Diseño de un Modelo Tecnológico para la Estandarización del Proceso de Elaboración de Propuestas Comerciales en el Área de Preventa de Ciberseguridad de Controles Empresariales

(Monografía)

Autores:

Diana Marcela Medina Calderón

Paula Andrea Valentín Panqueva

Director:

Juliana Alejandra Arévalo Herrera

UNIVERSIDAD SANTO TOMAS

FACULTAD DE INGENIERIA DE TELECOMUNICACIONES

ESPECIALIZACIÓN EN GESTIÓN DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN

BOGOTÁ, 2025

Contenido

RESUMEN

Esta monografía presenta el diseño de un modelo tecnológico para estandarizar el proceso de elaboración de propuestas comerciales en el área de preventa de ciberseguridad de Controles Empresariales. Se identificó como problema principal la falta de una metodología estructurada, con información descentralizada, procesos manuales y baja trazabilidad, lo que afecta la eficiencia operativa, la tasa de cierre y la competitividad. La propuesta tecnológica se basa en la integración de servicios de Microsoft Azure, incluyendo almacenamiento centralizado (Azure SQL Database, Blob Storage), automatización de flujos (Power Automate, Logic Apps), visualización de datos (Power BI) e inteligencia artificial (Azure OpenAI Service). El modelo de negocio propuesto busca optimizar recursos internos, aumentar la productividad del equipo de preventa y mejorar la experiencia del cliente, asegurando cumplimiento normativo, seguridad de la información y escalabilidad. La solución fue estructurada con un cronograma de implementación de 12 semanas, que incluye fases de diseño, desarrollo, pruebas, capacitación y puesta en producción.

ABSTRAC

This monograph presents the design of a technological model to standardize the commercial proposal development process within the cybersecurity presales area of Controles Empresariales. The main problem identified is the lack of a structured methodology, with decentralized information, manual processes, and low traceability, which negatively impacts operational efficiency, business closing rates, and competitiveness. The proposed solution is based on Microsoft Azure services, including centralized storage (Azure SQL Database, Blob Storage), workflow automation (Power Automate, Logic Apps), data visualization (Power BI), and artificial intelligence (Azure OpenAI Service). The business model aims to optimize internal resources, enhance the presales team's productivity, and improve customer experience, ensuring regulatory compliance, information security, and scalability. The solution is structured through a 12-week implementation plan, including phases of design, development, testing, training, and production deployment.

1. PROBLEMA

1.1 ARBOL DE PROBLEMAS

En las empresas integradoras de tecnología, el área de preventa cumple un papel fundamental en el diseño de soluciones alineadas con las necesidades del cliente, combinando un enfoque técnico con objetivos comerciales. Para garantizar la viabilidad y competitividad de cada propuesta, es clave una coordinación eficiente con mayoristas, equipos de postventa y aliados estratégicos, quienes proporcionan información esencial sobre especificaciones, disponibilidad y costos.

En este contexto, el equipo de preventa de ciberseguridad de Controles Empresariales, conformado por diez ingenieros, enfrenta desafíos críticos debido a la falta de una metodología estandarizada para la gestión de propuestas. Actualmente, la información se maneja de manera manual y descentralizada, lo que genera inconsistencias y dificulta su organización, ya que cada ingeniero administra su propia base de datos. Además, la dependencia de mayoristas y terceros para la obtención de cotizaciones prolonga los tiempos de respuesta, una situación agravada por la ausencia de un área de postventa interna. Estos factores impactan directamente la tasa de cierre de negocios y el cumplimiento de los objetivos comerciales.

El crecimiento del mercado y la demanda de soluciones especializadas requieren procesos ágiles y estructurados. Sin embargo, la falta de un sistema centralizado para la elaboración de propuestas aumenta la carga operativa y el riesgo de errores, afectando la competitividad en un entorno donde la rapidez y precisión son determinantes. La dispersión de la información y la dependencia de múltiples fuentes generan esfuerzos duplicados, retrasan las respuestas y disminuyen la efectividad del área. Asimismo, la falta de sincronización con los tiempos de respuesta de terceros afecta la entrega oportuna de ofertas, impactando la satisfacción del cliente y la rentabilidad del negocio.

A partir de este análisis, el siguiente árbol de problemas **¡Error! No se encuentra el origen de la referencia.** identifica las principales causas y consecuencias de la ausencia de un sistema estructurado en el área de preventa, destacando los factores clave que afectan su eficiencia y competitividad.

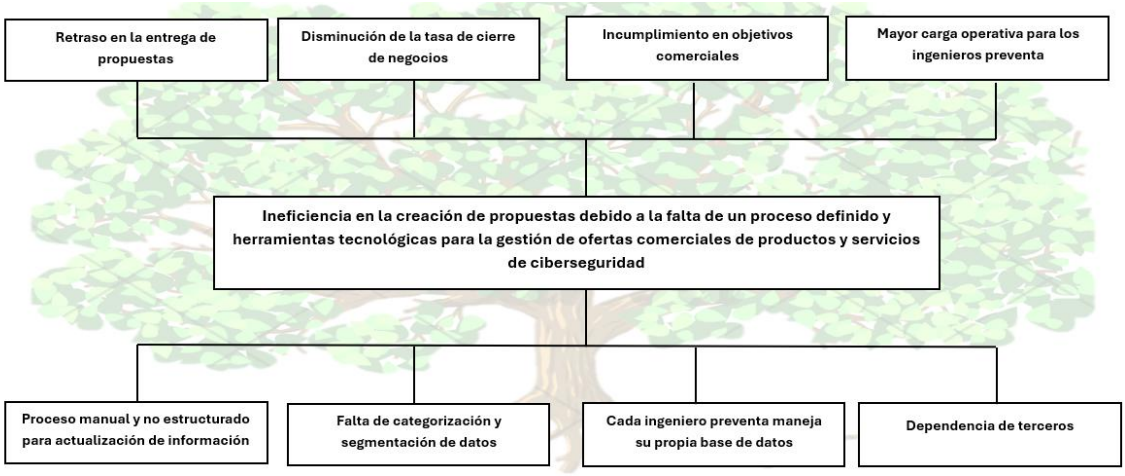

Figura 1 Árbol de problemas - Fuente propia.

1.2 QUE SE QUIERE SOLUCIONAR

En Controles Empresariales, el área de ingeniería preventa enfrenta uno de sus mayores retos: la falta de una base de datos centralizada y eficiente. La información necesaria para la elaboración de propuestas en ciberseguridad se encuentra actualmente dispersa, desactualizada y desorganizada, lo que dificulta la generación de ofertas precisas y ajustadas a las necesidades de cada cliente.

La carencia de un sistema integrado y de herramientas tecnológicas adecuadas obliga a los ingenieros preventa a depender de procesos manuales y fuentes de información aisladas. Esta situación no solo retrasa la entrega de propuestas, sino que también reduce la capacidad de respuesta ante las exigencias del mercado. Como resultado, se ve comprometida la calidad de las soluciones ofrecidas, disminuye la tasa de cierre de negocios y se afecta la rentabilidad y el

posicionamiento competitivo de la empresa en un entorno tan dinámico como el de la ciberseguridad.

El problema principal radica en la falta de un sistema unificado que consolide la información. Los datos no están actualizados, contienen duplicados y carecen de una segmentación adecuada, lo que afecta directamente la calidad y precisión de las propuestas. Además, los procesos manuales y no estructurados para la actualización y gestión de la información generan inconsistencias, errores y retrasos. La dispersión de la información es otro desafío crítico, ya que cada ingeniero preventa gestiona su propia base de datos, lo que resulta en fragmentación y falta de estandarización. Esto incrementa el tiempo invertido en la búsqueda de datos y el riesgo de utilizar información obsoleta o inexacta. A esto se suma la falta de segmentación y categorización de los datos, lo que dificulta identificar soluciones adecuadas para cada cliente y limita la capacidad de ofrecer un servicio diferenciado.

Las consecuencias de esta ineficiencia son múltiples y afectan significativamente el desempeño del área preventa. En primer lugar, el retraso en la entrega de propuestas surge como resultado directo de la falta de herramientas tecnológicas y de una base de datos centralizada. En segundo lugar, la baja tasa de cierre de negocios se debe a la incapacidad de crear propuestas con datos segmentados, estructurados y actualizados. En tercer lugar, el incumplimiento de los objetivos comerciales se convierte en una realidad, ya que la ineficiencia impacta directamente en la capacidad de generar ingresos. Además, la sobrecarga de trabajo y el estrés del equipo aumentan debido a la dependencia de bases de datos dispersas y desactualizadas, lo que reduce la productividad y aumenta el riesgo de errores.

Para abordar estas problemáticas, es esencial implementar un sistema integrado y eficiente que permita gestionar de manera ágil, estandarizada y colaborativa la

creación de propuestas de ciberseguridad. La centralización de la información, junto con herramientas tecnológicas adecuadas, optimizará los flujos de trabajo y permitirá adaptar las propuestas a las necesidades específicas de cada cliente. Esto no solo mejorará la calidad de las ofertas y reducirá los tiempos de respuesta, sino que también aumentará la competitividad de la empresa en el mercado.

Finalmente, la falta de una base de datos centralizada y de procesos eficientes ha generado desafíos significativos, pero con la implementación de soluciones tecnológicas y organizativas, es posible superar estas limitaciones y potenciar el crecimiento del negocio.

2. IDEACIÓN DE LA SOLUCIÓN

La eficiencia en la gestión de propuestas en el área de preventa de ciberseguridad es un factor clave para mejorar la competitividad y la conversión de oportunidades comerciales. Actualmente, la falta de una estructura optimizada en estos procesos genera retrasos, inconsistencias y una sobrecarga operativa, lo que impacta la calidad de las ofertas y la capacidad de respuesta ante clientes estratégicos.

Para abordar esta problemática, se plantea una solución basada en la automatización y centralización del flujo de trabajo en la elaboración de propuestas. Este sistema integrará procesos y herramientas para la gestión categorizada de datos, lo que permitirá la generación eficiente de propuestas, asegurando la trazabilidad de la información y reduciendo los tiempos operativos.

