



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

DESARROLLO DE UNA PLATAFORMA PARA AUDITORÍA DE CUMPLIMIENTO
DE SISTEMA GENERAL DE SEGURIDAD DE INFORMACIÓN (SGSI)

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN COMPUTACIÓN

GABRIEL ROJAS CHAMORRO

PROFESOR GUÍA:
EDUARDO GODOY VEGA

SUPERVISOR:
MAURICIO CASTRO GARCÍA

MIEMBROS DE LA COMISIÓN:
ALEJANDRO HEVIA A.
CAMILO GÓMEZ

SANTIAGO DE CHILE
2024

Resumen

El desarrollo de una plataforma para la auditoría de cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI) en una empresa sigue un enfoque metodológico claro y riguroso. La motivación principal radica en la necesidad de garantizar la seguridad de la información en un entorno digital cada vez más complejo, donde las amenazas cibernéticas y la interconexión de sistemas presentan desafíos constantes.

El problema identificado se centra en la carencia de una herramienta eficiente y específica para la gestión del SGSI, que permita a las empresas cumplir con los estándares internacionales, como la ISO 27001, sin depender de soluciones externas que pueden ser costosas y difíciles de integrar. La dependencia de software de terceros no solo implica costos adicionales, sino también riesgos asociados con la continuidad del servicio y la necesidad de migrar datos en caso de cambios en los proveedores.

El objetivo del proyecto es desarrollar una solución integral que facilite la gestión de documentos, activos, riesgos y procesos, permitiendo a la empresa no solo cumplir con los requisitos de la ISO 27001, sino también mejorar su postura de seguridad de manera sostenible y escalable. La plataforma desarrollada incluye módulos específicos para cada uno de estos componentes, proporcionando funcionalidades detalladas que abarcan desde la creación y gestión de documentos hasta la evaluación y mitigación de riesgos.

La solución propuesta se basa en tecnologías robustas y probadas, como Django para el backend, PostgreSQL para la base de datos y TypeScript para el frontend, garantizando así la escalabilidad y el rendimiento del sistema. La arquitectura de despliegue se realiza mediante contenedores Docker, lo que facilita la replicación y el balanceo de carga, permitiendo una fácil adaptación a las necesidades cambiantes de la empresa.

Los resultados obtenidos demuestran la eficacia de la plataforma en un contexto real, con una mejora significativa en la gestión de la seguridad de la información y una reducción de los riesgos asociados. La encuesta de usabilidad realizada arroja resultados positivos, confirmando que la solución no solo cumple con los requisitos técnicos, sino que también es fácil de usar y adaptar a diferentes contextos empresariales.

En resumen, la plataforma desarrollada representa un avance significativo en la gestión del SGSI, ofreciendo a las empresas una herramienta estratégica que mejora la seguridad de la información, reduce los costos de cumplimiento y asegura la continuidad operativa en un entorno digital dinámico.

Dedicado a aquellos que no tuvieron la oportunidad de terminar este camino con nosotros.

Agradecimientos

Agradecimientos especiales a Nicolás Alexandroff, Luis Reyes, Gilberto Salazar, Nicolás Santibáñez, Nicolás Zúñiga, familia Zúñiga Ostermann, mis padres, Edgardo Rojas e Ingrid Chamorro y mis hermanos, Maximiliano Rojas y Josefina Rojas, por siempre apoyarme en este camino y por compartir esos conocimientos que no son enseñadas en salas de clases.

