INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES (2020)

ASIGNATURA: IT GOVERNACE

TARE: ANÁLISIS DE FACTIBILIDAD

INTEGRANTES:

- PÉREZ MARCELO CRISTOPHER
- SALAZAR GARCÍA ALDO EMMANUEL
- ZETINA HERNÁNDEZ ISSAC

PROFESOR: PALACIOS SOLANO ROCÍO

ESTUDIO DE FACTIBILIDAD DEL PROYECTO

Plataforma de Servicios Gestionados de Ciberseguridad “FortaGuard”
03 de diciembre de 2025

1. FACTIBILIDAD TÉCNICA

La viabilidad técnica se sustenta en una arquitectura de cuatro capas diseñada para alta disponibilidad y seguridad en profundidad, utilizando estándares de industria modernos que garantizan la escalabilidad.

1.1 Arquitectura de Infraestructura

El sistema implementa una infraestructura Cloud segmentada para garantizar el desacoplamiento de servicios y la seguridad:

- **Capa 1 - Acceso y Usuarios:** Interfaces web diferenciadas para el Cliente PyME (Usuario Web) y el Equipo SOC Interno (Admin), asegurando la segregación de funciones y control de acceso.
- **Capa 2 - Seguridad Perimetral:** Implementación de WAF (*Web Application Firewall*) y protección anti-DDoS. El enrutamiento se gestiona mediante un *API Gateway* con encriptación TLS 1.3 obligatoria para todo el tráfico.
- **Capa 3 - Microservicios:** Clúster de Kubernetes con *auto-scaling* que orquesta los servicios críticos: Simulación de Phishing, Ingesta de Agentes y el Escaneo de Vulnerabilidades.
- **Capa 4 - Datos y Almacenamiento:** Estrategia híbrida que utiliza bases de datos relacionales (SQL) para la gestión multi-tenant de clientes y bases de datos NoSQL/Time-Series para procesar la telemetría de logs a alta velocidad.

---

2. FACTIBILIDAD ECONÓMICA

El proyecto presenta indicadores financieros sólidos basados en la recurrencia de ingresos y un ahorro operativo evidente para el mercado objetivo.

2.1 Proyección de Ingresos

Se estima alcanzar ingresos recurrentes anuales de $4.5 millones de pesos al consolidar una cartera inicial de 50 clientes. El modelo SaaS permite una escalabilidad lineal de ingresos con un incremento marginal en los costos de infraestructura.

2.2 Propuesta de Valor y Retorno (ROI) para el Cliente

La viabilidad comercial se justifica por el impacto directo en las finanzas de la PyME:

- **Ahorro Operativo Directo:** Reducción superior al 80% en comparación con el costo de implementar un SOC interno propio (personal, licencias, hardware).
- **Mitigación de Riesgo Financiero:** Prevención de pérdidas financieras estimadas en hasta $2 millones de pesos por incidente de seguridad promedio (ransomware, fraude).

2.3 Inversión en Capital Humano

La estructura de costos operativos iniciales se concentra en el talento especializado requerido durante el primer año de desarrollo:

1. **Project Manager** (Gestión, metodología y cumplimiento).
2. **Ingeniero de Ciberseguridad** (Arquitectura, seguridad cloud y hardening).
3. **Desarrollador Full-Stack** (Backend de microservicios y Frontend).
4. **Diseñador UI/UX** (Experiencia de usuario y diseño de interfaces).

---

3. FACTIBILIDAD OPERATIVA

La operación es viable mediante la automatización de procesos bajo la filosofía *DevSecOps*, asegurando mantenibilidad, resiliencia y respuesta rápida.

3.1 Acuerdos de Nivel Operativo Interno (OLA)

Se han definido métricas estrictas para los elementos de configuración de la infraestructura:

- **Rendimiento:** Uso de CPU mantenido por debajo del 80% mediante reglas de *auto-scaling*.
- **Resiliencia (RPO):** Punto Objetivo de Recuperación menor a 1 hora ante desastres, mediante snapshots georredundantes.
- **Mantenibilidad:** Tiempo de aprovisionamiento de nueva infraestructura menor a 30 minutos mediante Infraestructura como Código (IaC).

3.2 Niveles de Servicio al Usuario (SLA)

El compromiso de calidad hacia el cliente final incluye:

- **Disponibilidad:** 95% de disponibilidad operativa, salvo breves mantenimientos programados.
- **Soporte:** Tiempo de primera respuesta a incidencias críticas menor a 4 horas.
- **Continuidad:** Actualizaciones y parches críticos.

4. MATRIZ DE RIESGOS Y MITIGACIÓN.

Riesgo Detectado	Descripción e Impacto	Nivel	Estrategia de Mitigación
Escasez de Talento	Dificultad para reclutar perfiles especializados debido a la brecha de profesionales en México.	**Alto**	Implementar plan de capacitación temprana y retención.
Dependencia Tecnológica	Riesgo de aumentos de precio o fallos en las APIs de proveedores externos (EDR).	**Alto**	Diseño modular agnóstico para poder cambiar de proveedor si es necesario.
Adopción del Mercado	Resistencia Cultural de las PyMES por la adopción del un servicio de seguridad externo.	**Medio**	Programa piloto con 10 clientes para generar casos de éxito.
Seguridad Propia	Compromiso de la infraestructura FortaGuard, afectando la reputación de confianza.	**Crítico**	Auditorías continuas y separación estricta de entornos.

5. CONCLUSIÓN

El análisis integral confirma que el proyecto FortaGuard es VIABLE, ya que ataca un problema de mercado urgente (seguridad en PyMEs) con una solución técnica robusta y financieramente atractiva. El éxito del proyecto no depende de la factibilidad tecnológica, que está asegurada por el diseño actual, sino de la ejecución operativa, específicamente en la contratación oportuna del talento y la gestión de proveedores externos.