El diseño del sistema se fundamenta en estándares internacionales de calidad y seguridad con un enfoque estructurado y alineado con las mejores prácticas del sector. Asimismo, la incorporación de buenas prácticas permitirá mejorar la estandarización y optimización de los servicios, asegurando eficiencia en la toma de decisiones estratégicas y en la entrega de soluciones de ciberseguridad.

2.1 POR QUÉ SE PLANTEA AHORA LA SOLUCIÓN

El planteamiento de esta solución responde a la rápida evolución del mercado de ciberseguridad y a la creciente demanda de propuestas precisas y estructuradas en tiempos cada vez más reducidos. La descentralización de la información y la dependencia de metodologías manuales generan ineficiencias operativas que afectan la competitividad y limitan la capacidad de respuesta ante las oportunidades de negocio.

A nivel global, la inversión en ciberseguridad sigue en aumento. Según Kaspersky IT Security Economics, las pérdidas financieras por incidentes cibernéticos han llevado a un crecimiento proyectado del 9 % en los presupuestos de seguridad informática [1]. Para aprovechar esta tendencia, es fundamental optimizar los procesos de preventa, asegurando rapidez y precisión en la elaboración de propuestas.

Actualmente, la falta de un sistema centralizado dificulta la trazabilidad de la información, retrasa la entrega de propuestas y puede generar la pérdida de oportunidades estratégicas. Sin una metodología estructurada, la generación de propuestas sigue siendo un proceso manual, poco escalable y con impacto negativo en la eficiencia operativa y la capacidad de respuesta ante los clientes.

Desde una perspectiva normativa, adoptar estándares internacionales mejora la gestión de preventa. ISO 9001 enfatiza la optimización de procesos para garantizar la satisfacción del cliente, mientras que ISO/IEC 27001 subraya la importancia de la seguridad en la gestión de la información, un aspecto clave en la elaboración de propuestas de ciberseguridad. Además, ITIL facilita la estandarización de flujos de trabajo y la mejora en la entrega de servicios en entornos regulados.

La automatización es clave para superar estos desafíos. Gartner señala que la digitalización transforma los modelos de negocio, generando nuevas oportunidades y optimizando la eficiencia operativa [2]. Sin un sistema estructurado, la escalabilidad y sostenibilidad del área de preventa se ven comprometidas, aumentando la dependencia de procesos manuales y elevando el riesgo de errores. Implementar una solución centralizada y automatizada facilitará la integración de herramientas que mejoren la trazabilidad, reduzcan los ciclos de revisión y optimicen la capacidad de respuesta ante los clientes.

En definitiva, transformar la gestión de preventa con procesos automatizados y estandarizados no solo mejorará la eficiencia operativa, sino que también fortalecerá la posición de la empresa en el mercado de ciberseguridad. Este enfoque garantizará un crecimiento sostenible y una ventaja competitiva a largo plazo.

2.2 SECTOR OBJETIVO

Para optimizar la generación de propuestas técnicas y comerciales en la preventa de soluciones de ciberseguridad, es fundamental establecer procesos eficientes que permitan responder con rapidez y precisión a las necesidades del cliente. Actualmente, el equipo de preventa de ciberseguridad de Controles Empresariales enfrenta desafíos en la integración de componentes, la gestión de información técnica y la automatización de tareas repetitivas, lo que afecta los tiempos de respuesta y la calidad de las propuestas comerciales.

La solución requiere un flujo de trabajo estructurado, soportado en herramientas tecnológicas avanzadas y metodologías ágiles, que optimicen la colaboración y reduzcan la carga operativa. El objetivo es que el equipo de preventa disponga de plataformas de trabajo eficientes, acceso centralizado a información actualizada sobre soluciones y normativas, así como procesos automatizados que agilicen la elaboración de propuestas comerciales.

Además, una mayor integración entre las áreas involucradas garantizará que cada propuesta refleje con precisión las capacidades de la solución y su alineación con los riesgos y necesidades del cliente. Esto no solo mejorará los tiempos de respuesta, sino que también elevará la calidad y diferenciación de las propuestas, fortaleciendo la competitividad en el mercado.

2.3 TENDENCIAS DEL SECTOR

El proceso de preventa en ciberseguridad ha evolucionado significativamente en los últimos años debido a la creciente complejidad de las amenazas y la necesidad de soluciones adaptadas a entornos empresariales dinámicos. Las organizaciones han implementado diversas tendencias para mejorar la eficiencia en la elaboración de propuestas técnicas y comerciales, optimizando tiempos y asegurando una mayor precisión en la entrega de soluciones de seguridad.

Una de las principales tendencias es la automatización de los procesos de preventa mediante herramientas especializadas en la generación de propuestas. Plataformas como CPQ (Configure, Price, Quote) permiten estandarizar la configuración de soluciones, calcular costos de manera precisa y generar cotizaciones en menor tiempo. Estas herramientas no solo agilizan la elaboración de ofertas, sino que también reducen errores en la configuración de los servicios y productos de ciberseguridad [3].

Otra tendencia relevante es el uso de inteligencia artificial (IA) y analítica avanzada para la personalización de propuestas. Mediante el análisis de datos históricos y patrones de adquisición de clientes, los equipos de preventa pueden anticipar necesidades específicas y diseñar soluciones más alineadas con los requisitos de cada organización. Además, el uso de IA permite optimizar la selección de productos y servicios, asegurando una mejor adecuación a los riesgos y requerimientos del cliente [4].

En este contexto, la adopción de plataformas en la nube como AWS, Azure y Google Cloud (GCP) ha sido clave en la gestión de procesos y gobernanza de datos dentro de la preventa en ciberseguridad. Estas plataformas ofrecen herramientas avanzadas para la clasificación, protección y monitoreo de datos, garantizando el cumplimiento de normativas como GDPR, ISO 27001 y el marco NIST. La implementación de políticas de gobernanza en la nube permite estandarizar el

manejo de información sensible, asegurando la trazabilidad y control de accesos en cada fase del proceso de preventa. Asimismo, la integración de soluciones como AWS Lake Formation, Azure Purview y Google Data Catalog facilita la centralización y administración de datos, optimizando la toma de decisiones basada en información confiable y estructurada. Con ello, los equipos de preventa pueden generar propuestas alineadas con requisitos de seguridad y cumplimiento normativo, fortaleciendo la confianza del cliente y reduciendo riesgos operacionales.

El enfoque en la colaboración interdepartamental también ha cobrado relevancia. Las empresas han implementado plataformas de trabajo colaborativo donde los equipos de preventa pueden interactuar con ingenieros, consultores y especialistas en cumplimiento normativo. Esta sinergia facilita la construcción de propuestas integrales que no solo consideran aspectos técnicos, sino también normativas y requerimientos específicos del sector, como ISO 27001 o el marco NIST [5].

Por último, la integración de metodologías ágiles en la preventa ha demostrado ser una estrategia efectiva. A través de la implementación de frameworks como Scrum o Kanban, los equipos pueden gestionar de manera eficiente el ciclo de vida de una propuesta, estableciendo entregables parciales y optimizando la iteración con clientes y equipos internos. Esto permite ajustes rápidos en las propuestas y una mayor adaptabilidad ante cambios en los requerimientos de seguridad [6].

2.4 ÁRBOL DE OBJETIVOS

El árbol de objetivos se centra en la mejora de la gestión del área de preventa de productos y servicios de ciberseguridad, partiendo de la necesidad de implementar y unificar bases de datos que actualmente se encuentran fragmentadas. Al no contar con información centralizada, se dificulta la eficiencia en los procesos y se incrementan los tiempos de entrega de propuestas. Por ello, se busca estandarizar y categorizar los datos, adoptando herramientas tecnológicas que permitan una gestión más integrada y eficiente. Este enfoque no solo facilitará el acceso a la

información, sino que también fortalecerá el rol estratégico del área de preventa, asegurará el cumplimiento de los objetivos comerciales y mejorará la satisfacción del cliente al reducir los tiempos de respuesta y optimizar la calidad del servicio.

A continuación, en la **¡Error! No se encuentra el origen de la referencia.** se detallan los impactos esperados y los objetivos propuestos para transformar significativamente los procesos de gestión del área de preventa.

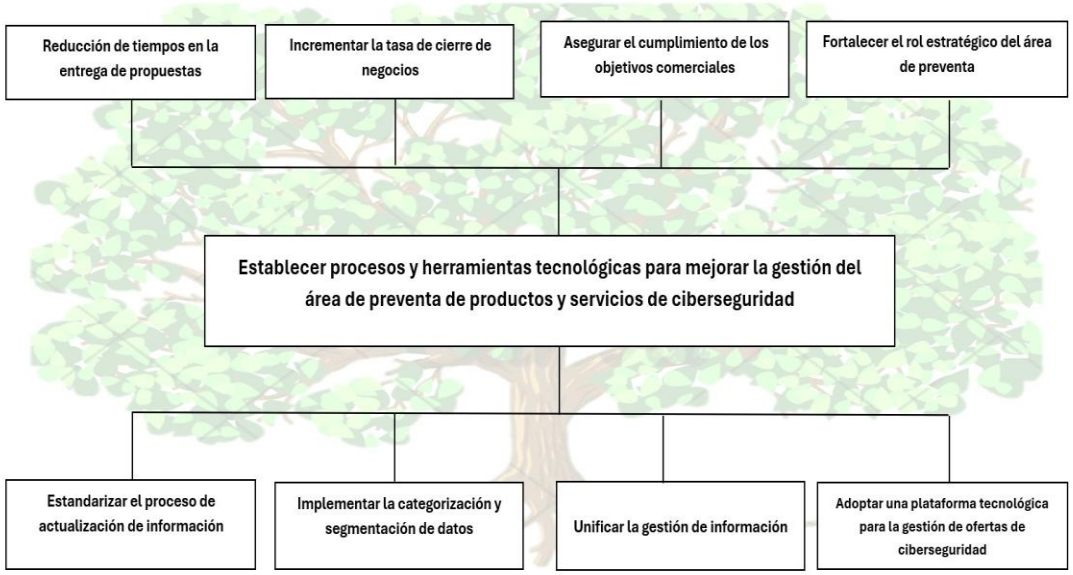

Figura 2 Árbol de objetivos - Fuente propia

2.5 CUÁL ES LA SITUACIÓN DESEADA

Para optimizar la generación de propuestas técnicas y comerciales en la preventa de soluciones de ciberseguridad, es fundamental establecer procesos eficientes que permitan responder con rapidez y precisión a las necesidades del cliente. Actualmente, el equipo de preventa de ciberseguridad de Controles Empresariales enfrenta desafíos en la integración de datos, la gestión de información técnica y la automatización de tareas repetitivas, lo que afecta los tiempos de respuesta y la calidad de las propuestas.