Tabla de Contenido

1. Introducción	1
1.1. Contexto	1
1.2. Problema y Relevancia	3
1.3. Objetivos	4
1.4. Descripción general de la solución	5
2. Situación actual	7
2.1. MyLenio	7
2.2. Gapps	13
2.3. Necesidad de un trabajo novedoso	15
3. Solución	17
3.1. Tecnologías escogidas	17
3.2. Django Project Template (DPT)	18
3.3. Perfiles de usuario del sistema	20
3.4. Módulo de Usuarios	21
3.5. Módulo de Documentos	25
3.6. Módulo de Activos	35
3.7. Módulo de Riesgos	42
3.8. Módulo de Procesos	45
4. Evaluación	56
4.1. Uso en un Contexto Real	56
4.2. Encuesta de Usabilidad	57
4.3. Análisis de la Encuesta	58
4.4. Conclusiones de la Evaluación	58
5. Conclusiones	59
5.1. Resumen del Trabajo Realizado	59
5.2. Objetivos Alcanzados y No Alcanzados	59
5.3. Análisis Crítico de los Resultados	60
5.4. Relevancia e Impacto del Trabajo Realizado	60
5.5. Lecciones Aprendidas	60
5.6. Trabajo Futuro	60

Bibliografía	62
6. Anexo	63
6.1. Modelo de datos módulo de Usuarios	63
6.2. Vistas módulo de Usuarios	64
6.3. Modelo de Datos módulo de Documentos	67
6.4. Vistas modulo de Documentos	69
6.5. Modelo de Datos módulo de Activos	74
6.6. Vistas modulo de Activos	75
6.7. Modelo de Datos módulo de riesgos	76
6.8. Modelo de Datos módulo de procesos	77
6.9. Vistas modulo de procesos	79

Capítulo 1

Introducción

En el mundo actual, donde la información se ha convertido en uno de los activos más valiosos para las organizaciones, la seguridad de la información es crucial para la continuidad y la confianza en las operaciones empresariales. La presente introducción abordará el contexto general del proyecto, el problema y su relevancia, los objetivos planteados, y finalmente, una descripción general de la solución implementada.

1.1. Contexto

En el vertiginoso panorama actual, caracterizado por la revolución digital y la saturación de datos e información, la seguridad de la información emerge como un baluarte fundamental para asegurar la continuidad y la confianza en las operaciones empresariales. En este contexto, la constante evolución de las amenazas ciberneticas y la creciente interconexión de sistemas han convertido la salvaguarda de la confidencialidad, integridad y disponibilidad de la información en una prioridad crítica, desafiando a las organizaciones a mantenerse a la vanguardia de la seguridad informática.

Las organizaciones, en este desafío constante, se ven compelidas a garantizar que sus sistemas no solo cumplan con los estándares de seguridad, sino que también sigan las mejores prácticas establecidas. Es en este contexto que el Sistema de Gestión de Seguridad de la Información (SGSI), especialmente dentro del marco del estándar ISO 27001, emerge como una guía esencial para diseñar, implementar y mantener sistemas de seguridad robustos. La certificación ISO 27001, por ende, no solo proporciona un marco sólido para la gestión de la seguridad de la información, sino que también otorga a las empresas un distintivo reconocido internacionalmente, validando su compromiso inquebrantable con la seguridad.

En el epicentro de este escenario complejo se halla la empresa Magnet, una entidad con una sólida trayectoria de más de una década en la provisión de soluciones tecnológicas a medida. Para Magnet, la necesidad imperante de asegurar la integridad y confidencialidad de su información y la de sus clientes, especialmente en el contexto de la certificación ISO 27001, adquiere una importancia estratégica.

1.1.1. Magnet

Magnet es una empresa con una fuerte presencia en el mercado de software y tecnología, ofreciendo una amplia gama de servicios y productos. Entre los principales se encuentran:

