
- Detectar y documentar los riesgos del proyecto.
- Ejecutar el cierre formal del proyecto.

Dentro de la presente oferta se incluye el desarrollo por parte del PM asignado al proyecto de las siguientes reuniones:

- Una (1) reunión de KickOff del Proyecto de manera remota o en sitio (solo en Bogotá).
- Una (1) reunión quincenal de seguimiento durante el tiempo establecido para las fases de diagnóstico e implementación de manera remota o en sitio (solo en Bogotá).

- Una (1) reunión de Cierre del Proyecto de manera remota o en sitio (solo en Bogotá).

NOTA 1: NO se incluye la realización periódica de reuniones de seguimiento de proyecto no estipulados en el presente documento de oferta.

4.2.6.2. Líder de proyecto de parte del cliente:

El cliente deberá contar un líder de proyecto con las siguientes responsabilidades:

- Guiar la planeación del proyecto.
- Monitorear y controlar el proyecto.
- Realizar el seguimiento del proyecto y participar en los comités para realizar la toma de decisiones que ayuden al curso del proyecto.
- Manejar la relación interna (stakeholders gerenciales y equipo de proyecto).
- Garantizar los permisos de entrada y trabajo dentro de sus instalaciones.
- Garantizar los recursos y ventanas de instalación predefinidos.
- Facilitar la ejecución del proyecto y los contactos para la obtención de información.
- Definir políticas a aplicar sobre los equipos.
- Facilitar recursos tanto físicos como funcionales para la realización de tareas.
- Recibir las pruebas funcionales y los avances entregados.

4.2.7. SERVICIO DE SOPORTE TÉCNICO:

Los servicios de soporte técnico de la(s) solución(es) objeto de la actual propuesta están considerados en el presente documento de oferta.

WEXLER SAS prestará los servicios de soporte técnico en modalidad 24x7 para todas la(s) solución(es) objeto de la actual propuesta, por el término de 12 meses.

WEXLER SAS garantizará el siguiente alcance para los servicios de soporte técnico:

- Apertura de casos de cualquier criticidad a través de nuestra Mesa de Ayuda, vía telefónica **(+57 314 7881987)** o vía correo electrónico (soporte@wexler.com.co). Por ambos medios la atención de incidentes estará disponible en horario 24x7x365.
- Una vez abiertos los casos se realizará su registro, gestión y seguimiento a través de nuestro sistema de gestión de incidentes.
- Durante la atención inicial del caso se determinará su criticidad y la metodología para su resolución.
- Se establecerá un primer nivel de atención con el Agente Nivel I de la Mesa de Ayuda a través de la ejecución de un checklist, en conjunto con el cliente, y la validación del problema identificado en nuestra base de conocimiento.
- Si la incidencia aún no es resuelta se procederá con la asignación de 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.
- La atención en sitio con un Ingeniero de Nivel II está disponible únicamente para soluciones instaladas en la ciudad de Bogotá.

A continuación, se detallan los tiempos de 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.

INCIDENTE	TIEMPO DE NOTIFICACIÓN	TIEMPOS DE RESPUESTA	
		Nivel 1	Nivel 2
Crítico	15 min	30 min	1 hora
Alta	30 min	1 hora	1 hora
Media	4 horas	6 horas	12 horas
Baja	8 horas	12 horas	24 horas

- **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.

4.2.8. SERVICIO DE ADMINISTRACIÓN Y GESTIÓN:

Los servicios de administración y gestión de la(s) solución(es) objeto de la actual propuesta están considerados en el presente documento de oferta.

WEXLER SAS prestará los servicios de administración y gestión en modalidad 8x5, a través de la atención de los requerimientos de MACs (modificaciones, adiciones o cambios) elevados por el cliente para todas la(s) solución(es) objeto de la actual propuesta; por el término de 12 meses.

WEXLER SAS garantizará el siguiente alcance para los servicios de administración y gestión:

- Apertura de requerimientos de gestión de cambios de cualquier criticidad a través de nuestra Mesa de Ayuda, vía telefónica **(+57 314 7881987**) o vía correo

electrónico (soporte@wexler.com.co). Por ambos medios la recepción de requerimientos de gestión de cambios estará disponible en horario 8x5.