La solución requiere un flujo de trabajo estructurado, soportado en herramientas tecnológicas avanzadas que optimicen la colaboración y reduzcan la carga

operativa. El objetivo es que el equipo de preventa disponga de plataformas de trabajo eficientes, acceso centralizado a información actualizada sobre soluciones y normativas, así como procesos automatizados que agilicen la elaboración de propuestas.

Además, una mayor integración entre las áreas involucradas garantizará que cada propuesta refleje con precisión las capacidades de la solución y su alineación con los riesgos y necesidades del cliente. Esto no solo mejorará los tiempos de respuesta, sino que también elevará la calidad y diferenciación de las propuestas, fortaleciendo la competitividad en el mercado.

2.6 INTRODUCCIÓN A LA SITUACIÓN DESEADA

La Figura 3 representa un diagrama de flujo en notación BPMN que describe el proceso de preventa del área de ciberseguridad en Controles Empresariales, destacando la interacción entre diversas áreas, como comercial, ingeniería preventa, cliente y mayoristas/aliados. El flujo inicia con el registro de una oportunidad en el CRM por parte del área comercial, seguido de la asignación del requerimiento a un ingeniero preventa. En esta etapa, se evalúa si es necesaria una sesión con el cliente para comprender sus necesidades y recopilar información. Si se requiere, se agenda una reunión y se documentan los requerimientos; de lo contrario, se analiza el RFP del cliente y, si es necesario, se formulan preguntas para su aclaración. Posteriormente, se realiza la cotización siempre que los costos de productos y servicios estén disponibles en la base de datos. De no ser así, se consulta con mayoristas y aliados antes de elaborar y enviar la propuesta final al cliente.

El proceso evidencia una dependencia significativa de la disponibilidad de precios en la base de datos, lo que puede generar demoras si es necesario consultar con terceros. Asimismo, resalta la importancia de la comunicación efectiva con el cliente para recopilar información clave y aclarar dudas mediante la interacción con

mayoristas y aliados. Desde una perspectiva de ingeniería preventa, este flujo pone de manifiesto la necesidad de optimizar la gestión de la información , sugiriendo oportunidades de mejora como la consolidación de una base de datos actualizada que agilice el proceso de cotización y propuesta, reduciendo tiempos de respuesta y aumentando la eficiencia operativa.

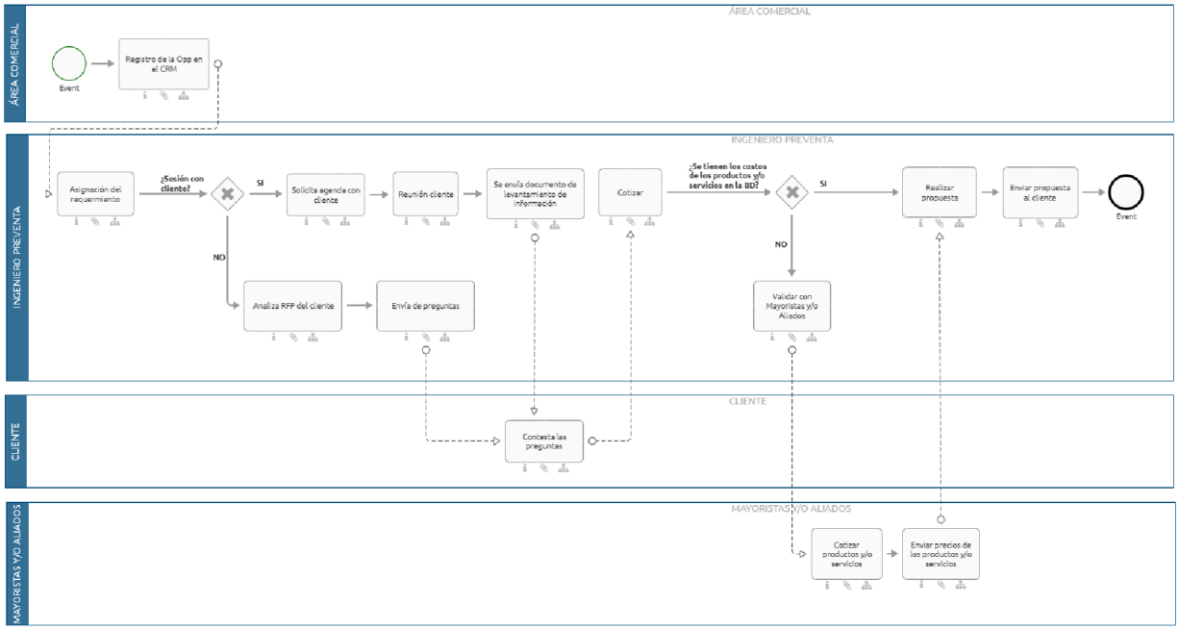

Figura 3 Diagrama proceso actual - Fuente propia.

Frente a esta situación, la implementación de un sistema centralizado y automatizado permitiría optimizar la gestión del área, mejorando la eficiencia y reduciendo la carga operativa de tareas repetitivas. La incorporación de herramientas tecnológicas facilitaría la agilización de los flujos de trabajo, permitiendo tiempos de respuesta más rápidos y precisos. Además, el crecimiento del mercado de ciberseguridad representa una oportunidad para fortalecer las relaciones con aliados estratégicos mediante procesos más eficientes, lo que contribuiría a mejorar la competitividad de la empresa en un entorno cada vez más exigente.

A pesar de estas oportunidades, la competencia con empresas que han optimizado sus procesos representa una amenaza latente. La dependencia de los tiempos de respuesta de terceros puede afectar la capacidad de respuesta ante los clientes, generando demoras que impactan la percepción del servicio. Asimismo, los cambios en la demanda de servicios pueden requerir una adaptación rápida para evitar la obsolescencia de las estrategias comerciales. También existen posibles dificultades en la adopción de nuevos estándares, lo que podría retrasar la implementación de mejoras tecnológicas clave para la optimización del área de preventa.

No obstante, Controles Empresariales cuenta con fortalezas que pueden ser aprovechadas para impulsar esta transformación. La presencia de un equipo de ingenieros especializados permite un enfoque técnico sólido en la elaboración de propuestas, mientras que la relación con mayoristas y aliados estratégicos facilita el acceso a soluciones innovadoras. Además, la combinación de conocimientos técnicos y comerciales brinda una ventaja competitiva al momento de diseñar estrategias adaptadas a las necesidades del mercado. La visión estratégica orientada a mejorar la competitividad debe ser el eje central para la toma de decisiones, asegurando que las mejoras implementadas no solo resuelvan las deficiencias actuales, sino que también preparen a Controles Empresariales para enfrentar desafíos futuros con mayor solidez.

La situación deseada implica establecer procesos claros y adoptar herramientas tecnológicas que permitan mejorar la gestión del área de preventa en ciberseguridad. Para lograrlo, es fundamental realizar un análisis detallado de las debilidades, oportunidades, fortalezas y amenazas mediante la metodología DOFA, lo que permitirá diseñar una estrategia efectiva para optimizar el desempeño del área y consolidar una ventaja competitiva en el mercado.

A continuación, en la Tabla 1**¡Error! No se encuentra el origen de la referencia.** presentamos el análisis desde la matriz DOFA, donde se identifican los factores

clave que influyen en la gestión del área de preventa en ciberseguridad de Controles Empresariales.

DEBILIDADES:	OPORTUNIDADES:
(A) Falta de metodología estandarizada. (B) Uso de procesos manuales y descentralizados. (C) Dependencia de mayoristas y terceros. (D) Ausencia de un área de postventa interna. (E) Dispersión y falta de actualización en la base de datos. (F) Retrasos en la entrega de propuestas y baja tasa de cierre.	(1) Implementación de un sistema centralizado y automatizado. (2) Uso de herramientas tecnológicas para agilizar flujos de trabajo. (3) Crecimiento del mercado de ciberseguridad. (4) Fortalecimiento de relaciones con aliados estratégicos mediante procesos más eficientes.
FORTALEZAS:	**AMENAZAS:**
(A) Equipo de ingenieros especializados. (B) Relación con mayoristas y aliados estratégicos. (C) Enfoque técnico y comercial en la elaboración de propuestas. (D) Visión estratégica para mejorar competitividad.	(1) Competencia con empresas que han optimizado sus procesos. (2) Dependencia de los tiempos de respuesta de terceros. (3) Cambios en el mercado que afecten la demanda de servicios. (4) Posibles dificultades en la adopción de nuevos estándares.

Tabla 1 Análisis DOFA. Fuente propia

La siguiente matriz Tabla 2 permite evaluar la relación entre las debilidades y fortalezas de la organización con las oportunidades y amenazas del entorno. Su propósito es identificar el grado de influencia y dependencia de cada factor dentro del análisis estratégico, facilitando la toma de decisiones.

El cruce de factores se representa mediante marcas que indican la interacción entre debilidades y fortalezas con oportunidades y amenazas. Estas interacciones reflejan el impacto de cada variable en el entorno y ayudan a visualizar la importancia de cada una dentro del análisis.

		OPORTUNIDADES				AMENAZAS			
		1	2	3	4	1	2	3	4
DEBILIDADES	A	x	x			x			x
	B	x	x				x	x	
	C				x		x		
	D	x					x		
	E	x	x					x	
	F		x		x	x	x		
FORTALEZAS	A			x		x			
	B				x		x		
	C	x		x				x	
	D		x	x	x				x

Tabla 2 Matriz DOFA - Fuente propia

Por otra parte, en la Tabla 3, las filas representan los factores que ejercen influencia, mientras que las columnas muestran aquellos que dependen de estas influencias. Los valores numéricos reflejan la intensidad de la relación entre cada par de elementos, donde un número mayor indica una mayor influencia o dependencia.

Los totales de la última columna y fila permiten visualizar qué factores tienen mayor capacidad de afectar a otros (influencia) y cuáles son más susceptibles a ser afectados (dependencia). Este análisis facilita la toma de decisiones estratégicas al resaltar los puntos críticos en la estructura organizacional.