- *Desarrollo a medida*: Magnet desarrolla código para brindar valor, simplificar procesos y establecer la trazabilidad de los proyectos.
- *Proyectos del Estado*: Trabaja con instituciones del gobierno, con un Acuerdo Marco vigente, y una sólida experiencia en la colaboración con el Estado de Chile.
- *Aumento de equipo en EE. UU.*: Proporciona desarrolladores y diseñadores para fortalecer los equipos de sus clientes.
- *Transformación Digital*: Implementa, mantiene y mejora continuamente los servicios relacionados con la transformación digital.
- *Integraciones*: Facilita la integración de Django con diversas aplicaciones y servicios en la nube para aumentar la eficiencia y productividad.
- *Proceso UX*: Entrega soluciones innovadoras alineadas con los objetivos empresariales mediante un diseño centrado en el usuario.
- *E-commerce*: Provee plataformas personalizadas para aplicaciones móviles de comercio electrónico.
- *Infraestructura*: Ofrece servicios en la nube seguros, escalables y flexibles para optimizar el crecimiento empresarial.

Magnet cuenta con un equipo compuesto por entre 30 y 40 empleados. El área de operaciones está estructurada en diversos roles y departamentos que incluyen Jefes de Proyectos (PM), Technical Leads (TL), desarrolladores frontend y backend, analistas TI, y diseñadores UX.

1.1.2. Equipo de Proyecto

Para este trabajo de título, el equipo involucrado se compone principalmente de tres personas:

- *Gerente de Operaciones*: Mauricio Casto, quien toma un rol de apoyo técnico y supervisión, actuando como un Senior Advisor.
- *Gerente General*: Ignacio Munizaga, desempeñando el rol de Product Owner, proporcionando orientación y visión para el proyecto.
- *Jefe de Proyecto y Desarrollador*: El autor de este trabajo, responsable de la planificación, ejecución y desarrollo del proyecto.

1.1.3. Rol del Supervisor

El supervisor del autor, Mauricio Casto, es uno de los socios de Magnet y el Gerente de Operaciones. Su rol principal es estandarizar los procesos, herramientas y prácticas del área de Operaciones y coordinar los recursos entre proyectos. En el contexto de este trabajo de título, su responsabilidad principal ha sido asegurar que lo que se está desarrollando sea de utilidad para la empresa, proporcionando apoyo y supervisión técnica.

La interacción con el supervisor ha sido positiva, especialmente al principio del proyecto, donde se recibió un considerable apoyo en la planificación de la idea principal. Posteriormente, el Gerente General también ha proporcionado apoyo significativo en el refinamiento de la plataforma.

1.1.4. Formas de Trabajar en Magnet

Magnet utiliza una metodología ágil basada en Scrum, adaptada a las siguientes consideraciones:

- El producto se desarrolla fuera de la organización que será dueña del producto, usualmente con un Product Owner externo.
- Los incentivos de la organización pueden no estar siempre alineados con los de Magnet.
- Existen contratos y compromisos de buen servicio que norman el proyecto más allá del óptimo para el desarrollo del producto.

La gestión de proyectos y la comunicación dentro del equipo se realiza principalmente a través de Slack para la comunicación asíncrona, y mediante reuniones semanales (weeklys) y reuniones de avances. Los weeklys se enfocan en el desarrollo y en resolver trabas, mientras que las reuniones de avances se centran en mostrar avances concretos de la aplicación.

Las herramientas utilizadas incluyen Jira para la gestión de proyectos, Google Workspace para videoconferencias y almacenamiento, y Slack para la comunicación. Magnet fomenta un ambiente de trabajo colaborativo y una cultura abierta, promoviendo la participación de todos en la toma de decisiones y manteniendo un flujo constante de feedback para mejorar continuamente.

1.2. Problema y Relevancia

La creciente sofisticación de las amenazas ciberneticas y la diversificación de los vectores de ataque subrayan la relevancia y la urgencia de contar con un sistema de gestión de seguridad de la información robusto para proteger los activos digitales y salvaguardar la reputación de la empresa u organización en el escenario empresarial y regulatorio actual.

