



UNIVERSIDAD DE CHILE  
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS  
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Plataforma para auditoria de cumplimiento de Sistema de Gestión de Seguridad de la  
Información

INFORME FINAL DE CC6907 PARA OPTAR AL TÍTULO DE  
INGENIERO CIVIL EN COMPUTACIÓN

Gabriel Rojas Chamorro

MODALIDAD:  
Práctica Extendida

PROFESOR GUÍA:  
Eduardo Godoy Vega

SUPERVISOR:  
Mauricio Castro García

SANTIAGO DE CHILE  
2023

# 1. Introducción

En la era digital en la que vivimos, la seguridad de la información se ha convertido en un componente crítico para el funcionamiento y la supervivencia de las organizaciones. Con la creciente dependencia de los sistemas de información y la gestión de datos sensibles, la necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información se ha vuelto fundamental. En este contexto, el Sistema de Gestión de Seguridad de la Información (SGSI) emerge como un marco de referencia esencial para abordar estos desafíos.

El SGSI proporciona un conjunto de directrices y mejores prácticas que permiten a las organizaciones diseñar, implementar y mantener sistemas de seguridad de la información eficaces. Sin embargo, la complejidad y la constante evolución de las amenazas cibernéticas hacen que la auditoría de cumplimiento del SGSI sea una tarea crítica pero desafiante. Evaluar de manera exhaustiva si una organización cumple con los estándares y requisitos del SGSI requiere un enfoque metódico, recursos especializados y herramientas adecuadas.

En este contexto, este trabajo de título se centra en la creación y desarrollo de una «Plataforma para Auditoría de Cumplimiento del Sistema de Gestión de Seguridad de la Información». Esta plataforma se concibe como una solución integral que combina metodologías de auditoría robustas y la capacidad de automatizar gran parte del proceso de evaluación de cumplimiento del SGSI.

A lo largo de este trabajo, exploraremos en detalle los desafíos asociados con la auditoría de cumplimiento del SGSI, analizaremos las necesidades de las organizaciones en este ámbito y describiremos la arquitectura y funcionalidades clave de la plataforma que proponemos. Además, evaluaremos los beneficios potenciales que esta plataforma puede aportar en términos de eficiencia al momento de auditar el cumplimiento del SGSI.

En última instancia, esta investigación tiene como objetivo contribuir al fortalecimiento de la seguridad de la información en las organizaciones al proporcionar una herramienta efectiva y avanzada para la evaluación y mejora continua del cumplimiento del SGSI. A medida que avanzamos en la era digital, el papel de esta plataforma se vuelve cada vez más crucial para salvaguardar la información crítica en un entorno altamente cambiante y amenazante.

Magnet, la empresa con la cual se trabajara esta memoria, es una empresa con más de 10 años de experiencia, dedicada a ofrecer soluciones tecnológicas a problemas complejos de negocios a través de software a la medida. Para Magnet este sistema es relevante dado que las soluciones actuales generan una dependencia permanente de otra empresa para obtener la certificación ISO27001. Al tener su propia plataforma de auditoria, Magnet puede dejar

de depender de externos y además puede tener una solución que se adecue mejor a sus necesidades.

## 2. Situación Actual

Hoy en día existen programas capaces de manejar la auditoria para SGSI, la mayoría de estos programas son soluciones de software como servicio (SaaS, por sus siglas en inglés), pero también existen algunas soluciones de código abierto. En esta sección hablaremos de principalmente 2 aplicaciones, MyLenio y Gapps.

### MyLenio

Entre las opciones SaaS, se encuentra MyLenio, una plataforma la cual se compone de 3 principales módulos, «organización del equipo», «recursos humanos» y «cumplimiento y seguridad».

#### 2.1.1. Organización del equipo<sup>1</sup>

El módulo de organización del equipo permite asignar a cada empleado a los equipos a los cuales pertenece. Los equipos son la unidad básica de organización de MyLenio, estos también permiten asignar roles a cada empleado, para obtener mayor granularidad. Al tener organizado a cada empleado dentro de un equipo, esto permite tener mayor visibilidad de como se componen estos mismos dentro de la empresa, incluso ofreciendo un organigrama de los roles de cada proyecto.