MATRIZ DE INFLUENCIA	A	B	C	D	E	F	INFLUENCIA
A-Metodología estandarizada		3	1	0	3	3	**10**
B-Procesos manuales y descentralizados	3		1	0	3	3	**10**
C-Dependencia de mayoristas y terceros	1	1		3	2	3	**10**
D-Area de postventa interna	1	2	3		0	3	**9**
E-Dispersión y falta de actualización en la base de datos	3	3	2	0		3	**11**

F-Retrasos en la entrega de propuestas y baja tasa de cierre	3	3	3	0	3		**12**
DEPENDENCIA	**11**	**12**	**10**	**3**	**11**	**15**	

Tabla 3 Matriz de influencia - Fuente propia

Teniendo en cuenta el análisis anterior, en la **¡Error! No se encuentra el origen de la referencia.** se visualiza el análisis de influencia y dependencia el cual revela que los principales problemas de los ingenieros del área de preventa se concentran en los actores de alcance, lo que significa que, aunque dependen de factores externos, también tienen un alto impacto en la operación. La falta de metodología estandarizada, el uso de procesos manuales, dispersión y falta de actualización de la base de datos y la dependencia de mayoristas afectan la eficiencia y competitividad, generando retrasos en la entrega de propuestas y reduciendo la tasa de cierre. Para mejorar estos aspectos, la solución debe centrarse en la automatización y centralización de procesos optimizando la gestión.

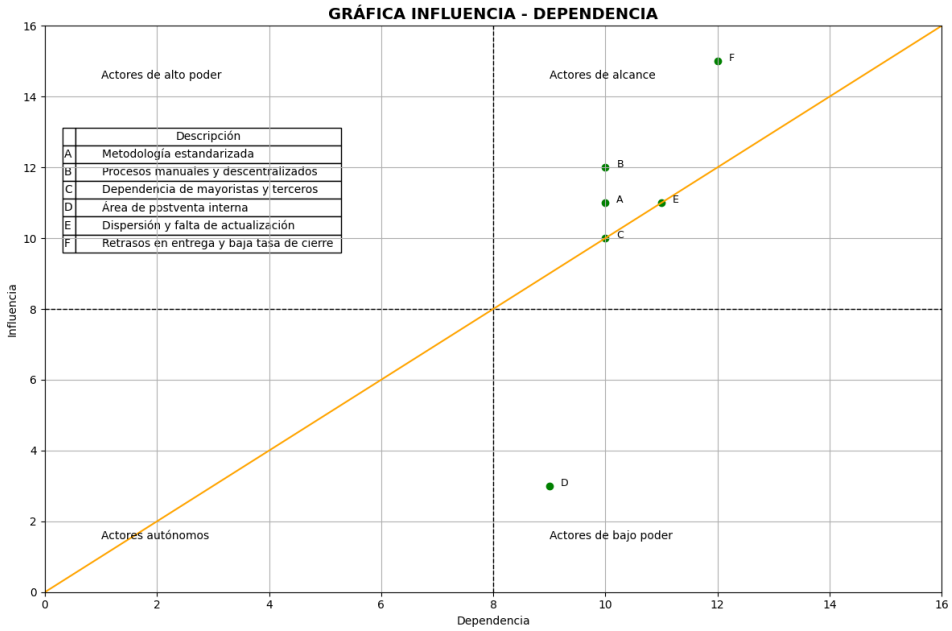

Figura 4 Gráfica Influencia - Dependencia - Fuente propia.

3. ANÁLISIS DE LAS ALTERNATIVAS TÉCNICAS PARA SOLUCIONAR EL PROBLEMA

Para optimizar la gestión de propuestas en el área de preventa de ciberseguridad, se pueden considerar diversas soluciones en la nube que permitan centralizar la información, automatizar procesos, mejorar la generación de propuestas y facilitar la visualización de datos. En cuanto al almacenamiento y gestión de datos, Azure SQL Database, Amazon RDS y Google Cloud Firestore son opciones escalables y seguras. Azure SQL Database se integra de manera nativa con Microsoft 365, facilitando la administración de datos relacionales, mientras que Amazon RDS permite una mayor flexibilidad en la selección de motores de bases de datos, lo que brinda más personalización. Por otro lado, Google Cloud Firestore es ideal para entornos con sincronización en tiempo real, aunque su enfoque NoSQL puede no ser el más adecuado si se requiere una estructura relacional estricta. La elección dependerá del nivel de integración necesario y la estrategia de gestión de datos de la empresa.

Para mejorar la eficiencia operativa mediante la automatización de procesos, se pueden evaluar Azure Logic Apps y Power Automate, AWS Step Functions y Lambda, y Google Cloud Workflows. Power Automate destaca por su facilidad de uso dentro del ecosistema Microsoft, permitiendo la integración con SharePoint y Dynamics 365 sin necesidad de programación avanzada, aunque algunas funciones requieren licencias premium. AWS Step Functions y Lambda proporcionan una orquestación sin servidor altamente flexible, pero requieren mayor conocimiento técnico para su configuración. Google Cloud Workflows ofrece una alternativa eficiente dentro de GCP con capacidades avanzadas de orquestación de procesos, aunque su adopción puede ser más compleja. Un aspecto clave en esta optimización es la visualización de datos, donde Power BI se presenta como una alternativa más robusta que Excel, ya que permite la conexión directa a bases de datos en la nube, generación de dashboards interactivos y actualización en tiempo

real de los datos. A diferencia de Excel, que tiene limitaciones en el manejo de grandes volúmenes de información y carece de capacidades avanzadas de visualización e integración con IA, Power BI ofrece análisis predictivos, integración con servicios en la nube y un acceso más eficiente a reportes dinámicos.

En la generación automatizada de propuestas, la inteligencia artificial juega un papel clave con soluciones como Azure OpenAI, AWS Bedrock y Google Vertex AI
Azure OpenAI permite la integración directa con Word y SharePoint, facilitando la creación automática de propuestas y optimizando la redacción basada en datos históricos. AWS Bedrock ofrece modelos de IA generativa altamente personalizables con almacenamiento en S3, lo que lo hace ideal para empresas que buscan mayor control sobre su información. Google Vertex AI, por su parte, permite la personalización avanzada de modelos de aprendizaje automático, aunque su implementación puede ser más compleja. Para potenciar el análisis de la información generada, Power BI se destaca nuevamente al ofrecer reportes interactivos y en tiempo real sobre métricas clave como tiempos de respuesta, costos y tasas de cierre de negocios. La elección de las herramientas dependerá de la infraestructura existente y del grado de personalización requerido.

4. MODELO DE NEGOCIO

Este capítulo describe el modelo de negocio que respalda la solución tecnológica diseñada para el área de preventa de Controles Empresariales. Se presenta cómo cada componente: propuesta de valor, segmentos de clientes, canales, relaciones, fuentes de ingresos, recursos, actividades, socios y estructura de costos, donde se integran para ofrecer un valor diferencial en la generación de cotizaciones y la gestión de servicios de ciberseguridad. El enfoque de esta propuesta muestra la viabilidad y sostenibilidad de la solución y cómo impacta tanto a los equipos internos como a los clientes externos.

1. Propuesta de Valor

La propuesta de valor se basa en dos pilares: automatización del flujo de trabajo de preventa e inteligencia artificial aplicada al análisis de oportunidades. La automatización puede generar convertir en minutos la generación de cotizaciones para servicios de ciberseguridad, eliminando tareas manuales de compilación y envío de documentos. Con esto, el equipo de preventa puede concentrarse en el análisis técnico de cada oportunidad y en la relación directa con el cliente, en lugar de perder tiempo en procesos administrativos.

Simultáneamente, herramientas de visualización unifican métricas clave en tiempo real: número de cotizaciones emitidas, tasa de conversión, margen proyectado y estado de aprobaciones internas. Esta visibilidad facilita la toma de decisiones del gerente de preventa y la dirección de Controles Empresariales para ajustar asignaciones de recursos, identificar tendencias de demanda por sector detectar servicios de baja aceptación. Adicionalmente, la capa de inteligencia artificial se puede configurar en servicios basadas en patrones históricos: por ejemplo, incluir monitoreo continuo para clientes del sector financiero cuando detecta

oportunidades similares previas. Esta recomendación automatizada no solo agiliza la elaboración de propuestas, sino que aumenta la pertinencia de las ofertas.

Por último, es fundamental contar con soluciones que integren políticas estrictas de seguridad y cumplimiento. El adecuado resguardo de información sensible como cotizaciones, plantillas contractuales y aprobaciones, así como el control de accesos basado en roles, permiten garantizar la confidencialidad y trazabilidad de los datos. Esta gestión segura de la información fortalece la confianza de los clientes y asegura el cumplimiento de los estándares internos de ciberseguridad. En este contexto, la incorporación de procesos automatizados, inteligencia artificial y medidas de seguridad sólidas se convierte en un elemento diferenciador que mejora la eficiencia y calidad del área de preventa en Controles Empresariales.

2. **Segmentos de Clientes**

El modelo de negocio identifica dos niveles de clientes: internos y externos.

- **Clientes internos (dirección y gerencia de Controles Empresariales):** Requieren visibilidad consolidada de la operación de preventa relacionados con el volumen de cotizaciones, tasas de cierre, rentabilidad proyectada, entre otros, con el fin para planificar recursos, justificar inversiones en herramientas y diseñar estrategias comerciales.

- **Clientes externos (empresas que solicitan servicios de ciberseguridad):** Principalmente organizaciones medianas y grandes en sectores regulados tal como banca, educación y salud, que demandan propuestas técnicas detalladas, con requisitos de cumplimiento normativo claros y en plazos reducidos. Estos clientes valoran la rapidez de respuesta y la calidad de las recomendaciones.

La solución beneficia a ambos segmentos: el equipo interno dispone de métricas en tiempo real y flujos estandarizados, mientras que los clientes externos reciben propuestas precisas, alineadas con sus requerimientos y la normativa aplicable.

