MICROHOME
Líderes en Tecnología



DIMAR

PROPUESTA DE SERVICIOS:

1. Assessment y Puesta a Punto de Microsoft Defender for Office 365 Plan 2

www.microhome.com.co

MICROHOME
Líderes en Tecnología

PRESENTACIÓN

Bogotá, 27 de febrero 2026

Respetados Señores:
DIMAR
Dirección General Marítima
Bogotá DC

PV-086-JA-26- DIMAR

Atendiendo su requerimiento, nos permitimos presentar la propuesta de servicios para la ejecución de un proyecto especializado de **Assessment y Puesta a Punto de Microsoft Defender for Office 365 Plan 2**, orientado a optimizar las capacidades de protección de correo electrónico y colaboración actualmente disponibles en su entorno Microsoft 365.

DIMAR cuenta actualmente con licenciamiento Office 365 E1 y E3, y ha adquirido Microsoft Defender for Office 365 para la totalidad de las cuentas. El objetivo de este proyecto no es ampliar licenciamiento, sino **maximizar el valor de las capacidades ya disponibles**, fortalecer el nivel de protección frente a amenazas modernas (phishing avanzado, BEC, malware, campañas dirigidas) y optimizar configuraciones existentes bajo buenas prácticas actualizadas del ecosistema Microsoft.

Este servicio se estructura como un proyecto de acompañamiento especializado con enfoque práctico, técnico y estratégico, que permitirá:

- Evaluar el estado actual de configuración y madurez.
- Optimizar capacidades de Plan 1 y Plan 2.
- Ajustar controles en función del contexto real del tenant.
- Transferir conocimiento al equipo técnico interno.
- Entregar una hoja de ruta clara de evolución.

Para Microhome es un honor acompañar a DIMAR en este proceso, aportando experiencia especializada en tecnologías Defender, gobierno de seguridad y protección de la información dentro del ecosistema Microsoft 365.

MICROHOME
Líderes en Tecnología

TABLA DE CONTENIDO

PRESENTACIÓN 2
TABLA DE CONTENIDO 3
SOBRE NOSOTROS 5
Quienes Somos 5
Certificaciones y Reconocimientos 5
Transformación digital 6
Ocho pilares 6
Framework de Ciberseguridad de Microhome 7
PROPUESTA COMERCIAL 9
Propuesta de valor 9
Estrategia y Enfoque de Entrega 9
Principios de ejecución 10
Beneficios Estratégicos del Servicio 10
Detalle de Actividades 11
Workshops Iniciales de Alineación Conceptual 11
Levantamiento y Assessment Técnico 12
Puesta a Punto – Capacidades Base (Plan 1) 13
Puesta a Punto – Capacidades Avanzadas (Plan 2) 14
Hoja de Ruta y Mejora Continua 15
Entregables por Fases 16
Equipo Consultor 17
Credenciales del Equipo Consultor 17
Metodología de Ejecución del Proyecto 18
Indicadores de Éxito 18
Supuestos, Dependencias Y Exclusiones Del Servicio 19
Supuestos y Dependencias 19
Exclusiones del Servicio 19

Consideraciones Finales 20
Valor Agregado de Microhome 20
Propuesta Económica 22
Forma de pago 22
Validez de la Oferta 23
Modalidad del Servicio 23
Condiciones del servicio 23
Confidencialidad y propiedad intelectual 24
Vigencia y ejecución 24