- Una vez abiertos los casos de requerimientos de gestión de cambios se realizará su registro, gestión y seguimiento a través de nuestra plataforma de soporte.
- Durante la revisión inicial el cliente informará la criticidad de los requerimientos y **WEXLER SAS** informará la metodología para su atención.
- Antes de la ejecución de cualquier cambio, el cliente deberá garantizar que tiene una copia de seguridad de la última configuración vigente en la solución, la cual será restaurada en la solución en caso de que la aplicación del cambio sea fallida y se deba realizar un procedimiento de rollback.
- El cliente deberá autorizar la realización de las actividades administración y gestión bajo la metodología corporativa que tenga vigente sobre su procedimiento de gestión de cambios aprobado al interior de la organización.
- El Ingeniero asignado realizará la configuración de los parámetros de operación y de gestión de la(s) solución(es) objeto de la actual propuesta en modalidad remota.
- El Ingeniero asignado ejecutará las pruebas y validación de funcionalidades de los cambios efectuados.
- Al finalizar el servicio se documentará en la plataforma de soporte con la información detallada sobre los cambios efectuados y con la confirmación del cierre del requerimiento.

A continuación, se detallan los tiempos de atención de requerimientos de gestión de cambios, este tiempo se define como el transcurrido entre el registro del cambio y el inicio de la atención de este por parte de un asesor de soporte y servicio.

SOLICITUD DE CAMBIO	TIEMPOS DE RESPUESTA	HORARIO DE ATENCIÓN
Estándar	6 horas	8x5xNBD
Normal	6 horas	8x5xNBD
Emergencia	2 horas	7x24

- **Cambio Estándar:** Cambios de configuración en los que su riesgo de impacto a la operación es bajo.
- **Cambio Normal:** Cambios de configuración en los que su riesgo de impacto requiere programar su ejecución.
- **Cambio Emergencia:** Cambios requeridos para dar solución a un incidente de prioridad alta/crítica. Puede llegar a requerirse programación para su ejecución.

4.3. PREMISAS Y/O SUPUESTOS

- El alistamiento y entrega de los recursos no especificados en esta propuesta y que resulten de la etapa de diseño son responsabilidad del cliente, **WEXLER SAS** no realizará ninguna tarea de alistamiento o aprovisionamiento de hardware y/o software diferente al que hace referencia esta propuesta.

- Cualquier adecuación adicional o instalaciones de cableado, rack, energía, Internet y demás necesarias para el funcionamiento en el centro de datos o el lugar asignado por el cliente en sus empresas y sitios involucrados en el servicio ofrecido son responsabilidad total de éste, en cumplimiento de las especificaciones del fabricante necesarias para la instalación y funcionamiento adecuado de la solución ofrecida.
- El valor y alcance del servicio que llegare a realizarse se limita al alcance descrito en el presente documento los cuales se corresponden con la solicitud recibida del cliente, todos los servicios no especificados en este documento o sus cambios se encuentran excluidos y pueden tener un valor adicional.
- El cliente es responsable de mantener planes de contingencia y backup de toda su información y a su discreción realizará las acciones requeridas para el manejo de esta, remplazo o restauración en caso de ocurrencia de pérdida o daño por cualquier causa.
- **WEXLER SAS** no tendrá ninguna responsabilidad en la prestación del servicio en el caso de cualquier interrupción causada directa o indirectamente por el cliente y que prohíba o de otro modo limite a **WEXLER SAS** a proporcionar el servicio, entregar soporte según el acuerdo de nivel de servicio o descripciones del servicio administrado, incluyendo, pero no limitado a: mala conducta, negligencia, información inexacta o incompleta, conectividad, entre otros.
- El cliente proveerá a **WEXLER SAS** de un espacio de trabajo en sus instalaciones (en caso de ser necesario) para el acomodamiento de su personal, sitio que deberá incluir como mínimo el aprovisionamiento de servicios de teléfono, impresión, conectividad interna y conexión a Internet, sin costo.
- WEXLER SAS no estará a cargo ni realizará modificación de la configuración de ninguno de los elementos previamente instalados por el cliente entre otros y como ejemplo mencionamos: de comunicaciones o de seguridad o de aplicaciones desarrolladas o de red o de sistemas operativos o cualquiera otro.
- El cliente entregará acceso a los recursos asignados por **WEXLER SAS** a todas las áreas de trabajo que por definición del alcance sean requeridas, de acuerdo con un previo entendimiento entre las partes.
- El cliente dispondrá del personal propio o de sus terceros necesario durante el desarrollo del proyecto para poder garantizar los tiempos de entrega y calidad del servicio.
- El cliente reconoce que el suministro oportuno de espacios de oficinas, instalaciones, equipos, asistencia, cooperación, información completa y exacta por parte de los directores, sus agentes y empleados es esencial para el desempeño de cualquiera de los servicios establecidos en esta propuesta y que no será responsabilidad directa de **WEXLER SAS** el retraso o incumplimiento debido al no acceso oportuno a ellos.

