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[1]

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

[1] 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[2]

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 guardad 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[3]

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

[2]https://www.mylenio.com/human-resources-hr
[3]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 de un vistazo.

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 computadoras, 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 de programación robusto 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 SOC2, PCI, HIPAA.

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[4].

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[5].

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

[4]https://github.com/bmarsh9/gapps
[5]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

Durante este trabajo se desea construir un software que permita auditar el cumplimiento de SGSI. Este software será la plataforma donde se registraran documentos, activos, riesgos y flujos asociados a los diferentes controles de seguridad de ISO27001.

Objetivos Específicos

Para cumplir el objetivo general, primero, se debe incorporar un módulo que permita manejar documentos, donde estos queden versionados y se les pueda dar una aprobación o pedir cambios, con el propósito de tener un único lugar con todos los archivos de las políticas para los controles de ISO27001.

El segundo módulo deberá encargarse de mantener un registro de los activos de la empresa, entre estos encontramos equipos electrónicos, lugares físicos, personas, servicios y software, permitiendo definir un dueño, una clasificación y su criticidad.

El tercer módulo se compondrá de un gestor de riesgo. Este complementará los 2 módulos anteriores, permitiendo definir diferentes planes de acción frente a los posibles riesgos, basándose en las políticas del primer módulo.

Por último, se agregará un motor de procesos para manejar flujos de los distintos controles, que se iniciaran tanto manualmente como cada ciertos periodos de tiempo predefinidos. De esta manera se podrá mantener un registro de que se están cumpliendo las actividades definidas por los controles.

Evaluación

Para evaluar el desempeño del sistema frente a los objetivos mencionados se usarán principalmente encuestas de satisfacción y usabilidad. Además, se intentará que expertos en seguridad usen la plataforma, den su opinión y sugieran posibles mejoras.

4. Solución Propuesta

La solución consiste en una plataforma capaz de manejar documentos, activos, riesgos y flujos. La idea es poder auditar un SGSI basado en ISO27001, por ende se debe tener una forma de acceso para múltiples tipos de usuarios como auditor, administrador y trabajadores.

Como principal base del sistema se usarán los controles que se definen por parte ISO27001, donde cada empresa tendrá la responsabilidad de decidir cuáles implementara y cuáles serán sus políticas internas.

Para guardar todos los datos generados por la aplicación se usará una base de datos relacional, en específico PostgreSQL. Se decide usar esta base de datos, ya que se posee previa experiencia con la misma, por ser de código abierto y tener funcionalidades que otras opciones como MySQL no poseen.

Para el backend se usará Django. Esta decisión viene dada de que Django posee un ORM («Modelo de programación que permite mapear las estructuras de una base de datos relacional» [1]) ya integrado, tiene una buena documentación, es de código abierto, esta basado en Python y se tiene experiencia previa con el framework y el lenguaje, esto es tanto para el alumno como la empresa.

Para el frontend, ya que se está usando Django se usará un sistema de plantillas de HTML. Además, se usará un framework de CSS para estilar estas plantillas, probablemente siendo este Bootstrap. De ser necesario se usará Typescript para obtener datos o hacer algún componente reactivo. Se decide no usar un framework de Javascript, debido a que la página en sí será bastante estática, por lo que usar un framework más interactivo no muestra una clara ventaja. Al igual que para las herramientas y tecnologías backend, se posee experiencia previa tanto del alumno como la empresa.

Se espera que este proyecto quede desplegado en un servidor, posiblemente en DigitalOcean. Este servidor contará con el sistema operativo Linux y se harán los despliegues usando ansible para tener reproducibilidad y Docker para evitar problemas de portabilidad y consistencia.

Cabe destacar que tener experiencia previa tanto el alumno como la empresa con las herramientas y tecnologías que se usarán ayudara al mantenimiento del software y permitirá hacer futuras mejoras sin tener que invertir en aprender nuevas tecnologías.

Para realizar las encuestas de satisfacción y usabilidad, para evaluar el sistema, se decide en usar los forms de Google dada su facilidad de uso y de distribución.

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

[1] J. A. Muro, «¿Qué es un ORM?». [En línea]. Disponible en: https://www2.deloitte.com/es/es/pages/technology/articles/que-es-orm.html