MICROHOME
Líderes en Tecnología

SOBRE NOSOTROS

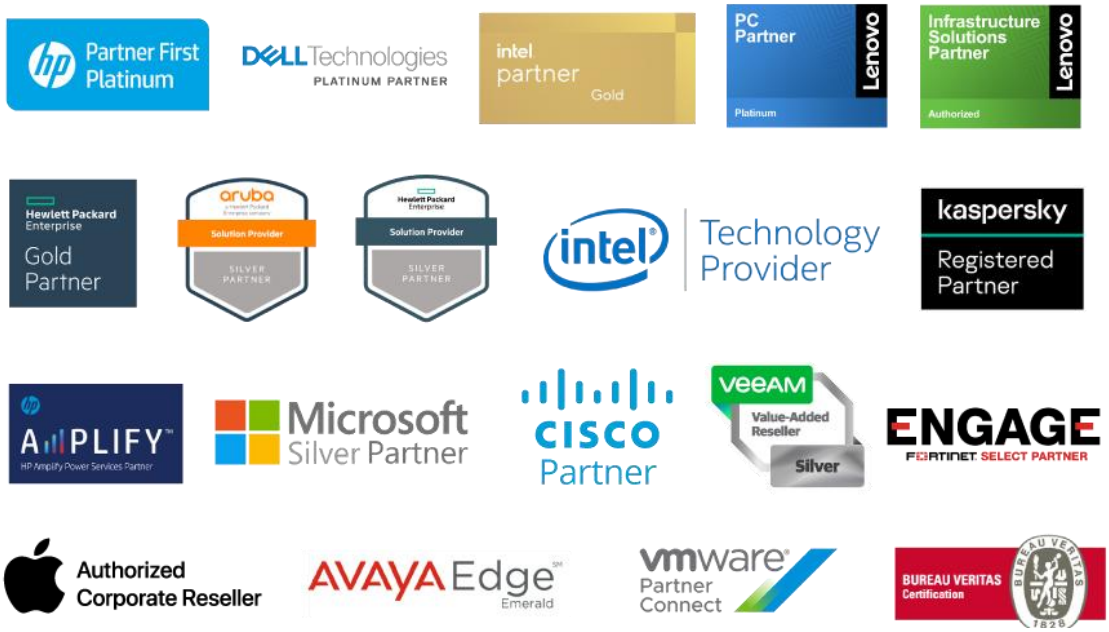
"Contamos con profesionales calificados, que están 100% comprometidos en diseñar y desarrollar las mejores soluciones a nuestros clientes, bajo los mayores estándares de calidad."

Quienes Somos

Microhome S.A.S. es una empresa líder en el área de suministro de soluciones informáticas avanzadas, constituida en 1994 con el objetivo de atender las necesidades crecientes de la tecnología del mercado colombiano, buscando siempre la satisfacción de nuestros clientes.

Contamos con más de 30 años de experiencia en la integración y creación de soluciones de tecnología. Contamos con una infraestructura humana a nivel nacional para atender los requerimientos de nuestros clientes, respaldado por aliados estratégicos quienes siempre nos apoyan aportando valor a su compañía.

Certificaciones y Reconocimientos



MICROHOME
Líderes en Tecnología

Transformación digital

Utilizamos nuestra creatividad y experiencia para garantizar que cada solución que ofrecemos sea flexible, escalable y eficaz para resolver los desafíos empresariales que enfrentan nuestros clientes, permitiendo así, maximizar su potencial y alcanzar sus objetivos comerciales.

Somos una empresa certificada ISO 9001:2015 CO24.05658 en nuestros procesos empresariales garantizando calidad y mejora continua a nuestros clientes.

Ocho pilares



Imagen 1 Pilares de servicios

Con nuestros ocho pilares buscamos brindar un **servicio integral** a todos nuestros clientes ofrecemos precisión técnica en un mercado en rápido movimiento, con escalabilidad y respaldo.

Contando con el apoyo y la confianza de nuestros Partners reconocidos a nivel internacional transmitiendo esta misma confianza, seguridad y respaldo a todos nuestros clientes.

MICROHOME
Líderes en Tecnología

Framework de Ciberseguridad de Microhome

El **Framework de Ciberseguridad de Microhome** constituye la base metodológica que guía todos nuestros servicios y proyectos, integrando las mejores prácticas internacionales con la experiencia acumulada en múltiples industrias.



Imagen 2 Framework de Ciberseguridad

Este marco combina los **pilares del modelo Zero Trust** (Identidad, Dispositivos, Aplicaciones, Datos, Infraestructura y Red) con los **dominios funcionales del NIST Cybersecurity Framework v2.0** (Govern, Identify, Protect, Detect, Respond, Recover).

A través de esta integración, Microhome logra ofrecer una visión **holística, orquestada y medible** de la seguridad organizacional.

Nuestro enfoque permite **alinear tecnología, procesos y personas** bajo una estrategia coherente que:

- Conecta los objetivos de negocio con las políticas de protección de datos y cumplimiento normativo.
- Integra capacidades del ecosistema Microsoft 365, incluyendo **Defender** y otros componentes de seguridad.

- Reduce la complejidad operativa mediante escenarios prácticos y rutas de adopción progresiva.
- Permite medir el avance de madurez en seguridad y cumplimiento en cada etapa del proceso.

El **Framework** se implementa de forma modular y progresiva, adaptándose al nivel de madurez y a las **prioridades reales** de cada cliente. En el caso de DIMAR, este enfoque permite priorizar **controles de protección** sobre el correo electrónico y las plataformas colaborativas, **reducir** la superficie de ataque frente a amenazas modernas como phishing avanzado y suplantación de identidad, y **fortalecer** las capacidades de **detección e investigación** dentro de Microsoft Defender for Office 365. De esta manera, el proyecto no se limita a ajustes técnicos puntuales, sino que contribuye a una evolución estructurada del modelo de operación de seguridad.

De esta manera, cada servicio de Microhome -desde el asesoramiento técnico hasta la implementación avanzada- se ejecuta bajo una misma visión estructurada y sostenible.