5. PROPUESTA COMERCIAL

4.4. OFERTA ECONÓMICA

ITEM	DESCRIPCIÓN TÉCNICA DE LOS BIENES Y/O SERVICIOS POR CONTRATAR	Unidad de medida / presentación	Cantidades	Precio Unitario	Precio Total
1	Suscripción Licenciamiento solución de protección de marca x 1 año de acuerdo con el anexo técnico detallado	Unidad	1	$496.440.000,00	$496.440.000,00
2	Licenciamiento Gestionado de Prevención de Pérdida de Datos (DLP)– x 1 año	Unidad	100		$43.734.000,00
3	Licenciamiento de Gestión de Accesos Privilegiados (PAM) – x 1 año	Unidad	30		$65.601.000,00
4	Servicio de apoyo para el Plan Estratégico de Seguridad de la Información (PESI) – x 1 vez	Global	1	$118.200.000,00	$118.200.000,00
	VALOR TOTAL				$723.975.000,00

4.5. CONDICIONES COMERCIALES

4.5.1. VIGENCIA DE LA OFERTA:

- Esta oferta tiene una vigencia de treinta (30) días calendario a partir de la fecha de entrega estipulada en la carta de presentación.

4.5.2. INTEGRIDAD DE LA OFERTA:

- La presente oferta es integral y NO podrá ser aprobada/adquirida de manera parcial y/o fraccionada por parte del cliente.

4.5.3. IMPUESTOS:

- Los precios ofertados no incluyen ni IVA ni otros impuestos; en caso de requerirse serán adicionados en los porcentajes y/o montos establecidos por las leyes nacionales, municipales, departamentales que apliquen según la normatividad vigente.

4.5.4. MONEDA:

- La moneda utilizada para la propuesta económica es **pesos COP.**
- La liquidación de la TRM corresponderá a la fecha de emisión de la factura correspondiente.

4.5.5. TIEMPOS DE ENTREGA:

- **WEXLER SAS** entregará los equipos al cliente en un tiempo de 15 días calendario.

- El tiempo para las labores de planeación, diagnóstico, implementación, configuración, puesta a punto y entrega propuesto para todas la(s) solución(es) que son objeto en el presente documento de oferta será de 60 días calendario. Este tiempo comienza a correr desde el momento que se hayan entregado todos los appliances físicos y virtuales, las licencias, suscripciones y demás soluciones que son objeto en el presente documento de oferta.
- **WEXLER SAS** prestará los servicios de soporte técnico en modalidad 24x7 para todas la(s) solución(es) objeto de la actual propuesta, por el término de 12 meses.
- **WEXLER SAS** prestará los servicios de administración y gestión en modalidad 8x5, a través de la atención de los requerimientos de MACs (modificaciones, adiciones o cambios) elevados por el cliente para todas la(s) solución(es) objeto de la actual propuesta; por el término de 12 meses.

4.5.6. MODO DE FACTURACIÓN:

- **WEXLER SAS** emitirá factura de los componentes de hardware y software al 100% después de entregada la totalidad de los componentes de hardware y software.
- **WEXLER SAS** emitirá factura de los servicios profesionales al 100% después de entregados la totalidad de los servicios profesionales.

4.5.7. FORMA DE PAGO:

- El cliente deberá realizar pago hasta treinta (30) días después de la fecha de emisión de la factura correspondiente.
- El pago se realizará en pesos colombianos con la liquidación de la TRM correspondiente a la fecha de emisión de la factura correspondiente.