##### 2.1.1.1. Manejo de permisos

Dentro de cada equipo se puede se pueden crear, editar y remover permisos a distintos SaaS. Estos permisos se pueden asignar tanto a nivel de equipo, rol o empleado, pudiendo así manejar todos los permisos de diferentes SaaS desde un único lugar. Cuando se agregan nuevos integrantes a estos equipos, también se le asignan todos los permisos a las aplicaciones SaaS configuradas, haciendo más facil el proceso de incorporación de nuevos miembros a los equipos. Entre los SaaS se encuentran Bitbucket, DocuSign, GitHub, GitLab, Google G-Suite, Jira, Keeper password, Office 365, Slack y Trello.

##### 2.1.1.2. Documentos, capacitaciones y tareas

A cada uno de los miembros de un equipo se les puede asignar documentos, capacitaciones o tareas. Asignar documentos por este medio permite el cumplimiento del sistema de seguridad de la información y le facilita a los empleados firmar, de ser necesario. Asimismo, permite asignar capacitaciones y mostrar el progreso de estas, pudiendo notificar

---

<sup>1</sup><https://www.mylenio.com/team-organization>

a los empleados que aún no la han completado. Análogamente, se le pueden asignar tareas a los empleados y notificarlos para que las terminen.

### **2.1.2. Recursos Humanos<sup>2</sup>**

El módulo de recursos humanos proporciona herramientas para realizar las actividades diarias de forma organizada, ayudando al área de recursos humanos, valga la redundancia.

#### **2.1.2.1. Incorporación de empleados**

La integración con G-Suite y Office 365 permite incorporar a empleados con mayor facilidad al crearle cuentas, poder asignarlo a sus futuros equipos, pedirle la firma en documentos, asignarle capacitaciones o tareas a realizar.

#### **2.1.2.2. Participación y eficiencia del equipo**

MyLenio proporciona la habilidad de entregar reconocimientos a sus empleados mediante la plataforma, también permite manejar los anuncios, beneficios, vacaciones y otros tipos de solicitudes. Esto ayuda a ahorrar tiempo, al estar todo en una única aplicación.

#### **2.1.2.3. Reclutamiento**

Dentro del área de recursos humanos se entrega una herramienta para darle seguimiento a las posiciones abiertas, los candidatos y en qué parte del proceso se encuentra actualmente cada candidato.

#### **2.1.2.4. Información de los empleados**

La información de cada empleado es guardada en G-Suite u Office 365, así facilitando su visualización, además se puede manejar la edición de esta información desde la aplicación. De ser necesario también se tiene una vista con toda la información del empleado, sus documentos, tareas, capacitaciones, etc.

### **2.1.3. Cumplimiento y Seguridad<sup>3</sup>**

El módulo de cumplimiento y seguridad de MyLenio puede ser dividido en varios submódulos, cada uno con su propia funcionalidad y propósito.

---

<sup>2</sup><https://www.mylenio.com/human-resources-hr>

<sup>3</sup><https://www.mylenio.com/compliance-and-security>

### **2.1.3.1. Reporte de Cumplimiento en Tiempo Real**

Este submódulo proporciona una visión completa de la empresa con múltiples paneles que muestran todo lo que está sucediendo en la compañía. Permite saber exactamente quién ha firmado los documentos, cómo está progresando la formación y ver todas las tareas y flujos pendientes.

### **2.1.3.2. Manejo de Inventario**

Este submódulo permite manejar el inventario de la empresa en un solo lugar. Se pueden crear elementos como computadores, monitores, etc., y asignar esos activos a los empleados. De esta manera, se puede hacer un seguimiento de quién está en posesión de los activos y saber exactamente dónde se encuentra todo en este momento.

### **2.1.3.3. Modelamiento de Procesos**

El módulo de Flujos permite modelar los procesos existentes en un sistema robusto donde se puede hacer un seguimiento del progreso, ver quién tiene algo pendiente y cómo avanzan los procesos en tiempo real. Al modelar los flujos, se puede poner el conocimiento sobre cómo se hacen las cosas en el departamento en un sistema, facilitando el crecimiento del equipo.