No obstante, en medio de esta búsqueda de seguridad, las organizaciones enfrentan limitaciones al depender de soluciones externas para manejar la implementación y el almacenamiento de evidencia, piezas cruciales al momento de ser auditados para obtener certificaciones o demostrar el cumplimiento de leyes. Es en este punto crítico que surge la motivación para el desarrollo de una solución interna y personalizada, impulsada por las tendencias actuales hacia la autonomía y la adaptabilidad en el dinámico panorama de la seguridad de la información.

Las empresas, ahora más que nunca, buscan soluciones que no solo cumplan con estándares reconocidos, como la ISO 27001, sino que también ofrezcan flexibilidad y capacidad de adaptación a las cambiantes condiciones del entorno digital. La ausencia de un sistema

interno eficiente para la gestión de SGSI puede resultar en desafíos operativos, costos adicionales y riesgos incrementados de no conformidad con las normas establecidas, lo que podría tener consecuencias significativas en términos de sanciones y pérdida de confianza de los clientes.

1.3. Objetivos

En respuesta a este desafío, el proyecto propuesto tiene como objetivo la creación de una «Plataforma para Auditoría de Cumplimiento del Sistema de Gestión de Seguridad de la Información», abordando de manera específica los desafíos que enfrenta Magnet y otras organizaciones en este ámbito crucial. Esta plataforma no solo aspira a cumplir con los requisitos de auditoría; se concibe como un habilitador estratégico que otorga a Magnet autonomía en la gestión de su certificación ISO 27001.

Los objetivos específicos del proyecto incluyen:

- *Desarrollar una plataforma que permita la gestión eficiente de documentos, activos, riesgos y procesos asociados a los controles de ISO 27001:* Esto incluye la implementación de módulos especializados para cada uno de estos aspectos, asegurando una integración fluida y una fácil usabilidad.
- *Garantizar la escalabilidad y la adaptabilidad de la solución:* Utilizando tecnologías robustas como Django, PostgreSQL y TypeScript, se busca crear una base sólida que permita la evolución de la plataforma a medida que cambian las necesidades y los desafíos de seguridad.
- *Facilitar la certificación ISO 27001 para Magnet y otras organizaciones:* Proporcionando una herramienta que simplifica la gestión de la seguridad de la información y el cumplimiento normativo, se busca reducir los costos y el tiempo asociados con estos procesos.
- *Contribuir al fortalecimiento de la postura de seguridad informática de Magnet:* Al desarrollar una solución interna que se adapta específicamente a las necesidades de la empresa, se busca mejorar la protección de los activos digitales y la resiliencia ante amenazas ciberneticas.

En última instancia, este trabajo de título no se limita a resolver un problema específico de auditoría de cumplimiento del SGSI para Magnet; va más allá al buscar contribuir al panorama más amplio de la seguridad de la información. La plataforma propuesta no solo será una herramienta para alcanzar la certificación; será un activo estratégico que impulsa la seguridad, la adaptabilidad y la autonomía en un entorno empresarial digital en constante evolución. A medida que el proyecto avance, se espera que sus resultados no solo beneficien a Magnet, sino que también sirvan como un referente valioso para otras organizaciones que buscan fortalecer su postura en seguridad informática en un mundo cada vez más interconectado.

1.4. Descripción general de la solución

El sistema desarrollado tiene como objetivo principal facilitar la gestión del Sistema de Gestión de Seguridad de la Información (SGSI) de una empresa, siguiendo las buenas prácticas definidas en los controles que fija el estándar ISO 27001. La solución está estructurada en varios módulos, cada uno diseñado para cubrir aspectos específicos del SGSI: documentos, activos, riesgos y procesos. A continuación se presenta una descripción general de cada módulo y sus funcionalidades clave:

1.4.1. Módulo de Documentos

Este módulo centraliza la gestión de todos los documentos relevantes para el SGSI. Los documentos pueden ser políticas, procedimientos, registros y otros tipos de documentación necesarios para demostrar la conformidad con el estándar ISO 27001. Las funcionalidades incluyen:

- Creación, edición y eliminación de documentos.
- Versionado de documentos para mantener un registro histórico.
- Aprobación de versiones de documentos.
- Vinculación de documentos con controles específicos del SGSI.
- Gestión de la evidencia asociada a los documentos.