MICROHOME
Líderes en Tecnología

PROPUESTA COMERCIAL

Propuesta de valor

El proyecto de Assessment y Puesta a Punto de Microsoft Defender for Office 365 Plan 2 tiene como propósito asegurar que DIMAR obtenga el máximo valor de su inversión en seguridad, fortaleciendo la protección del correo electrónico y las plataformas colaborativas frente a amenazas actuales.

En muchos entornos Microsoft 365, las capacidades de Defender for Office 365 se encuentran habilitadas parcialmente o con configuraciones por defecto que no reflejan el perfil real de riesgo de la organización. Este proyecto permite pasar de una configuración básica o heredada a una configuración optimizada, alineada con:

- Buenas prácticas Microsoft actualizadas.
- Nivel de exposición real del tenant.
- Análisis de telemetría histórica.
- Revisión de Secure Score con criterio técnico.
- Activación controlada de capacidades avanzadas de Plan 1 y 2.

El enfoque combina análisis técnico profundo, implementación práctica, validación conjunta y transferencia estructurada de conocimiento, asegurando sostenibilidad posterior al cierre del proyecto.

Estrategia y Enfoque de Entrega

El servicio contempla la ejecución integral de un proyecto de Assessment y Puesta a Punto de Microsoft Defender for Office 365 Plan 2, incluyendo:

- Alineación conceptual y técnica.
- Evaluación profunda del estado actual del tenant.
- Optimización de capacidades base (Plan 1).
- Activación y ajuste de capacidades avanzadas (Plan 2).
- Implementación controlada y validada.
- Transferencia de conocimiento.
- Entrega de hoja de ruta de evolución.

El proyecto no contempla ampliación de licenciamiento ni implementación de soluciones adicionales fuera del ecosistema Defender for Office 365.

Principios de ejecución

Los principios de ejecución aseguran que el proyecto se mantenga acotado, eficiente y alineado a los objetivos definidos.

- Enfoque en resultados concretos y medibles.
- Alcance acotado y ejecutable dentro de la duración del proyecto
- Priorización de quick wins sobre iniciativas complejas.
- Uso de buenas prácticas y estándares Microsoft.
- Transferencia de conocimiento como parte integral del servicio.
- Alineación con el Framework de Ciberseguridad de Microhome.

Beneficios Estratégicos del Servicio

El proyecto de Assessment y Puesta a Punto de Microsoft Defender for Office 365 Plan 2 permite a DIMAR fortalecer de manera estructurada su postura de seguridad frente a amenazas modernas dirigidas al correo electrónico y entornos colaborativos.

Más allá de una simple revisión de configuración, este servicio genera beneficios estratégicos en cuatro dimensiones clave:

1. Reducción real de superficie de ataque

Mediante el endurecimiento de políticas anti-phishing, protección contra suplantación de identidad (impersonation) y optimización de Safe Links y Safe Attachments, se disminuye significativamente la probabilidad de éxito de campañas de phishing avanzado, Business Email Compromise (BEC) y distribución de malware.

2. Mejora en capacidad de detección e investigación

La activación y optimización de capacidades avanzadas de Plan 2, como Automated Investigation & Response (AIR), Campaign View y Threat Explorer, permite:

- Identificar patrones de ataque de forma más rápida.
- Reducir el tiempo medio de respuesta (MTTR).
- Disminuir carga operativa manual.
- Estandarizar procesos de investigación.

Esto fortalece la capacidad del equipo interno para gestionar incidentes con mayor autonomía y criterio técnico.

3. Optimización basada en telemetría real

El proyecto no se limita a aplicar buenas prácticas genéricas, sino que analiza alertas, incidentes históricos y comportamiento real del tenant. Esto permite tomar decisiones basadas en riesgo concreto y no únicamente en recomendaciones automáticas del Secure Score.

4. Transferencia de conocimiento y madurez operativa

La combinación de sesiones técnicas estructuradas y trabajo hands-on garantiza que el equipo de DIMAR no solo reciba una configuración optimizada, sino que adquiera claridad sobre:

- Cómo operar las herramientas.
- Cómo interpretar alertas.
- Cómo ajustar políticas en el tiempo.
- Cómo evolucionar el modelo de protección.

De esta manera, el proyecto contribuye a una mejora sostenible en la madurez de operación de seguridad y no únicamente a una intervención puntual de configuración.

Detalle de Actividades

El proyecto se estructura en bloques progresivos que combinan alineación conceptual, análisis técnico profundo, optimización controlada y definición de hoja de ruta, asegurando que cada intervención tenga un propósito claro en términos de reducción de riesgo y mejora de madurez.

