Fecha de elaboración

0	7	1	0	2	0	2	5

1. INFORMACIÓN GENERAL DEL PROYECTO DE TI

Nombre del Servicio/ solución tecnológica/ proyecto:	Desarrollo e Implementación de la Plataforma de Servicios Gestionados de Ciberseguridad "FortaGuard" para PyMEs.	**Clave:**	ID-FD-2025-001
Fecha Propuesta de Inicio:	**29-agosto-2025**	**Fecha de Fin Propuesta:**	**07-enero-2026**
Nombre del Administrador del Proyecto	Cristopher Pérez Marcelo		

2. ANTECEDENTES

El entorno digital en México se ha transformado en un sector vulnerable aún más para las Pequeñas y Medianas Empresas (PyMEs), estas constituyen el 98.7% del tejido empresarial y generan el 52% del Producto Interno Bruto (PIB) de México. Los ciberdelincuentes las consideran objetivos de bajo riesgo y alta recompensa, aprovechando sus limitados recursos y defensas a menudo rudimentarias, la brecha de preparación es abismal: a nivel nacional, apenas un 2% de las organizaciones ha alcanzado un nivel "maduro" de ciberseguridad. La situación en las PyMEs es aún más precaria, con menos del 28% contando con políticas de seguridad activas, menos del 23% habiendo designado formalmente a un responsable del área, y solo un alarmante 13.6% capacitando a su personal de forma regular. Para muchas, la principal y única línea de defensa sigue siendo un simple antivirus, una herramienta anacrónica frente a las amenazas sofisticadas de hoy.

El factor humano se confirma como el principal vector de riesgo, ya que el error humano es una de las principales puertas de entrada a las redes corporativas, una vulnerabilidad explotada sistemáticamente mediante técnicas de ingeniería social como el **phishing**. La falta de una cultura de ciberseguridad es palpable, con estudios que revelan que el 70% de los usuarios mexicanos no es capaz de reconocer un intento de suplantación de identidad, esta debilidad se ve magnificada por la consolidación del trabajo remoto, un modelo en el que el 83% de las empresas permite a sus empleados conectarse desde dispositivos personales no gestionados, expandiendo masivamente la superficie de ataque y creando puntos ciegos para la seguridad.

La situación actual de las PyMEs mexicanas es el resultado de una convergencia de factores que crea un ciclo de vulnerabilidad difícil de romper, por un lado, carecen de los recursos financieros para invertir en tecnologías de seguridad avanzadas, por otro lado, la severa escasez de talento especializado (con una brecha estimada de 1.3 millones de profesionales en América Latina y un déficit de 400,000 en México) ha disparado los salarios de los expertos, poniéndolos fuera del alcance de una PyME. Sin expertos internos, estas empresas no pueden gestionar

herramientas complejas y se ven forzadas a depender de defensas inadecuadas, esto las convierte en el blanco perfecto para ataques automatizados y de bajo costo para los criminales, al ser víctimas de un ataque exitoso, sufren pérdidas financieras que merman aún más su capacidad de invertir en seguridad, perpetuando así el ciclo. Siendo así, este proyecto busca romper el círculo de vulnerabilidad de las PyMEs frente a la crisis de ciberseguridad en México, democratizando el acceso a la tecnología y la experiencia necesarias para garantizar su supervivencia y competitividad en la economía nacional.

3. JUSTIFICACIÓN TÉCNICA DEL PROYECTO

El proyecto "FortaGuard" se justifica técnicamente como una solución integral, gestionada y proactiva, diseñada desde su concepción para abordar las amenazas específicas y las limitaciones operativas que enfrentan las PyMEs mexicanas. La propuesta no consiste en revender productos aislados, sino en construir una plataforma unificada que materialice los valores de Simplicidad y Proactividad de FortaDigital, traduciendo la complejidad de la ciberseguridad en tranquilidad y valor de negocio para el cliente.