### **2.1.3.4. Eventos Recurrentes y Automatización de Cumplimiento**

MyLenio permite programar Flujos, Documentos, Tareas y Formaciones en un sistema que permite establecer cosas recurrentes que suceden en la empresa, como la firma de documentos cada año, asignar formación cada 6 meses a los empleados, etc. De esta manera, se pueden automatizar los procesos, ahorrar tiempo y dinero, y encaminarse hacia el cumplimiento de diversas certificaciones.

### **2.1.3.5. Manejo de Riesgos**

Este módulo permite hacer un seguimiento de todos los riesgos de la empresa, estableciendo los activos, amenazas y vulnerabilidades. También permite gestionar los proveedores y establecer el personal de BCDR (Business Continuity and Disaster Recovery).

## **Gapps**

Gapps es una plataforma de cumplimiento de seguridad que facilita el seguimiento de su progreso en relación con varios marcos de seguridad. Actualmente, el principal contribuyente al proyecto desaconseja su uso en entornos de producción<sup>4</sup>.

En el momento de la lectura, Gapps ofrece soporte para más de 10 marcos de cumplimiento de seguridad, incluyendo ISO27001. Además, cuenta con más de 2000 controles y 30 políticas, lo que permite recopilar evidencia para luego visualizarla en un panel de control<sup>5</sup>.

Es importante destacar que, aunque Gapps es una herramienta poderosa para el seguimiento del cumplimiento de seguridad, su uso debe ser considerado cuidadosamente, especialmente en entornos de producción. Esto se debe a que el principal contribuyente al proyecto ha expresado su preocupación sobre su uso en tales entornos.

Con más de 2000 controles y 30 políticas disponibles, Gapps ofrece una amplia gama de opciones para ayudar a las organizaciones a seguir su progreso en el cumplimiento de la seguridad. Estos controles y políticas pueden ser utilizados para recopilar evidencia, que luego puede ser visualizada en un panel de control.

En resumen, Gapps es una plataforma de cumplimiento de seguridad que ofrece una amplia gama de herramientas para ayudar a las organizaciones a seguir su progreso en el cumplimiento de la seguridad. Sin embargo, su uso debe ser considerado cuidadosamente, especialmente en entornos de producción.

## **Necesidad de un trabajo novedoso**

La urgencia de desarrollar un software innovador se fundamenta en la carencia de una solución que se ajuste a las especificidades de Magnet. Actualmente, Magnet gestiona sus propios sistemas para abordar múltiples módulos de MyLenio, como la información de los empleados, anuncios y periodos de vacaciones, entre otros. La utilización simultánea de una plataforma externa como MyLenio podría generar confusión y redundancia en los procesos internos de la organización.

Además, la dependencia de un software externo implica la asunción de pagos mensuales sujetos a cambios imprevistos, sin la certeza de que el proveedor mantendrá la continuidad del servicio a largo plazo. La posibilidad de tener que migrar información entre distintos proveedores presenta un riesgo considerable, especialmente en el contexto de la necesidad de mantener certificaciones específicas.

Una consideración adicional radica en la viabilidad de comercializar esta aplicación a una amplia gama de clientes, tanto dentro de la misma industria como en otros sectores

---

<sup>4</sup><https://github.com/bmarsh9/gapps>

<sup>5</sup><https://web-gapps.pages.dev/>

e incluso entre la competencia. La concepción de un software que no solo satisfaga las necesidades internas de Magnet, sino que también tenga potencial para ser implementado por otras organizaciones, amplía significativamente el alcance y la relevancia del proyecto.

Es imperativo abordar estas problemáticas de manera estratégica, asegurando que el desarrollo del software no solo satisfaga las necesidades actuales de Magnet, sino que también tenga una proyección a largo plazo. La consideración de la escalabilidad y la capacidad de adaptación a diferentes contextos se torna esencial para garantizar la eficacia y la sostenibilidad del software propuesto.

En resumen, el impulso de crear un trabajo novedoso no solo se basa en subsanar las deficiencias actuales, sino también en explorar oportunidades de expansión y comercialización, consolidando así un proyecto que no solo beneficie internamente a Magnet, sino que también tenga un impacto positivo en el panorama empresarial más amplio.