Workshops Iniciales de Alineación Conceptual

Objetivo

Alinear al equipo técnico de DIMAR respecto a las capacidades reales de Microsoft Defender for Office 365 Plan 1 y Plan 2, su arquitectura de protección, y el impacto directo que cada configuración tiene en la reducción de superficie de ataque.

Relevancia

Muchas organizaciones activan capacidades de Defender sin comprender completamente:

- Cómo fluye un correo dentro del pipeline de análisis.
- En qué punto actúa Safe Links o Safe Attachments.
- Qué diferencia existe entre detección, prevención y remediación automática.
- Cómo opera Automated Investigation & Response (AIR).
- Qué significa realmente mejorar el Secure Score.

Una correcta comprensión conceptual evita configuraciones superficiales o mal priorizadas.

Riesgos Comunes

- Activar políticas sin entender su impacto operacional.
- Configurar Safe Links sin revisar experiencia de usuario.
- No proteger cuentas prioritarias frente a impersonation.
- Asumir que Plan 2 está correctamente operando solo por estar licenciado.
- Tomar decisiones basadas únicamente en el número de Secure Score sin análisis técnico.

Actividades Incluidas

- Revisión de licenciamiento E1/E3 + MDO.
- Diferencias entre Plan 1 y Plan 2.
- Arquitectura técnica de protección de correo.
- Flujo completo de análisis y detención.
- Explicación de ZAP (Zero-hour Auto Purge).
- Modelo de amenazas moderno (phishing dirigido, BEC, malware polimórfico).
- Introducción a Campaign View y Threat Explorer.
- Marco de madurez esperado.

Levantamiento y Assessment Técnico

Objetivo

Determinar el estado real de configuración, madurez y exposición del entorno actual, identificando brechas técnicas, configuraciones heredadas y oportunidades de mejora priorizadas.

Relevancia

El Secure Score por sí solo no refleja el nivel real de protección.

El assessment técnico permite:

- Identificar configuraciones inconsistentes.
- Detectar políticas heredadas o superpuestas.
- Revisar configuraciones por defecto no endurecidas.
- Analizar telemetría real de amenazas.
- Validar si las capacidades de Plan 2 están efectivamente activas.

Riesgos Comunes

- Políticas anti-phishing con protección de impersonation deshabilitada.
- Safe Attachments en modo monitoreo permanente.
- Cuentas críticas sin protección avanzada.

- DKIM/DMARC incompletos o mal configurados.
- Alertas generadas pero no investigadas.
- AIR deshabilitado o sin configuración adecuada.
- Tenant Allow/Block List descontrolada.

Actividades Incluidas

Revisión detallada de:

- Anti-spam policies.
- Anti-phishing policies.
- Safe Links por workload.
- Safe Attachments (Dynamic Delivery).
- Tenant Allow/Block List.
- Preset Security Policies.
- Priority Accounts.
- SPF / DKIM / DMARC.
- Transport Rules asociadas a seguridad.
- ZAP.
- AIR.
- Campaign View.
- Threat Explorer.
- Alertas últimos 90 días.
- Incidentes históricos.
- Secure Score técnico contextualizado.

El análisis se realizará sobre telemetría real del tenant.

Puesta a Punto – Capacidades Base (Plan 1)

Objetivo

Optimizar las capacidades fundamentales de protección preventiva, asegurando que los controles básicos operen bajo estándares endurecidos y alineados al perfil de riesgo de DIMAR.

Relevancia

Las capacidades base son la primera línea de defensa frente a:

- Phishing masivo.

- Malware automatizado.
- Enlaces maliciosos.
- Suplantación de identidad básica.

Si estas configuraciones no están correctamente ajustadas, las capacidades avanzadas pierden efectividad.

Riesgos Comunes

- Safe Links sin protección en Teams o aplicaciones Office.
- Safe Attachments sin Dynamic Delivery.
- Anti-phishing sin protección de dominios similares.
- Cuarentena mal configurada generando fricción operativa.
- Cuentas críticas sin priorización especial.
- Políticas con demasiadas excepciones.

Actividades Incluidas

- Endurecimiento anti-phishing avanzado.
- Configuración avanzada de impersonation protection.
- Optimización Safe Links (correo, Teams, Office).
- Optimización Safe Attachments.
- Protección de cuentas prioritarias.
- Ajuste de cuarentena.
- Eliminación de configuraciones redundantes.
- Validación controlada en entorno productivo.

Puesta a Punto – Capacidades Avanzadas (Plan 2)

Objetivo

Activar y optimizar las capacidades de detección avanzada e investigación automatizada que permiten reducir tiempo de respuesta y contener campañas sofisticadas.

Relevancia

Plan 2 no es solo prevención; es capacidad de investigación y respuesta.