3. **Canales y Relaciones con Clientes**

Para el área de preventa, los canales de interacción incluyen:

- **Plan directo especializado**: Demostraciones personalizadas, análisis de procesos y elaboración de un plan de implementación.
- **Portal de autoservicio con PoC**: Prueba de concepto breve para evaluar funcionalidades (cotizaciones, dashboards) y acceder a manuales y foros.
- **Consultoría pre-venta**: Un consultor guía la configuración inicial y actúa como punto de contacto para alinear procesos internos.
- **Programas de capacitación y webinars periódicos**: Diseño de flujos y programas de capacitación.

4. **Fuentes de Ingresos**

Aunque la herramienta no genera ingresos directos externos por sí misma, optimiza la eficiencia interna y reduce el costo de oportunidad en el área de preventa de Controles Empresariales. Esto se traduce en:

- **Mayor tasa de cierre de contratos de servicios de ciberseguridad**, gracias a propuestas más rápidas y precisas.
- **Reducción de costos operativos internos**, al disminuir las horas dedicadas a tareas manuales de compilación y seguimiento.
- **Incremento en la satisfacción del cliente**, que suele generar renovaciones y expansión de servicios, traduciéndose en ingresos recurrentes para la organización.

En consecuencia, el modelo se apoya en la eficiencia y calidad para captar más oportunidades de negocio y aumentar la facturación de productos y/o servicios, sin necesidad de crecer proporcionalmente en personal.

5. **Recursos y Actividades Clave**

Los recursos fundamentales comprenden:

- **Infraestructura en Azure**: Azure SQL Database para almacenamiento centralizado de cotizaciones y plantillas, Azure Blob Storage para repositorios de documentos, Azure Active Directory para gestión de identidades y Azure OpenAI Service para recomendaciones automáticas.
- **Licencias de Power Automate y Power BI**: Permiten la automatización de flujos y la creación de dashboards interactivos.
- **Recurso interno especializado**: Ingenieros Cloud/Dev los cuales estarán en el desarrollo, integración y mantenimiento de flujos y dashboards. Ingenieros de seguridad/QA y Project Manager.

6. **Socios Clave**

Los socios estratégicos incluyen:

- **Equipos de Infraestructura**: Responsables de ceder entornos seguros en Azure y garantizar el cumplimiento de lineamientos corporativos de seguridad y costos.
- **Partners de Microsoft y consultoras especializadas**: Proveen soporte en licenciamiento y capacitación oficial en Azure.

Estas colaboraciones aseguran que la solución esté alineada con las mejores prácticas tecnológicas y con los requerimientos operativos.

7. Estructura de Costos

La inversión se divide en:

- **Infraestructura en la nube**: Consumo de Azure SQL Database (horas CPU y almacenamiento), Azure Blob Storage (GB almacenados) y Azure OpenAI Service (tokens), así como licencias de Power Automate y Power BI.
- **Recurso interno especializado**: Horas de ingenieros Cloud/Dev, ingenieros de seguridad/QA y Project Manager para desarrollo, pruebas y capacitación.
- **Gastos operativos de soporte y monitoreo**: Seguimiento de desempeños y atención de tickets de soporte.
- **Actualización de contenidos de capacitación**: Diseño y generación de manuales, videos y materiales didácticos.

5. PROPUESTA DE LA SOLUCIÓN TECNOLÓGICA

La propuesta presentada está diseñada sobre la infraestructura de Microsoft Azure, optimizando la gestión de los 10 ingenieros preventas de ciberseguridad de Controles Empresariales, así como el procesamiento de datos, la automatización de flujos de trabajo y la implementación de inteligencia artificial para mejorar la eficiencia operativa y la toma de decisiones. Esta solución permite conectar múltiples servicios en la nube de manera cohesionada, garantizando un entorno confiable y flexible para las organizaciones.

El diseño arquitectónico está centrado en Microsoft Dynamics 365 como plataforma de gestión de clientes (CRM), integrando Azure SQL Database para el almacenamiento estructurado de datos y Azure Blob Storage para documentos y archivos no estructurados. La automatización de procesos se logra mediante Power Automate y Azure Logic Apps, permitiendo la reducción de tareas manuales y la optimización de los flujos de trabajo empresariales.

Para el análisis de datos y generación de reportes, Power BI permite visualizar información clave, facilitando una toma de decisiones basada en datos en tiempo real. Adicionalmente, Azure Data Factory desempeña un papel crucial en la extracción, transformación y carga de datos (ETL), asegurando la integración de diversas fuentes de información dentro de la solución. La inteligencia artificial se introduce con Azure OpenAI Service, agregando capacidades avanzadas de procesamiento de lenguaje natural y automatización cognitiva.

La seguridad y el cumplimiento normativo son pilares fundamentales en la arquitectura propuesta. Azure Active Directory (Azure AD) gestiona identidades y accesos, garantizando que solo usuarios autorizados interactúen con los sistemas. Complementariamente, Azure Security Center ofrece monitoreo y protección contra

amenazas en tiempo real, asegurando la integridad de los datos y la continuidad del negocio.

El uso de Microsoft Azure responde a la necesidad de una infraestructura escalable, altamente disponible y con integración nativa entre sus servicios. Azure SQL Database y Blob Storage ofrecen almacenamiento seguro y accesible, mientras que Power Automate y Logic Apps permiten reducir la carga operativa con flujos automatizados. La incorporación de Power BI fortalece el análisis de datos y la generación de reportes dinámicos, impulsando la inteligencia empresarial.

Asimismo, Azure OpenAI Service introduce modelos de IA avanzados para mejorar la interacción con clientes y la automatización de procesos. Además, esta solución aprovecha que Controles Empresariales ya cuentan con una arquitectura en Azure, lo que facilita la interoperabilidad, el cumplimiento normativo y la integración eficiente con los sistemas existentes. Actualmente, la solución está diseñada para atender a 20 usuarios, pero su arquitectura escalable permite ampliar su capacidad conforme a las necesidades del negocio sin afectar el rendimiento ni la seguridad.

La solución se caracteriza por su alta disponibilidad, escalabilidad y automatización extensiva, permitiendo una operación eficiente y segura. Su integración nativa con servicios en la nube garantiza interoperabilidad y flexibilidad para adaptarse a las necesidades del negocio. Sin embargo, al tratarse de una solución en la nube, depende de una conectividad estable a internet y requiere una adecuada planificación de costos operativos para optimizar la inversión. Además, su implementación demanda capacitación y gestión del cambio organizacional para una adopción efectiva.

La arquitectura propuesta ofrece una solución robusta y escalable para la gestión de clientes, la automatización de procesos y el análisis de datos, garantizando seguridad y eficiencia operativa. Su diseño modular y flexible permite a las

organizaciones adaptarse rápidamente a los cambios del entorno digital, mejorando la productividad y optimizando la toma de decisiones. A continuación, se presenta la representación gráfica de la solución.

A continuación, en la **¡Error! No se encuentra el origen de la referencia.** se presentará la Arquitectura propuesta de la solución técnica, donde se detallará la estructura de los componentes implementados, su interconexión y el flujo de datos dentro del ecosistema digital. Esta representación permitirá visualizar cómo los diferentes servicios y tecnologías trabajan en conjunto para ofrecer una solución eficiente y escalable.

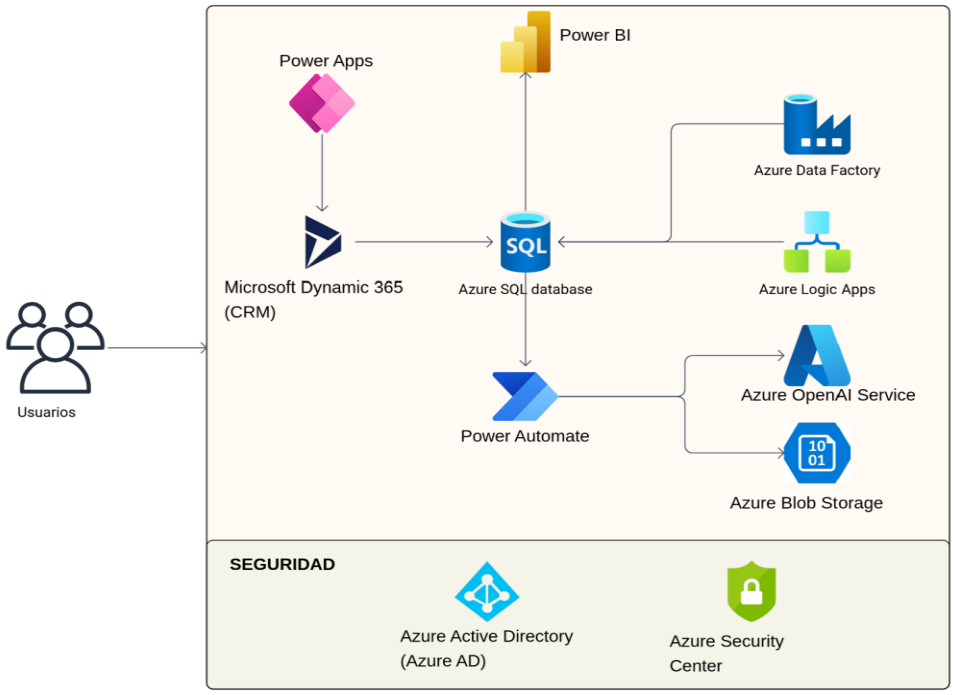

Figura 5 Arquitectura propuesta solución técnica - Fuente propia.

Asimismo, el diagrama UML presentado en la Figura 6 ilustra el flujo de trabajo en la gestión de propuestas dentro del ecosistema de Microsoft Azure según la arquitectura propuesta anteriormente, destacando la interacción entre actores y diversas tecnologías de la plataforma.

