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

PROPUESTA DE TEMA DE MEMORIA 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». El módulo de «cumplimiento y seguridad» es el de mayor interés, ya que, es el que proporciona ayuda para el cumplimiento de un SGSI.

2.1.1. Organización del equipo[1]

El módulo de organización del equipo permite organizar equipos en roles y grupos, permitiendo asignarles en la plataforma:

- Formación
- Documentos
- Tareas a realizar
- Permisos automáticos a otras aplicaciones SaaS

2.1.2. Recursos Humano[2]

El módulo de recursos humanos proporciona ayuda en varios temas relacionados con esto. Entre estos temas se encuentran:

- Reclutamiento
- Incorporación de nuevos empleados
- Compromiso de los empleados
- Información de los empleados
- Modelar procesos de recursos humanos

2.1.3. Cumplimiento y Seguridad[3]

El módulo de cumplimiento y seguridad se puede separar en varios submódulos.

[1]https://www.mylenio.com/team-organization
[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 módulo proporciona la habilidad para saber quién firmo los documentos, el progreso de las formaciones y por último el estado en que se encuentran las tareas y flujos asignados al equipo.

2.1.3.2. Manejo de inventario

Este submódulo permite manejar el inventario de la empresa. Los elementos del inventario luego se le pueden asignar a los miembros del equipo.

2.1.3.3. Modelamiento de procesos

Este módulo permite modelar flujos existentes y monitorear su progreso.

2.1.3.4. Eventos recurrentes y automatización de cumplimiento

Este módulo permite asignar flujos, documentos, tareas y formación al equipo de manera automatizada. Estos puede ser fechas o acciones que se deban realizar cada cierto tiempo.

2.1.3.5. Manejo de riesgos

Este módulo permite hacer un seguimiento de todos los riesgos de la empresa, por medio del establecimiento de activos, amenazas y vulnerabilidades.

Gapps

Gapps es una plataforma de cumplimiento de seguridad que facilita el seguimiento de su progreso frente a varios marcos de seguridad. Actualmente, el principal contribuidor al proyecto desincentiva su uso en ambientes de producción[4].

Al momento de la lectura, Gapps cuenta con soporte para más de 10 marcos de cumplimiento de seguridad, entre ellos ISO27001. Además, cuenta con más de 2000 controles y 30 políticas, permitiendo recolectar la evidencia para luego poder visualizarla en un dashboard[5].

Necesidad de un trabajo novedoso

Esta necesidad surge debido a la falta de un software que se adecue a las necesidades de Magnet. Principalmente, el depender de un software de un externo, teniendo que pagar mensualidades y sin tener la certeza de que el software se seguirá manteniendo y no se tenga que migrar la información entre distintos proveedores.

3. Objetivos

[4]https://github.com/bmarsh9/gapps
[5]https://web-gapps.pages.dev/

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 y 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 y 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 usaran 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 usara 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 usaran 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?." https://www2.deloitte.com/es/es/pages/technology/articles/que-es-orm.html