Permite:

- Detectar campañas dirigidas.
- Visualizar patrones de ataque.

- Ejecutar remediaciones automáticas.
- Reducir carga operativa manual.
- Disminuir el tiempo medio de respuesta (MTTR).

Riesgos Comunes

- AIR deshabilitado o mal configurado.
- Alertas generadas pero no investigadas.
- No uso de Campaign View.
- Simulaciones de phishing inexistentes.
- No medir comportamiento de usuarios ante ataques.

Actividades Incluidas

- Activación y ajuste de Automated Investigation & Response.
- Configuración avanzada de Campaign View.
- Capacitación operativa en Threat Explorer.
- Definición y ejecución inicial de Attack Simulation Training.
- Ajustes en detección avanzada.
- Revisión de alertas automatizadas.
- Optimización del flujo de investigación.

Hoja de Ruta y Mejora Continua

Objetivo

Establecer una ruta clara de evolución que permita sostener el nivel de protección alcanzado y evolucionar hacia un modelo más maduro de operación de seguridad.

Relevancia

La seguridad no es un evento puntual sino un proceso continuo.

Sin hoja de ruta:

- Las configuraciones se degradan.
- No se ajustan frente a nuevas amenazas.
- El conocimiento se pierde.
- Se vuelve a depender exclusivamente del Secure Score.

Riesgos Comunes

- Falta de revisión periódica de políticas.
- No medir efectividad de simulaciones.
- No ajustar políticas frente a nuevos patrones.
- Desalineación entre configuración y cambios organizacionales.

Actividades Incluidas

- Documento de recomendaciones priorizadas.
- Identificación de quick wins adicionales.
- Propuesta de revisión trimestral.
- Recomendaciones de monitoreo continuo.
- Sugerencias de integración futura con otras capacidades Defender.

Entregables por Fases

Fase	Entregable	Descripción
Workshops	Documento de alineación técnica	Resumen de arquitectura, capacidades activadas y modelo de amenazas aplicable a DIMAR
Assessment	Informe de Assessment Técnico	Estado actual, brechas identificadas, nivel de madurez, riesgos priorizados
Puesta a Punto Plan 1	Documento de configuraciones base optimizadas	Detalle de políticas ajustadas y criterios aplicados
Puesta a Punto Plan 2	Documento de capacidades avanzadas activadas	Configuración de AIR, Campaign View, Simulación inicial
Cierre	Hoja de Ruta 30-60-90 días	Recomendaciones priorizadas y plan de evolución
Final	Acta de cierre	Validación formal del proyecto

Equipo Consultor

El servicio será ejecutado por un equipo de consultores especializados de Microhome, con experiencia en proyectos de seguridad Microsoft, con foco en Microsoft Defender, protección de correo electrónico y operación de seguridad en Microsoft 365.

La asignación del equipo considera los siguientes roles:

- **Consultor Senior / Arquitecto**

  Responsable del diseño de la arquitectura, toma de decisiones técnicas, validaciones críticas y definición de la hoja de ruta futura.

- **Consultor de Implementación**

  Responsable de la ejecución técnica de las configuraciones acordadas, implementación de controles de seguridad y validaciones funcionales.

- **Soporte Documental / Project Support**

  Apoyo en documentación técnica, elaboración de entregables, coordinación de actividades y soporte durante las fases de validación y cierre.

Microhome asignará los recursos adecuados en función del alcance definido, garantizando continuidad, calidad técnica y cumplimiento de los objetivos del proyecto.

Credenciales del Equipo Consultor

El proyecto será liderado y ejecutado por un equipo especializado en seguridad Microsoft, con experiencia comprobada en tecnologías Defender y gobierno de protección de información.

El liderazgo técnico está a cargo de un profesional con más de 25 años de experiencia en tecnología, ex Microsoft, con experiencia directa en implementación de soluciones Defender y Purview en múltiples organizaciones.

El equipo cuenta con las siguientes credenciales relevantes:

- Certificación SC-200: Microsoft Security Operations Analyst
  Especialización en Microsoft Defender XDR, detección, respuesta e investigación de incidentes.
- Certificación SC-401: Information Security Administrator Associate
  Especialización en protección de datos, gobierno de información y Microsoft Purview.
- Microsoft Most Valuable Professional (MVP) en Seguridad – mención Microsoft Purview
  Reconocimiento otorgado por Microsoft a expertos globales con contribución activa en la comunidad técnica y profundo conocimiento del ecosistema de seguridad.
- Microsoft Certified Trainer (MCT)
  Capacidad formal certificada para entrenar, capacitar y transferir conocimiento técnico de forma estructurada.