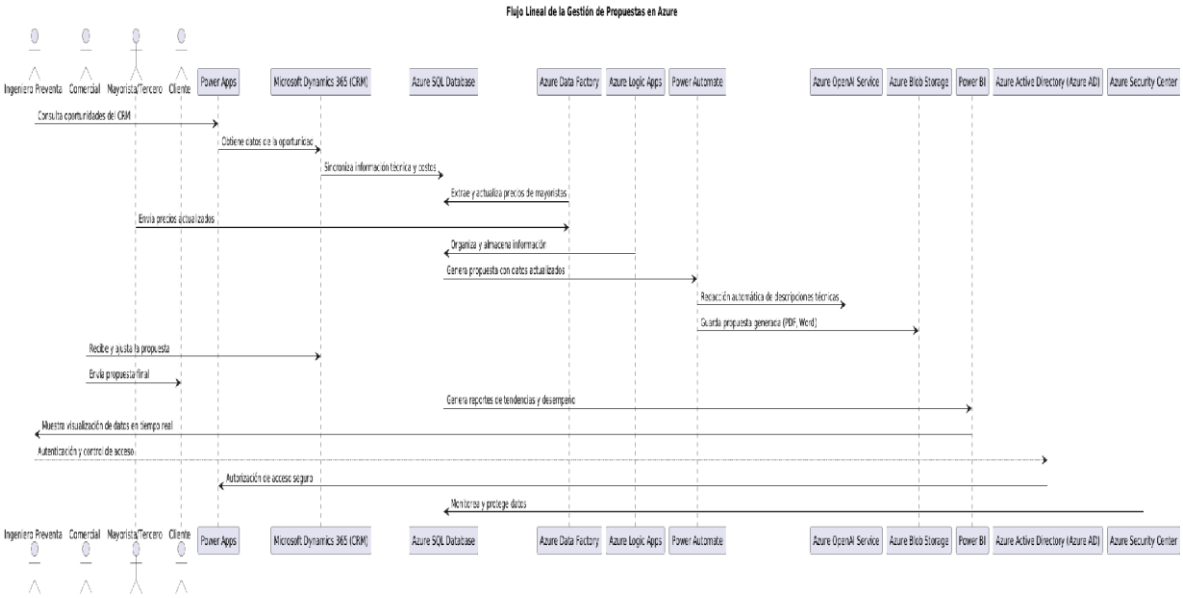

Figura 6 Diagrama propuesta solución técnica - Fuente propia

Para llevar a cabo la implementación de forma integral y coordinada, se definen los siguientes perfiles profesionales, cada uno asumiendo tareas específicas en las distintas etapas del proyecto:

1. **Ingeniero Cloud & Desarrollador Fullstack**

- **Responsabilidades principales:**

  - Levantamiento y análisis detallado de requisitos técnicos y funcionales.
  - Diseño de la arquitectura lógica en Azure: modelamiento de datos, definición de servicios y componentes.
  - Aprovisionamiento y configuración de recursos en Azure (Azure SQL Database, Azure Blob Storage, Azure Active Directory, App Services).
  - Implementación y desarrollo de flujos automatizados en Power Automate / Logic Apps para la recolección de datos y aprobación de cotizaciones.

- Creación y publicación de dashboards en Power BI: elaboración de consultas DAX y definición de visualizaciones.
- Integración del servicio Azure OpenAI: configuración de endpoints seguros, definición de prompts y despliegue de soluciones de IA.

2. Ingeniero de Seguridad & QA (Quality Assurance)

- **Responsabilidades principales:**

  - Definición de políticas de seguridad en Azure: control de accesos, roles, encriptación en reposo y en tránsito.
  - Configuración de Azure Security Center y establecimiento de alertas críticas.
  - Revisión y validación de los flujos de Power Automate y los informes de Power BI, garantizando niveles adecuados de confidencialidad e integridad de la información.
  - Ejecución de pruebas funcionales, de rendimiento y pruebas de penetración básica sobre los componentes desplegados.
  - Documentación de hallazgos y coordinación de las correcciones necesarias para subsanar vulnerabilidades o inconsistencias.

3. Project Manager & Coordinador de Capacitación

- **Responsabilidades principales:**

  - Elaboración y seguimiento del cronograma de actividades, asegurando el cumplimiento de plazos y la correcta secuencia de tareas.
  - Gestión de reuniones, recolección de requerimientos y validación de entregables parciales.

- Elaboración de la documentación oficial: actas de levantamiento de requisitos, bitácoras de decisiones y checklist de entregables en cada fase.
- Planificación y organización de las sesiones de capacitación a usuarios finales (Ingenieros Preventa), preparando materiales didácticos y guías de uso.
- Coordinación con los equipos de seguridad y desarrollo para la aprobación de cambios y supervisión de la puesta en producción.

El cronograma propuesto a continuación, contempla un total de 12 semanas. Cada fase incorpora la cobertura de tareas de infraestructura, desarrollo, seguridad, aseguramiento de calidad y gestión de proyecto.

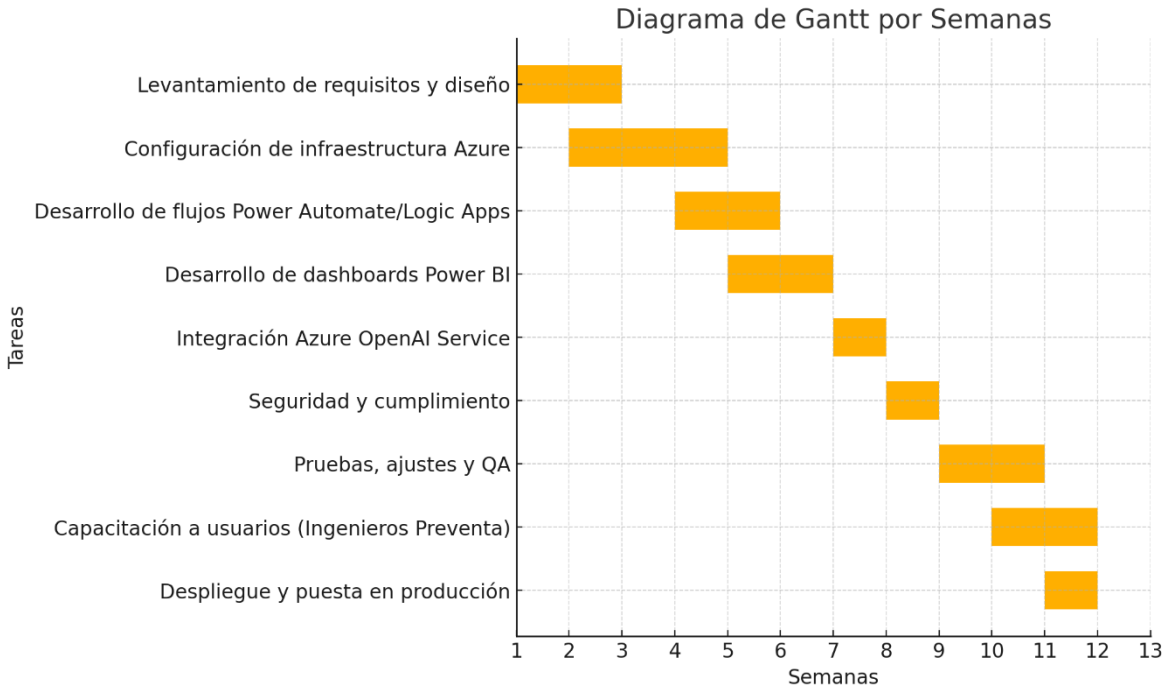

Figura 7 Diagrama de Gantt

A continuación, se establece la relación del desarrollo de la propuesta de la solución tecnológica la cual se divide de la siguiente manera según la **¡Error! No se encuentra el origen de la referencia.**:

Semana 1. En la primera semana se ejecuta íntegramente la fase de levantamiento de requisitos y diseño detallado. El equipo realiza entrevistas, se consolida requerimientos funcionales y no funcionales, define el modelo lógico de datos y esquematiza la arquitectura en Azure. Además, se establecen criterios iniciales de seguridad, como niveles de cifrado y roles de acceso, y se documenta el alcance técnico en un acta de diseño.

Semana 2. Durante la segunda semana se completa la fase de levantamiento y se inicia simultáneamente la configuración de infraestructura en Azure. Los primeros tres días se destinan a finalizar entrevistas y ajustar el documento de diseño según la retroalimentación recibida, garantizando que todos los componentes (Azure SQL Database, Blob Storage, Azure AD) estén correctamente especificados. A partir del cuarto día, se comienza el aprovisionamiento de recursos en Azure: creación de la base de datos, configuración de almacenamiento y establecimiento de los primeros pipelines en Azure.

Semana 3. En la tercera semana continúa la configuración de infraestructura Azure de manera intensiva. Se diseñan los esquemas físicos de la base de datos, se asignan roles y permisos en Azure AD, se implementan políticas de seguridad en Azure Security Center y se validan las conexiones entre los servicios. Paralelamente, se ajustan los pipelines de compilación y despliegue para garantizar que el código pueda trasladarse a los diferentes entornos (desarrollo y pruebas) de forma automatizada.

Semana 4. A lo largo de la cuarta semana se concluye la infraestructura y se arranca la construcción de flujos en Power Automate. En los primeros tres días se realizan pruebas finales de conectividad y se afinan parámetros de seguridad en los recursos de Azure. Inmediatamente después, se inicia la definición de la lógica de negocio para los flujos: diseño de triggers, acciones de recolección de datos y rutas de aprobación, así como la validación de cifrado en variables sensibles.

Semana 5. La quinta semana se dedica a finalizar el desarrollo de los flujos automatizados en Power Automate y al inicio de la construcción de dashboards en Power BI. Durante los primeros cuatro días se comprenden las interdependencias entre formularios, bases de datos y notificaciones, se implementan flujos de aprobación de cotizaciones y se ejecutan pruebas unitarias. En el último día de esta semana se establece la conexión inicial desde Power BI a Azure SQL Database y se realiza la configuración básica del modelo de datos.

Semana 6. En la sexta semana se finaliza el desarrollo de dashboards en Power BI. Se completan las consultas DAX necesarias para los indicadores clave como tasa de aprobación, tiempos promedio de respuesta, errores frecuentes y se diseñan visualizaciones interactivas. Además, se configuran los filtros y segmentaciones según roles de usuario y se validan la integridad y consistencia de los datos con muestras reales, dejando publicados los primeros informes en el servicio de Power BI.

Semana 7. Durante la séptima semana se implementa la fase de integración de Azure OpenAI Service. Se aprovisiona el recurso en Azure y se configura el endpoint con las medidas de seguridad correspondientes. Se definen los prompts que generarán recomendaciones automáticas (resúmenes de cotizaciones, alertas de anomalías) y se prueban las llamadas al servicio desde Power Automate o Logic Apps, verificando la coherencia semántica y la protección de datos sensibles.