### **3. Objetivos**

#### **Objetivo General**

El propósito fundamental de este proyecto es desarrollar un software dedicado a auditar el cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001. Esta plataforma centralizará la gestión de documentos, activos, riesgos y flujos vinculados a los diversos controles de seguridad establecidos por ISO 27001. La finalidad última es posibilitar que Magnet SPA obtenga y mantenga de manera eficiente la certificación ISO 27001, asegurando así la robustez y conformidad de sus prácticas de seguridad de la información.

#### **Objetivos Específicos**

Implementar un módulo que permita el manejo eficiente de documentos, asegurando la versión controlada y la posibilidad de aprobación o solicitud de cambios. Este módulo deberá ser intuitivo, garantizando una interfaz de usuario amigable para facilitar la colaboración y la gestión de documentos. Además, debe contar con un sistema de notificaciones para informar sobre cambios pendientes de aprobación y proporcionar un historial detallado de versiones para rastrear la evolución de los documentos a lo largo del tiempo.

Diseñar un módulo integral para mantener un registro detallado de los activos de la empresa, abarcando desde equipos electrónicos hasta lugares físicos, personas, servicios y software. Este módulo deberá permitir la fácil asignación de dueños, clasificación según criterios predefinidos y una evaluación de criticidad. Asimismo, se espera que tenga funciones de seguimiento de cambios en la información de activos y genere alertas ante modificaciones significativas.

Desarrollar un gestor de riesgos que complemente los módulos de gestión documental y registro de activos. Este permitirá la definición de planes de acción específicos frente a posibles riesgos, alineándose con las políticas establecidas en el primer módulo. La integración de estos elementos fortalecerá la capacidad de anticipar y abordar los desafíos potenciales para el SGSI.

Introducir un motor de procesos que gestionará los flujos asociados con los diferentes controles de ISO27001. Este motor debe ser configurable para permitir la ejecución manual y automática de los controles, con la capacidad de generar registros detallados de las actividades realizadas. Además, se espera que incluya mecanismos de notificación para alertar sobre cualquier desviación en la ejecución de los controles programados.

Implementar un módulo dedicado a la generación de informes y análisis de datos. Este módulo debe ofrecer capacidades de personalización de informes para adaptarse a las necesidades específicas de Magnet SPA. Además, deberá proporcionar métricas clave, gráficos visuales y análisis comparativos para facilitar una evaluación completa y detallada del estado del SGSI.

## **Evaluación**

La evaluación del desempeño del sistema con respecto a los objetivos planteados se llevará a cabo mediante encuestas de satisfacción y usabilidad, centradas en métricas específicas como la eficacia en la gestión documental, la facilidad de uso del registro de activos, la eficacia del gestor de riesgos, la flexibilidad del motor de procesos y la utilidad del módulo de reportes y análisis. Estas encuestas proporcionarán datos cuantificables sobre la experiencia del usuario y la eficacia general del software, asegurando una comprensión detallada de su rendimiento desde la perspectiva del usuario final.

Adicionalmente, se buscará la participación activa de expertos en seguridad, quienes someterán la plataforma a rigurosas pruebas y revisiones técnicas. Estos expertos aportarán una evaluación especializada sobre la seguridad del sistema, identificando posibles vulnerabilidades y ofreciendo sugerencias específicas para mejoras. Esta evaluación por parte de expertos complementará las percepciones de los usuarios finales, asegurando que el software no solo sea intuitivo y funcional, sino también robusto y conforme a los estándares más rigurosos de seguridad en el ámbito de la gestión de la información.

## 4. Solución Propuesta

La solución propuesta se adapta de manera efectiva para abordar desafíos relacionados con la escalabilidad, el rendimiento y la seguridad del sistema, incorporando consideraciones específicas en su diseño y arquitectura.

En términos de escalabilidad, si bien el proyecto no está inicialmente diseñado para manejar un gran flujo de usuarios, la implementación en contenedores Docker permite una fácil replicación y despliegue detrás de un balanceador de carga. Esto facilita la escalabilidad horizontal, permitiendo la adición de nuevos contenedores según sea necesario. Para la gestión de datos, la escalabilidad vertical de la base de datos PostgreSQL y la opción de utilizar réplicas para lectura proporcionan una respuesta eficiente a posibles aumentos en la carga de datos.