La combinación de certificaciones técnicas avanzadas, reconocimiento global como MVP y capacidad pedagógica como MCT permite no solo implementar correctamente las herramientas, sino también garantizar transferencia de conocimiento efectiva, asegurando que el equipo de DIMAR pueda operar, monitorear y evolucionar la solución de forma autónoma.

Metodología de Ejecución del Proyecto

El proyecto se desarrollará bajo un modelo estructurado por bloques progresivos, combinando capacitación, evaluación técnica e implementación controlada.

El modelo se compone de tres capas complementarias:

1. Capacitación y Alineación

Sesiones estructuradas orientadas a fortalecer el entendimiento técnico del equipo interno, asegurando decisiones informadas y sostenibles.

2. Evaluación Técnica Profunda

Análisis detallado del entorno actual, configuraciones, telemetría, alertas e incidentes históricos, permitiendo priorizar acciones con criterio basado en riesgo real.

3. Implementación y Optimización Controlada

Ajuste progresivo de políticas, validación en conjunto con el equipo interno y activación productiva bajo esquema controlado.

Este enfoque permite reducir riesgo operativo, asegurar transferencia de conocimiento y construir madurez técnica progresiva.

Indicadores de Éxito

Los indicadores de éxito permiten medir de forma objetiva el impacto del proyecto, asegurando que las mejoras definidas se traduzcan en un aumento verificable de protección, capacidad de investigación y madurez operativa en Microsoft Defender for Office 365.

Indicador	Resultado Esperado
Brechas críticas identificadas	100% documentadas
Capacidades Plan 2 activadas	>90% operativas
Optimización Secure Score técnico	Mejora cuantificable y contextualizada
Simulación de phishing ejecutada	Al menos 1 ciclo inicial
Transferencia de conocimiento	Ejecutada y validada

Hoja de ruta entregada	100%

Supuestos, Dependencias Y Exclusiones Del Servicio

La ejecución exitosa del servicio descrito en la presente propuesta depende del cumplimiento de ciertos supuestos técnicos, organizacionales y operativos por parte de DIMAR. Asimismo, se definen explícitamente las exclusiones del servicio con el fin de evitar interpretaciones ambiguas respecto al alcance acordado entre las partes.

Supuestos y Dependencias

La correcta ejecución del servicio descrito en la presente propuesta depende del cumplimiento de los siguientes supuestos técnicos, organizacionales y operativos por parte de DIMAR y/o del cliente final donde se ejecutarán las actividades:

1. DIMAR cuenta con licenciamiento Office 365 E1/E3 y Microsoft Defender for Office 365 activo.
2. Se otorgarán permisos administrativos necesarios (Security Admin / Global Reader).
3. Se dispone de logs de los últimos 90 días.
4. DIMAR designará un punto técnico responsable.
5. Las decisiones de activación productiva serán aprobadas por DIMAR.

El incumplimiento o retraso en cualquiera de los supuestos anteriormente descritos podrá impactar el cronograma definido y el esfuerzo estimado.

Exclusiones del Servicio

Quedan expresamente fuera del alcance de la presente propuesta, salvo acuerdo formal por escrito entre las partes:

1. Implementación de Microsoft Defender for Endpoint.
2. Implementación de Microsoft Sentinel.
3. Rediseño estructural de permisos en SharePoint/OneDrive.
4. Soporte continuo posterior al cierre.
5. Servicios fuera del alcance de Defender for Office 365.

Consideraciones Finales

Cualquier requerimiento adicional, modificación de alcance o actividad no contemplada en esta propuesta deberá ser evaluada y acordada formalmente entre DIMAR y Microhome S.A.S., pudiendo implicar ajustes en el cronograma, esfuerzo y condiciones económicas del servicio.

Valor Agregado de Microhome

Microhome aporta a DIMAR un valor diferencial basado en especialización avanzada en el ecosistema de seguridad de Microsoft, con foco particular en Microsoft Defender y en la operación real de entornos productivos.

El valor agregado de este proyecto no radica únicamente en la ejecución técnica de configuraciones, sino en la combinación de experiencia práctica, criterio estratégico y capacidad de transferencia de conocimiento.

Entre los principales elementos diferenciadores se destacan:

1. Especialización en tecnologías Microsoft Defender

El equipo asignado cuenta con certificación SC-200 (Microsoft Security Operations Analyst), directamente relacionada con Microsoft Defender XDR, detección, investigación y respuesta ante incidentes.

Esta certificación garantiza dominio técnico sobre:

- Arquitectura de Microsoft Defender for Office 365.
- Threat Explorer y Campaign View.
- Automated Investigation & Response (AIR).
- Gestión de alertas e incidentes.
- Análisis basado en telemetría real.
- Adicionalmente, la certificación SC-401 (Information Security Administrator Associate) aporta una visión complementaria en gobierno de información y protección de datos, fortaleciendo el criterio técnico al momento de definir controles y priorizar riesgos.