Semana 8. La octava semana se dedica a la revisión exhaustiva de controles de seguridad y al cumplimiento normativo. Se ejecutan escaneos de vulnerabilidades internas mediante Azure Security Center y herramientas complementarias, se realizan pruebas de penetración ligera contra los endpoints de Power Automate y Azure OpenAI, y se revisan roles y permisos en Azure AD y Power BI. Los hallazgos se documentan, se aplican las correcciones necesarias y se actualiza la documentación de políticas y alertas.

Semana 9. En la novena semana comienza la fase de pruebas, ajustes y aseguramiento de calidad (QA). El equipo diseña y ejecuta casos de prueba funcionales para cada componente: validación de la ejecución correcta de flujos en Power Automate, verificación de la precisión de datos en Power BI y comprobación de la generación de contenido con Azure OpenAI. También se realizan pruebas de rendimiento para evaluar tiempos de respuesta y latencia en el sistema.

Semana 10. La décima semana se completa la fase de pruebas y ajustes, a la vez que arranca el proceso de capacitación a usuarios. Durante los primeros tres días se documentan y priorizan los hallazgos de QA, se implementan correcciones en consultas DAX, flujos y prompts de IA, y se validan los resultados finales. En los últimos dos días de la semana se inician las sesiones de formación para los Ingenieros Preventa: introducción a Power BI, uso de Power Automate para generación de cotizaciones y buenas prácticas de seguridad.

Semana 11. En la undécima semana se finaliza la capacitación de los Ingenieros Preventa y se lleva a cabo el despliegue y puesta en producción. El primer día se concluye la formación con ejercicios prácticos y retroalimentación final. A continuación, se ejecuta el pipeline de despliegue en Azure para migrar datos definitivos a la instancia de producción, se verifican las conexiones de Power BI y se realizan pruebas de aceptación en vivo. Finalmente, se monitorean logs y métricas con Azure Monitor para asegurar la operación estable.

Semana 12. En la semana doce se disponen márgenes operativos para soporte inicial y posibles ajustes posteriores a la puesta en producción. Durante este período se monitorea el sistema, se atienden dudas de los usuarios y se corrigen incidencias menores que puedan surgir durante las primeras semanas de operación real, asegurando la estabilidad y la adopción completa de la solución.

6. ANÁLISIS DEL PROCESO DE TRANSFORMACIÓN DIGITAL

En el contexto actual de alta competitividad y evolución constante de las amenazas digitales, el área de preventa de ciberseguridad en Controles Empresariales enfrenta una serie de desafíos estructurales y tecnológicos que limitan su capacidad operativa y estratégica. Esta área, conformada por un equipo de diez ingenieros especializados, desempeña un papel fundamental en la construcción de propuestas técnicas alineadas con los riesgos, requerimientos y objetivos de los clientes.

Sin embargo, el modelo operativo vigente se caracteriza por la descentralización de la información, el uso intensivo de herramientas ofimáticas sin integración entre sí y la inexistencia de una metodología estructurada para la gestión del ciclo de preventa. Cada ingeniero trabaja sobre su propia base de datos, lo que impide la colaboración efectiva, promueve la duplicación de esfuerzos y genera inconsistencias en los contenidos y formatos de las propuestas.

La obtención de información crítica, como precios, condiciones técnicas y disponibilidad de productos, depende de la interacción manual con mayoristas y aliados, lo que introduce cuellos de botella y retrasa la entrega de propuestas. Asimismo, no existe trazabilidad en la gestión de oportunidades, ni indicadores automáticos de desempeño que permitan evaluar la eficacia del proceso o tomar decisiones basadas en datos.

Estas condiciones han generado impactos negativos como: baja eficiencia operativa, reducción en la tasa de conversión comercial, percepción de poca agilidad por parte del cliente, y dificultad para escalar el modelo ante el crecimiento del portafolio o la demanda.

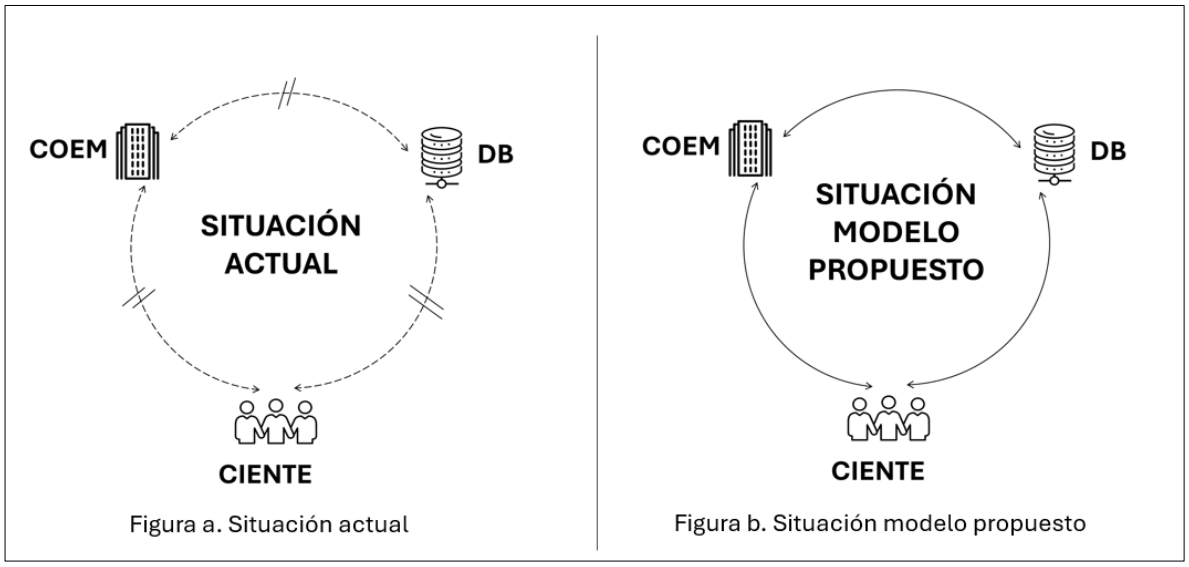

Figura 8 Situación actual COEM. Fuente propia

La Figura 8 a) evidencia la situación actual del proceso de preventa en Controles Empresariales, caracterizada por una comunicación fragmentada y procesos no integrados entre los actores principales: Controles Empresariales, la base de datos (DB) y los clientes. Las líneas segmentadas con interrupciones indican rupturas en el flujo de información, generadas por la falta de una infraestructura tecnológica que permita una interacción fluida, automatizada y trazable. La consulta de datos se realiza de manera manual y descentralizada, lo que dificulta la agilidad en la elaboración de propuestas y debilita la respuesta a las necesidades del cliente.

Además, la retroalimentación del cliente no se integra de forma sistemática al repositorio de datos, lo que impide una mejora continua. Este modelo revela ineficiencias críticas que deben ser atendidas para asegurar una mayor competitividad en el mercado de soluciones de ciberseguridad.

El proceso de preventa en su forma actual está conformado por una serie de actividades críticas (levantamiento de requerimientos, análisis técnico, solicitud de cotizaciones, elaboración de propuestas, validación y envío al cliente), las cuales se ejecutan sin automatización, sin integración sistémica y con alta intervención

humana. La inexistencia de un flujo de trabajo digitalizado impide la reutilización de componentes de propuestas anteriores, lo que reduce la eficiencia y aumenta los márgenes de error.

La cultura de trabajo se ha centrado en la especialización técnica individual, lo que ha generado una alta dependencia del conocimiento tácito de cada ingeniero. Aún no se ha consolidado una cultura digital que promueva la colaboración interdisciplinaria, el uso intensivo de herramientas tecnológicas o la gestión del conocimiento organizacional como activos estratégicos. La resistencia al cambio, en parte derivada de la falta de capacitación continua en herramientas digitales, también ha sido un factor limitante.

El perfil de cliente que atiende Controles Empresariales se caracteriza por requerimientos complejos, sensibilidad al cumplimiento de normativas de seguridad (ISO/IEC 27001, NIST, GDPR) y expectativa de propuestas rápidas, diferenciadas y basadas en valor. La demora en la respuesta, la falta de personalización y la escasa visibilidad del estado de las propuestas disminuyen la percepción de profesionalismo y confianza en la solución ofertada.

A pesar de contar con una infraestructura tecnológica basada en Microsoft Azure, y con profesionales técnicamente competentes, la empresa no ha explotado el potencial de automatización, inteligencia artificial ni analítica avanzada en los procesos de preventa. La innovación ha estado centrada en el producto y servicios de soluciones de ciberseguridad, pero no en los procesos internos ni en la experiencia del cliente.

Para revertir los problemas identificados y responder a las exigencias del mercado, se propone un modelo de transformación digital integral para el área de preventa. Este diseño se fundamenta en tres pilares: automatización, centralización y analítica.

1. ***Automatización de procesos***

   La implementación de flujos de trabajo automatizados mediante Power Automate y Azure Logic Apps permitirá reducir tareas manuales, eliminar cuellos de botella y estandarizar actividades repetitivas como generación de propuestas, recolección de datos de mayoristas y seguimiento a oportunidades.

2. ***Centralización de información***

   La creación de una base de datos unificada en Azure SQL Database y Azure Blob Storage garantizará el acceso centralizado y seguro a información técnica, precios actualizados, catálogos de productos, plantillas de propuestas y normativas vigentes.

3. ***Analítica y toma de decisiones***

   Mediante Power BI, el equipo de preventa podrá acceder a paneles de control interactivos que muestren indicadores clave (KPI) como tiempo promedio de elaboración de propuestas, tasa de cierre, razones de pérdida y carga de trabajo por ingeniero.

4. ***Inteligencia artificial aplicada***

   Con la integración de Azure OpenAI Service, se podrán automatizar partes del contenido técnico de las propuestas, ajustar el lenguaje de acuerdo con el perfil del cliente y sugerir configuraciones recomendadas con base en propuestas históricas y patrones de éxito.

En el modelo propuesto en la Figura 9, se evidencia el diagrama de flujo deseado donde cada oportunidad registrada en el CRM de Controles Empresariales se

asigna automáticamente al ingeniero disponible según criterios de carga laboral y especialización. El ingeniero accede a una base de datos técnica y comercial centralizada, que permite iniciar el análisis de la solicitud sin depender de terceros. Si se requiere contacto con el cliente, el sistema genera una agenda automática e integra un formulario digital para registrar los requerimientos.