En cuanto al rendimiento, la elección de tecnologías robustas y bien probadas, como Django, PostgreSQL y Typescript, proporciona una base sólida. La experiencia previa con sistemas similares garantiza que el escalamiento de la aplicación sea un proceso manejable, respaldado por las mejores prácticas y lecciones aprendidas de implementaciones anteriores.

La interoperabilidad entre las tecnologías utilizadas se ve respaldada por la compatibilidad inherente de Django con PostgreSQL y la elección de Typescript como lenguaje en el frontend. Además, se planea seguir estándares y prácticas documentadas para asegurar una integración fluida, aprovechando la documentación existente como guía.

En cuanto a la seguridad, se implementan múltiples capas de protección. La confidencialidad de la información se garantiza mediante permisos de usuario, y la autenticación y autorización se plantean a través de un sistema de Single Sign-On (SSO) utilizando G Suite, aunque también se considera el sistema de autenticación interno de Django como alternativa. La integridad de la información se asegura mediante la implementación de hashes para versionar archivos, brindando una capa adicional de seguridad contra manipulaciones no autorizadas.

Para abordar la experiencia del usuario durante el desarrollo, se planea mantener un servidor de desarrollo o staging en funcionamiento. Aunque actualmente no existen prototipos para la interfaz de usuario, se realizarán pruebas continuas de usabilidad durante el desarrollo para garantizar una experiencia intuitiva y fácil de navegar.

La estrategia de mantenimiento del software implica mantener todas las versiones en LTS (long term support), asegurando la obtención de actualizaciones de seguridad y la estabilidad a lo largo del tiempo. Se busca mantener un ciclo de vida de desarrollo continuo, priorizando la corrección de problemas y el desarrollo de nuevas funcionalidades, reconociendo que el tiempo invertido es un factor crítico.

La elección de DigitalOcean como plataforma de implementación se basa en la experiencia previa y en consideraciones económicas, ya que se percibe como una opción más rentable entre los grandes proveedores de servicios en la nube. Aunque se ha considerado Amazon Web Services (AWS) debido a la experiencia previa, la decisión se inclina hacia DigitalOcean por razones monetarias.

La colaboración con expertos en seguridad se plantea actualmente como una posibilidad abierta. Se espera utilizar herramientas de código abierto, como las proporcionadas por OWASP, para analizar posibles vulnerabilidades en el sistema, y se está abierto a sugerencias específicas para facilitar la colaboración con expertos en seguridad.

En relación con la internacionalización y localización, la plataforma se diseñará para ser accesible tanto en inglés como en español mediante la incorporación del sistema de internacionalización de Django. Este enfoque permitirá que la interfaz de usuario se adapte fácilmente a diferentes idiomas, brindando una experiencia inclusiva y personalizada para usuarios de distintas regiones y culturas.

La implementación de la internacionalización en Django facilitará la gestión de cadenas de texto en múltiples idiomas, permitiendo una fácil traducción de la interfaz de usuario. Esto no solo mejora la accesibilidad para un público global, sino que también establece una base sólida para futuras expansiones lingüísticas.

Además, se garantizará que la localización no se limite simplemente a la traducción de contenido, sino que también abarcará otros aspectos culturales relevantes, como formatos de fecha, hora y moneda. Este enfoque integral asegurará una experiencia consistente y adaptada a las preferencias locales de los usuarios, contribuyendo así a la usabilidad y aceptación del sistema en diferentes contextos.

En resumen, la adopción del sistema de internacionalización de Django refuerza el compromiso de la plataforma con la diversidad lingüística y cultural, promoviendo un entorno inclusivo y accesible para una audiencia global.

## 5. Plan de Trabajo (Preliminar)

El trabajo contemplará a grandes rasgos las siguientes tareas:

1. Creación de historias de usuario y subtareas
2. Creación del repositorio
3. Iniciar el proyecto Django
4. Creación del módulo de documentos
5. Creación del módulo de activos
6. Creación del módulo de riesgos
7. Creación del módulo de flujos
8. Realizar encuestas de satisfacción y usabilidad
9. Pedir comentarios de expertos en seguridad
10. Analizar el software con una herramienta en busca de vulnerabilidades
11. Redactar informe final

## Referencias