4. ALCANCE

El proyecto contempla el desarrollo integral de una plataforma en la nube con arquitectura de microservicios, APIs seguras y base de datos multi-tenant, junto con la creación de un portal web para clientes con visualización de datos en tiempo real y un portal de administración para el equipo interno de FortaDigital. Incluye la integración de tecnologías de terceros mediante API para funcionalidades de EDR y escaneo de vulnerabilidades, así como el desarrollo de un motor propio de simulación de phishing y una biblioteca inicial de contenidos de capacitación en español adaptados al contexto empresarial mexicano. Además, se desarrollará y probará un agente ligero compatible con Windows y macOS, se definirán e implementarán los procesos operativos estándar (SOPs) del equipo SOC con sus respectivos manuales de respuesta a incidentes, y se llevará a cabo un programa piloto con hasta 10 clientes para validar, ajustar y optimizar el servicio.

5. OBJETIVO

Desarrollar y lanzar el Producto Mínimo Viable (MVP) de la plataforma "FortaGuard" en un plazo de 12 meses y dentro del presupuesto asignado, con el fin de validar la solución en el mercado de las PyMEs mexicanas y alcanzar los objetivos iniciales de adquisición de clientes e ingresos que aseguren la viabilidad del negocio.

6. RIESGOS CLAVE

Descripción del Riesgo	*Impacto*	*Probabilidad*
Retrasos en el desarrollo debido a la escasez de talento especializado en ciberseguridad y desarrollo cloud. La alta demanda y la brecha de talento en México podrían dificultar la contratación y retención del personal necesario, afectando el cronograma.		
Adopción del mercado más lenta de lo previsto. A pesar del riesgo evidente, las PyMEs pueden mostrarse reacias a invertir en un nuevo servicio debido a restricciones presupuestarias o una percepción de que "no les pasará a ellas".		
Dependencia crítica de proveedores de tecnología de terceros (e.g., motor EDR). Un aumento súbito de precios, cambios disruptivos en las APIs, o la quiebra del proveedor podrían degradar o interrumpir el servicio de FortaGuard.		
Complejidad técnica subestimada en la integración de componentes. La interconexión del agente de endpoint, el backend en la nube, las bases de datos y las herramientas de terceros puede presentar desafíos técnicos imprevistos que generen retrasos.		
Ataque cibernético exitoso contra la propia plataforma FortaGuard. Un incidente de seguridad en la infraestructura de FortaDigital tendría un impacto devastador e irreparable en la reputación de la empresa y la confianza de los clientes		

7. DEFINICIÓN DE INDICADORES

Nombre del indicador	Tipo	Fórmula

8. BENEFICIOS ESPERADOS

Beneficios Cuantitativos:
El proyecto generará para FortaDigital un flujo de ingresos recurrente y escalable estimado en $4.5 millones de pesos anuales al alcanzar 50 clientes, fortaleciendo su posición como líder innovador en ciberseguridad para PyMEs en México y aprovechando un mercado con alto potencial de crecimiento. Para las PyMEs clientes, el impacto económico será significativo, con una reducción de hasta 95% en el riesgo financiero asociado a ciberataques (evitando pérdidas potenciales de hasta 2 millones de pesos por incidente) y un ahorro superior al 80% frente al costo de mantener un equipo interno de ciberseguridad.

Beneficios Cualitativos:
El lanzamiento de *FortaGuard* consolidará la misión y visión de FortaDigital al ofrecer ciberseguridad accesible y confiable, fortaleciendo su marca como referente de confianza y alianza con las PyMEs. Para los clientes, el servicio aportará tranquilidad y continuidad operativa al mitigar el temor de interrupciones por ciberataques, brindará una ventaja competitiva mediante reportes que demuestran una postura de seguridad sólida frente a socios comerciales, y democratizará el acceso a conocimientos y tecnologías de protección de nivel empresarial, permitiendo a las PyMEs competir en igualdad de condiciones en el entorno digital.