Posteriormente, se genera una propuesta técnica personalizada mediante inteligencia artificial, reutilizando contenidos validados y cumpliendo con normativas específicas del cliente. Todo el flujo se gestiona de manera digital, incluyendo la validación técnica, la entrega de la propuesta y el análisis del resultado a través de tableros Power BI. Esta transformación reduce drásticamente los tiempos de entrega, incrementa la calidad de la propuesta y mejora la experiencia del cliente, alineándose con estándares internacionales de eficiencia y seguridad.

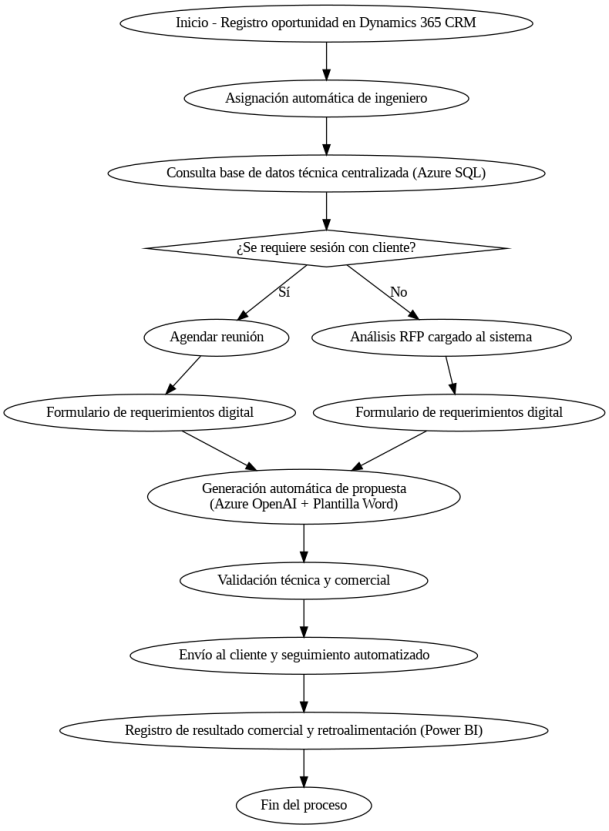

Figura 9 Diagrama TO BE

En el modelo propuesto de la Figura 8 b) se presenta una visión circular e interconectada del proceso de preventa en ciberseguridad, centrado en la mejora continua y la eficiencia operativa. En el centro del diagrama se encuentra la situación del modelo propuesto, que articula la relación dinámica entre tres actores clave: COEM (Controles Empresariales) como entidad responsable de diseñar e implementar soluciones, la base de datos (DB) como repositorio centralizado de información técnica y comercial, y el cliente, como receptor de propuestas adaptadas a sus necesidades. Este flujo cíclico simboliza la integración de procesos digitales: COEM consulta y actualiza información en la base de datos para construir propuestas, las cuales se entregan al cliente de forma personalizada; posteriormente, la retroalimentación del cliente nutre nuevamente la base de datos, generando un ciclo de mejora continua que fortalece la capacidad de respuesta y la competitividad organizacional.

7. ASPECTOS LEGALES Y CONTRATACIÓN

En la situación actual del área de preventa de ciberseguridad en Controles Empresariales, se identifican deficiencias significativas en el manejo y tratamiento de la información. La dispersión de datos y la ausencia de una base centralizada incrementan el riesgo de incumplimiento normativo en materia de protección de datos personales, tal como lo establece la Ley 1581 de 2012, reglamentada por el Decreto 1377 de 2013. Esta normativa establece el marco legal para el tratamiento de datos personales en Colombia, exigiendo a los responsables y encargados del tratamiento la implementación de medidas técnicas, humanas y administrativas que garanticen la confidencialidad, integridad, disponibilidad y seguridad de la información.

La Superintendencia de Industria y Comercio (SIC), como autoridad de control, ha emitido múltiples directrices que refuerzan estos principios, incluyendo el cumplimiento de los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. En particular, el principio de circulación restringida prohíbe compartir datos personales con terceros no autorizados sin el consentimiento del titular, lo cual cobra especial relevancia en los procesos de preventa que involucran datos de clientes, aliados estratégicos y proveedores.

El manejo manual y descentralizado de información sensible —incluyendo datos de contacto, perfiles técnicos y requerimientos específicos— genera múltiples riesgos: accesos no autorizados, pérdida de trazabilidad y tratamientos sin consentimiento explícito. Estas prácticas conllevan la posibilidad de que la SIC determine que se está incumpliendo no solo la Ley 1581 de 2012, sino también los lineamientos técnicos mínimos establecidos en la Guía de Responsabilidad Demostrada publicada por la entidad, donde se exige documentar el ciclo de vida del tratamiento

de datos y establecer políticas claras, accesibles y actualizadas de seguridad de la información.

En el contexto de contratación con mayoristas y otros aliados estratégicos, la carencia de cláusulas contractuales de protección de datos y de mecanismos que aseguren la corresponsabilidad en el tratamiento, como lo establece el Artículo 18 de la Ley 1581, representa una vulnerabilidad crítica. Esta norma obliga a los responsables del tratamiento a garantizar que los terceros que accedan a los datos personales también cumplan con la legislación, lo cual debe formalizarse a través de acuerdos de transmisión y anexos de tratamiento de datos personales (DPA). La falta de estos elementos puede derivar en sanciones que van desde multas hasta la suspensión de las actividades de tratamiento.

La nueva solución tecnológica, basada en la centralización de la gestión de la información y la automatización de los procesos de preventa mediante herramientas de Azure y Power Platform, está alineada con los requisitos legales y contractuales descritos. Al centralizar la base de datos de clientes y proveedores en Azure SQL Database, se garantiza la trazabilidad de los registros y el cumplimiento de los principios de confidencialidad e integridad. El uso de Azure Active Directory para el control de accesos cumple con las exigencias de la SIC en cuanto a autenticación, autorización y protección contra accesos no autorizados, asegurando que solo personal autorizado interactúe con datos sensibles. Además, la generación automática de reportes en Power BI permite registrar y auditar en tiempo real cualquier modificación, facilitando la demostración de cumplimiento normativo durante auditorías externas.

En materia contractual, la integración con Microsoft 365 permite incluir de manera sistemática cláusulas de protección de datos, acuerdos de transmisión, definiciones de responsables y encargados del tratamiento, y acuerdos de nivel de servicio (SLAs) en los contratos con proveedores. Esto asegura que cada aliado estratégico

cumpla con las obligaciones establecidas por la Ley 1581 de 2012, el Decreto 1377 de 2013, y los lineamientos de la Superintendencia de Industria y Comercio, consolidando un marco de gobernanza de la información que mitigue riesgos legales y reputacionales asociados al tratamiento de datos personales.

8. CONCLUSIONES

La ideación y el análisis de las alternativas técnicas demostraron que la adopción del ecosistema Microsoft (Azure y Power Platform) era la opción más adecuada, tanto por su capacidad de integración nativa con los procesos existentes como por la sólida experiencia de la organización como Partner de Microsoft. La automatización de flujos de trabajo mediante Power Automate y Logic Apps, la centralización de la información en Azure SQL Database y la capa analítica de Power BI aseguran la confiabilidad, la disponibilidad y la rapidez en la elaboración de propuestas. Además, el uso de Azure OpenAI Service para la generación inteligente de contenido refuerza la rapidez en la respuesta al mercado y la personalización de las cotizaciones.

La propuesta tecnológica contempla una implementación gradual y segura: un cronograma de doce semanas permitió levantar requisitos, configurar la infraestructura, desarrollar flujos, construir dashboards, evaluar pruebas de seguridad y capacitar al personal. Esto aseguró que, desde la fase inicial, se aplicaran prácticas de “security by design”, con controles de acceso vía Azure Active Directory, cifrado de datos en reposo y en tránsito, y auditorías continuas. De este modo, se redujeron riesgos de exposiciones no autorizadas y se cumplió con los estándares de calidad y seguridad requeridos por la organización.

El modelo de negocio para la solución dirigida al área de preventa de Controles Empresariales se fundamenta en la eficiencia operativa y la inteligencia artificial para elevar la calidad de las propuestas de ciberseguridad. Al automatizar flujos de trabajo, consolidar métricas en dashboards interactivos y ofrecer recomendaciones proactivas, la plataforma aporta un valor diferencial que impacta positivamente la productividad del equipo y la satisfacción de los clientes externos. La combinación de licenciamiento de Power Platform, infraestructura segura en Azure y talento interno especializado crea un ecosistema sostenible y escalable. En última

instancia, esta solución fortalece la posición competitiva de Controles Empresariales al permitir ofrecer propuestas más rápidas, precisas y alineadas con normativas de seguridad, lo que se traduce en mayores oportunidades de negocio y un crecimiento rentable para la organización.

Referencias

[1] Kaspersky, “Las empresas aumentarán hasta un 9% su presupuesto de seguridad informática,” 2025. [Online]. Available: https://latam.kaspersky.com/about/press-releases/las-empresas-aumentaran-hasta-un-9-su-presupuesto-de-seguridad-informatica-kaspersky

[2] Gartner, “Transformación Digital: Claves y Tendencias,” 2025. [Online]. Available: https://www.gartner.es/es/tecnologia-de-la-informacion/temas/transformacion-digital

[3] G. Brown, “The Impact of CPQ Systems on Cybersecurity Sales,” *Journal of Information Security*, vol. 12, no. 3, pp. 45–60, 2023.

[4] Ikusi, “Automatización de ciberseguridad: ¿Cómo realizarla eficientemente?,” 2025. [Online]. Available: https://www.ikusi.com/mx/blog/automatizacion-de-ciberseguridad-como-realizar-eficientemente/

[5] J. Smith, “Collaborative Frameworks for Pre-Sales Security Engineering,” *Cybersecurity Management Review*, vol. 10, no. 2, pp. 89–105, 2022.

[6] R. Thompson and L. White, “Agile Methodologies in Cybersecurity Pre-Sales: Enhancing Proposal Development Efficiency,” *International Journal of Secure IT Practices*, vol. 8, no. 4, pp. 150–167, 2023.