Plataforma SaaS para la Autoevaluación y Gestión de Cumplimiento de la Ley Marco de Ciberseguridad en Chile

Mariano Varas Ramos
Departamento de Informática
Universidad Técnica Federico Santa María
Santiago, Chile
mariano.varas@usm.cl

Matías Elgueta Chavarria
Departamento de Informática
Universidad Técnica Federico Santa María
Santiago, Chile
matias.elgueta@usm.cl

***Abstract*—Este documento presenta la especificación de un proyecto informático enfocado en el ámbito de la informática legal. Se propone el desarrollo de una plataforma SaaS (Software as a Service) de autoevaluación y gestión de cumplimiento, diseñada para asistir a las entidades designadas como "Operadores de Importancia Vital" (OIV) en Chile a diagnosticar y gestionar su conformidad con la nueva Ley Marco de Ciberseguridad. La solución busca cerrar la brecha entre las exigencias normativas abstractas y su implementación técnica y organizacional concreta, proveyendo una herramienta de diagnóstico, reporte y mejora continua.**

***Index Terms*—Informática Legal, Legal Tech, Ciberseguridad, Cumplimiento Normativo, SaaS, Ley Marco de Ciberseguridad, Chile**

I. Problemática

La implementación de la Ley Marco de Ciberseguridad en Chile ha impuesto un nuevo y complejo conjunto de obligaciones a entidades públicas y privadas que son designadas como "Operadores de Importancia Vital" (OIV). Estas organizaciones, críticas para el funcionamiento del país, deben implementar robustos sistemas de gobernanza, gestión de riesgos y notificación de incidentes. La problemática central es la ausencia de herramientas accesibles que permitan a estas entidades traducir los requisitos legales en controles técnicos y organizacionales verificables. Existe una brecha significativa entre el texto de la ley y la capacidad práctica de las organizaciones para evaluar su nivel de cumplimiento, identificar sus debilidades y planificar mejoras, lo que crea un alto riesgo de incumplimiento y exposición a ciberataques.

Este proyecto es de alta pertinencia para el curso, ya que aborda directamente la interacción entre las "reglas" (la ley) y las "herramientas" (el software), un concepto central de la informática legal. La plataforma actúa como un "modelo de dirección viable", utilizando la tecnología para guiar a las organizaciones hacia el cumplimiento.

II. Solución Propuesta

Se propone el desarrollo de una **plataforma SaaS (Software as a Service) de autoevaluación guiada y gestión de cumplimiento**. Esta herramienta estará diseñada específicamente para guiar a los OIV a través de las obligaciones de la Ley Marco de Ciberseguridad, permitiéndoles diagnosticar su estado de madurez, identificar brechas de cumplimiento y generar planes de acción para la remediación.

III. Funcionalidades

El producto mínimo viable se centrará en tres funcionalidades clave, presentadas en orden de importancia.

A. Módulo de Autoevaluación Guiada y Diagnóstico de Brechas

Esta es la funcionalidad principal. Consiste en un módulo que traduce cada obligación de la ley en un cuestionario interactivo y detallado. Los usuarios pueden responder a cada control y adjuntar evidencia documental. Basado en las respuestas, el sistema realiza un análisis de brechas (Gap Analysis) automático, identificando con precisión los requisitos no cumplidos y su criticidad. Su valor radica en ofrecer un diagnóstico rápido y objetivo que reemplaza las costosas auditorías manuales iniciales. Un CISO[1] de una empresa eléctrica, por ejemplo, podría usarlo para descubrir que su política de seguridad no ha sido formalmente aprobada por el directorio, generando una alerta de incumplimiento.

B. Dashboard Interactivo y Generación de Reportes Ejecutivos

Esta funcionalidad permite ver el nivel de cumplimiento de forma clara y visual. El sistema muestra un puntaje general, indicadores por cada área evaluada y un listado de brechas más relevantes. Además, permite descargar un reporte en PDF para presentar los resultados a la gerencia u otras áreas de la organización. Su valor está en facilitar la comprensión del estado actual y apoyar decisiones rápidas sobre posibles vulnerabilidades de la empresa. Por ejemplo, después de completar la autoevaluación, el CISO puede revisar el dashboard,

[1]El Chief Information Security Officer es el director de seguridad de la información, un alto ejecutivo responsable de supervisar la seguridad de la información y la ciberseguridad de una organización.

identificar que el dominio de gestión de incidentes está en nivel bajo y descargar un reporte ejecutivo para presentarlo en la próxima reunión.

C. Plan de Acción Sugerido y Biblioteca de Recursos

Por cada brecha identificada, el sistema genera un plan de acción con tareas sugeridas, prioridades y plazos estimados. Además, la plataforma incluye una biblioteca de plantillas y documentos útiles, como políticas y guías básicas, que ayudan a implementar mejoras más eficientemente. Su valor radica en facilitar la transición desde el diagnóstico hacia acciones concretas, sin depender totalmente de consultores externos. Por ejemplo, si la plataforma detecta que no existe un plan formal de control de accesos, propone la tarea "Crear y aprobar Política de Control de Accesos" y entrega una plantilla editable para comenzar su elaboración de forma inmediata.

IV. Requerimientos no Funcionales

- **Recursos Técnicos:** El backend se desarrollará en Python con el framework Django, el frontend como una Single Page Application con React o Vue.js, y se utilizará PostgreSQL como base de datos.
- **Arquitectura Multi-tenant:** La plataforma debe garantizar el aislamiento total de los datos entre los diferentes clientes (tenants).
- **Seguridad y Confidencialidad:** Se implementará cifrado de datos en tránsito y en reposo. Se garantizará que los datos de los clientes residan en servidores ubicados en Chile.
- **Escalabilidad y Mantenibilidad:** La arquitectura debe ser escalable para soportar un número creciente de OIVs y permitir actualizaciones sencillas del motor de reglas de cumplimiento.

V. Arquitectura de Funcionamiento

La solución se implementará como una aplicación SaaS multi-tenant de tres capas:

1) **Capa de Presentación (Frontend):** La interfaz de usuario web con la que interactúan los clientes.
2) **Capa Lógica (Backend):** La API construida en Django que contiene toda la lógica de negocio, incluyendo el motor de cumplimiento y la gestión de tenants.
3) **Capa de Datos:** Una base de datos PostgreSQL con un esquema dedicado por cada tenant para un aislamiento robusto, y un servicio de almacenamiento de objetos para la evidencia documental.

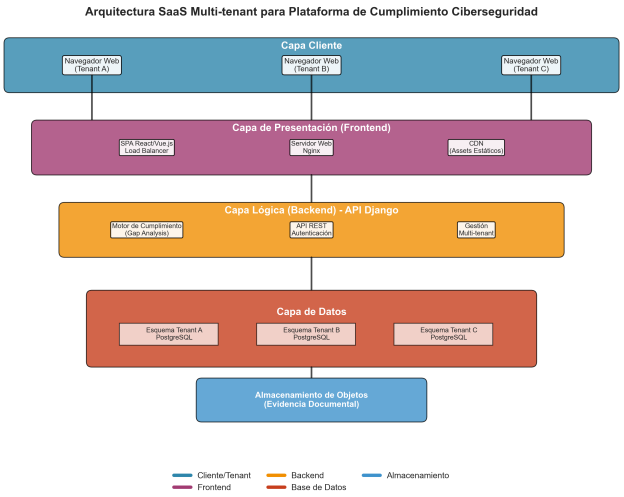

Fig. 1. Diagrama de la arquitectura SaaS multi-tenant propuesta.