2. Liderazgo técnico con reconocimiento global

La dirección técnica del proyecto está liderada por un Microsoft Most Valuable Professional (MVP) en Seguridad, reconocimiento otorgado por Microsoft a expertos que contribuyen activamente a la comunidad técnica global y mantienen un conocimiento actualizado de las capacidades del ecosistema Defender.

Este reconocimiento asegura acceso temprano a mejores prácticas, evolución de producto y escenarios reales de implementación.

3. Capacidad formal de transferencia de conocimiento

El liderazgo técnico cuenta además con la designación de Microsoft Certified Trainer (MCT), lo que garantiza que la transferencia de conocimiento no se limite a sesiones informales, sino que se estructure de forma pedagógica, clara y alineada a estándares oficiales de formación Microsoft.

Esto permite que el equipo de DIMAR no solo reciba una configuración optimizada, sino que adquiera autonomía para operar y evolucionar la solución.

4. Enfoque basado en riesgo real, no en configuraciones genéricas

Microhome aplica un enfoque basado en análisis de telemetría, revisión de incidentes históricos y evaluación contextual del tenant, evitando implementaciones estándar desconectadas de la realidad operativa.

Cada ajuste de política se realiza con criterio técnico y evaluación de impacto, reduciendo fricción operativa y fortaleciendo efectividad real de protección.

5. Metodología estructurada y sostenible

El proyecto se ejecuta bajo el Framework de Ciberseguridad de Microhome, alineado con principios de Zero Trust y NIST, permitiendo que las mejoras implementadas no sean aisladas, sino parte de una evolución progresiva del modelo de operación de seguridad.

MICROHOME
Líderes en Tecnología

Propuesta Económica

La presente propuesta económica corresponde al **proyecto Assessment y Puesta a Punto Microsoft Defender for Office 365 Plan 2**, con una duración estimada de **dos (2) a tres (3) meses**, de acuerdo con los alcances descritos en este documento. Los cuales incluyen:

- Ejecución integral del alcance descrito.
- Sesiones técnicas estructuradas.
- Análisis offline.
- Documentación formal.
- Entregables por fase.
- Acta de cierre.

El valor del servicio se estructura bajo un esquema de **precio fijo**, calculado en función del esfuerzo estimado, los roles involucrados y la ejecución de las actividades definidas.

Servicio de asesoramiento técnico			
Descripción	Valor neto	IVA	Total
Servicios profesionales – Assessment y Puesta a Punto Microsoft Defender for Office 365 Plan 2.	$ 25.180.000,00	19%	$29.964.200,00

NOTAS

- Los valores se encuentran expresados en pesos colombianos (COP).
- El alcance del proyecto considera un esfuerzo estimado asociado a las actividades indicadas en esta propuesta, distribuidas entre roles de consultoría senior, consultoría de implementación, soporte documental y gestión del proyecto.
- El proyecto tendrá una duración estimada de dos (2) a tres (3) meses contados a partir del acta de inicio formal.

Forma de pago

De acuerdo con las condiciones comerciales estándar de Microhome, se propone la siguiente forma de pago:

- **50%** al inicio del proyecto, contra emisión de orden de compra.
- **50%** al cierre del proyecto, contra entrega y aceptación formal de los entregables finales.

Los pagos se realizarán mediante transferencia bancaria a las cuentas registradas de Microhome S.A.S., dentro de los plazos acordados con el cliente.

MICROHOME
Líderes en Tecnología

Validez de la Oferta

La presente propuesta tendrá una validez de treinta (30) días calendario a partir de su fecha de envío.
Cualquier modificación en los alcances, duración o modalidad del servicio podrá requerir un ajuste proporcional en los valores y condiciones comerciales.

Modalidad del Servicio

El proyecto se ejecutará bajo modalidad de precio fijo (Fix Fee), con una duración estimada de dos (2) a tres (3) meses, dependiendo de la disponibilidad del equipo de DIMAR y los tiempos necesarios para validación y replicación de configuraciones.

La ejecución contempla:

- Al menos dos (2) sesiones semanales de trabajo colaborativo de dos (2) horas cada una.
- Actividades adicionales offline de análisis técnico, documentación y preparación de configuraciones.
- Validaciones conjuntas antes de habilitar cambios productivos.

El precio fijo corresponde al alcance completo descrito en esta propuesta, independiente del número de iteraciones requeridas dentro del marco definido.