9. PLANEACIÓN ALTO NIVEL

9.1 Cronograma Alto Nivel

Insertar Cronograma de Project Professional

**VER CRONOGRAMA*

9.2 Dependencia con Otros Proyectos

¿Existe dependencia con otros Proyectos?	NO	Describa con cuáles:	N/A

9.3 Personal Involucrado

Perfil	Número	Tipo de Contratación
Project Manager	1	Tiempo Completo
Ingeniero de Ciberseguridad	1	Tiempo Completo
Desarrollador Full-Stack	1	Tiempo Completo
Diseñador UI/UX	1	Tiempo Completo

10. JUSTIFICACIÓN ECONÓMICA DEL PROYECTO DE TI

10.1 Estudio de Mercado

N/A

10.2 Costos de Mantenimiento

N/A

10.3 Costos de Operación

N/A

10.4 Procedimiento de Adquisición

N/A

11. GLOSARIO TÉCNICO

Concepto	*Descripción*
DevSecOps	Es una filosofía y práctica de desarrollo de software que integra la seguridad en cada fase del ciclo de vida del desarrollo (desde la planificación hasta el despliegue y mantenimiento). En lugar de tratar la seguridad como una etapa final, se convierte en una responsabilidad compartida por desarrolladores, operaciones y personal de seguridad, automatizando las pruebas de seguridad para agilizar la entrega de software seguro.
Endpoint Detection and Response (EDR)	Tecnología de ciberseguridad que va más allá del antivirus tradicional. Monitorea de forma continua los dispositivos finales (endpoints) como laptops y servidores, registrando toda la actividad para identificar patrones de comportamiento sospechosos. Permite a los analistas de seguridad detectar, investigar y responder a amenazas avanzadas que evaden las defensas convencionales, como el ransomware o los ataques sin archivos (fileless).
Ingeniería Social	Conjunto de técnicas de manipulación psicológica utilizadas por los ciberdelincuentes para engañar a las personas y hacer que realicen acciones específicas o divulguen información confidencial. No se basa en explotar vulnerabilidades técnicas, sino en la confianza, el miedo o la curiosidad humana. El phishing es la forma más común de ingeniería social.
Malware	Abreviatura de "software malicioso". Es un término general que engloba cualquier tipo de software diseñado para dañar, interrumpir o obtener acceso no autorizado a sistemas informáticos. Incluye virus, gusanos, troyanos, spyware, adware y ransomware.
Multi-tenancy (Arquitectura Multi-inquilino)	Abreviatura de "software malicioso". Es un término general que engloba cualquier tipo de software diseñado para dañar, interrumpir o obtener acceso no autorizado a sistemas informáticos. Incluye virus, gusanos, troyanos, spyware, adware y ransomware.
Phishing	Es un tipo de ciberataque de ingeniería social que utiliza correos electrónicos, mensajes de texto o sitios web fraudulentos que suplantan la identidad de organizaciones o personas de confianza. El objetivo es engañar a la víctima para que revele información

	sensible, como contraseñas, números de tarjeta de crédito o credenciales de acceso, o para que descargue malware.
Producto Mínimo Viable (MVP)	Es la versión de un nuevo producto que permite a un equipo recopilar la máxima cantidad de aprendizaje validado sobre los clientes con el mínimo esfuerzo. Contiene solo las funcionalidades básicas necesarias para ser útil a un primer grupo de usuarios (early adopters) y probar una hipótesis de negocio fundamental en el mercado real.
Pruebas de Penetración (Pentesting)	Es un ciberataque simulado y autorizado contra un sistema informático, red o aplicación web para evaluar su seguridad. Los "pentesters" utilizan las mismas técnicas que los atacantes maliciosos para encontrar y explotar vulnerabilidades, con el fin de identificar los puntos débiles de la seguridad antes de que un adversario real pueda hacerlo.
Ransomware-as-a-Service (RaaS)	Un modelo de negocio delictivo en el que los desarrolladores de ransomware venden o alquilan su malware en la dark web a otros ciberdelincuentes, llamados "afiliados". Los afiliados lanzan los ataques y comparten un porcentaje de las ganancias del rescate con los desarrolladores. Este modelo ha reducido drásticamente la barrera técnica para lanzar ataques de ransomware, contribuyendo a su proliferación.
Software as a Service (SaaS)	Un modelo de licenciamiento y entrega de software en el que las aplicaciones son alojadas centralmente por un proveedor y se ponen a disposición de los clientes a través de una red, típicamente Internet, mediante un modelo de suscripción. El cliente no necesita instalar, mantener ni actualizar el software, ya que todo es gestionado por el proveedor.