Condiciones del servicio

- El servicio será ejecutado en modalidad **remota**, utilizando plataformas de colaboración aprobadas (Microsoft Teams, SharePoint u otras).
- La ejecución del proyecto depende de la disponibilidad de accesos, licencias y recursos técnicos por parte de DIMAR.
- La modalidad contractual corresponde a un **precio fijo**, asociado al alcance definido.
- Las sesiones presenciales, si son requeridas por el cliente, serán objeto de **presupuesto adicional** e incluirán costos de desplazamiento y viáticos en caso de ser fuera del área de Bogotá.
- Todos los valores están expresados en **pesos colombianos (COP)** e incluyen únicamente las actividades detalladas en esta propuesta.
- No se incluyen costos de licenciamiento, hardware, infraestructura ni soporte continuo posterior a la finalización del servicio.
- La aceptación del servicio o de cualquiera de las fases se formalizará mediante **actas de aceptación** firmadas por las partes.
- El cliente deberá designar un **líder o punto de contacto interno** responsable de la coordinación y validación de entregables.
- En esta propuesta no se incluyen alcances adicionales o actividades diferentes a los especificados en este documento.

- **MICROHOME** no se hace responsable por incumplimientos de terceros a los Servicios que se gestionen bajo esta propuesta.
- El cliente asignará a **MICROHOME** acceso remoto a la infraestructura y/o aplicaciones necesarias para cumplir el alcance de esta propuesta.
- El equipo y áreas del cliente deben estar disponibles para su contacto de acuerdo con lo requerido en cada una de las fases de la presente propuesta.
- Los días que se estiman en la presente propuesta son días hábiles, de lunes a viernes de 8:00 AM a 6:00 PM excluyendo los días festivos designados en Colombia.
- El contratante facilitará al contratista todos los requerimientos técnicos, equipos, accesos, permisos, cuentas de usuarios locales, cuentas de correo, insumos, bases de datos y autorizaciones necesarias para desarrollar las actividades con el fin de realizar el desarrollo definido en el alcance.
- El contratante será responsable de las demoras ocasionadas por la no disponibilidad de las necesidades técnicas que puedan afectar la ejecución, plazo y costos definidos.

Confidencialidad y propiedad intelectual

Los términos y condiciones aquí establecidos son de carácter confidencial y exclusivos para **DIMAR**.

Toda la información intercambiada entre DIMAR y Microhome S.A.S. durante la ejecución del servicio será tratada bajo estrictos estándares de confidencialidad y utilizada únicamente para los fines relacionados con el desarrollo del proyecto descrito en la presente propuesta.

Los entregables producidos en el marco del servicio (incluyendo, pero no limitándose a documentos técnicos, reportes, configuraciones, planes de trabajo y hojas de ruta) serán de uso exclusivo de DIMAR para fines internos de la organización.

Microhome S.A.S. conservará la propiedad intelectual de sus metodologías, frameworks, plantillas, modelos de trabajo y herramientas internas utilizadas para la elaboración de dichos entregables, sin que ello limite el derecho de uso interno por parte de DIMAR sobre los resultados obtenidos.

Las obligaciones de confidencialidad aquí descritas se mantendrán vigentes incluso después de finalizada la ejecución del servicio.

Vigencia y ejecución

El proyecto tendrá una duración total estimada de **dos (2) a tres (3) meses**, contados a partir de la fecha de inicio formal definida en el **acta de arranque del proyecto**, la cual será acordada entre DIMAR y Microhome S.A.S. una vez emitida la orden de compra correspondiente.

El cronograma detallado de actividades, hitos y entregables será definido y validado durante la fase inicial del proyecto, considerando las dependencias técnicas, la disponibilidad de recursos y los accesos requeridos por parte de DIMAR.

Cualquier ajuste en las fechas de ejecución, derivado de cambios en el alcance, dependencias técnicas, disponibilidad del cliente o situaciones ajenas a Microhome S.A.S., deberá ser acordado previamente entre las partes y podrá implicar una revisión del cronograma y, de ser necesario, del esfuerzo asociado.

La finalización del proyecto se formalizará mediante la **firma del acta de cierre**, en la cual se dejará constancia de la ejecución de las actividades acordadas y la aceptación de los entregables definidos en la presente propuesta.

MICROHOME
Líderes en Tecnología

MICROHOME
Líderes en Tecnología

GRACIAS

Quedamos atentos a sus inquietudes
o requerimientos adicionales.

Joseb Aldana Restrepo
Gerente de Cuentas Corporativas
Microhome S.A.S.
Móvil: 3144754759
E-mail: Joseb.aldana@microhome.com.co

Sebastián Zamorano A.
Director de Soluciones en Ciberseguridad
Microsoft MVP – Microsoft Purview
Microsoft Certified Trainer (MCT)
Microhome S.A.S.
E-mail: sebastian.zamorano@microhome.com.co