1.4.2. Módulo de Activos

Este módulo permite registrar y gestionar todos los activos de la empresa que son críticos para la seguridad de la información. Los activos pueden ser hardware, software, datos, personas, entre otros. Las funcionalidades incluyen:

- Creación, edición y eliminación de activos.
- Clasificación de activos por tipo.
- Asignación de roles a los activos para definir responsabilidades.
- Evaluación y actualización del estado de los activos.

1.4.3. Módulo de Riesgos

Este módulo está diseñado para identificar, evaluar y gestionar los riesgos asociados a los activos de la empresa. Cada riesgo está relacionado con un control específico del SGSI. Las funcionalidades incluyen:

- Identificación y registro de riesgos.
- Evaluación de la severidad y probabilidad de los riesgos.
- Asignación de responsables y tratamientos para cada riesgo.
- Monitoreo y actualización del estado de los riesgos.

1.4.4. Módulo de Procesos

Este módulo define y gestiona los procesos necesarios para cumplir con los controles del SGSI. Un proceso está compuesto por una serie de actividades que deben realizarse para generar evidencia de cumplimiento. Las funcionalidades incluyen:

- Definición de procesos y sus versiones.

- Asignación de actividades a grupos y usuarios.
- Gestión de la recurrencia y notificaciones de actividades.
- Monitoreo del cumplimiento de las actividades y generación de evidencia.

1.4.5. Tecnologías Utilizadas

La solución utiliza una combinación de tecnologías robustas y escalables, incluyendo:

- *Django*: Framework principal para el desarrollo del backend.
- *PostgreSQL*: La gestión de la base de datos.
- *Docker*: La contenedorización y despliegue de la aplicación.
- *TypeScript*: El desarrollo del frontend, mejorando la mantenibilidad del código.
- *Redis y Celery*: La gestión de tareas en segundo plano.
- *Nginx y Gunicorn*: El manejo eficiente de solicitudes web.

1.4.6. Arquitectura de Despliegue

El despliegue de la solución se realiza en contenedores Docker, lo que facilita su escalabilidad y mantenimiento. La infraestructura incluye:

- *Nginx*: El manejo de solicitudes HTTP/HTTPS.
- *Gunicorn*: Servir la aplicación Django.
- *Redis*: La caché y gestión de colas de tareas.
- *PostgreSQL*: El almacenamiento de datos.
- *Amazon S3*: El almacenamiento de archivos estáticos y de medios.

1.4.7. Escalabilidad y Rendimiento

La solución está diseñada para ser escalable, permitiendo la replicación de contenedores detrás de un balanceador de carga según sea necesario. La base de datos PostgreSQL y su capacidad de escalabilidad vertical y uso de réplicas para lectura aseguran un rendimiento eficiente incluso con aumentos en la carga de datos.

1.4.8. Seguridad y Cumplimiento

La seguridad es una prioridad en el diseño de la solución, con medidas como la verificación SHA-256 para archivos y la gestión de permisos detallada para usuarios y roles. La solución facilita el cumplimiento con el estándar ISO 27001, proporcionando las herramientas necesarias para la gestión de la seguridad de la información y la generación de evidencia para auditorías.

En resumen, la solución desarrollada proporciona una plataforma integral para la gestión del SGSI, alineada con el estándar ISO 27001, y ofrece a Magnet una herramienta estratégica para asegurar la conformidad y fortalecer su postura de seguridad informática.

Capítulo 2

Situación actual

Hoy en día existen programas capaces de manejar la auditoría 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, una solución de software como servicio, y Gapps, una solución de código abierto.

2.1. MyLenio

Entre las opciones SaaS, se encuentra MyLenio¹, una plataforma que se compone de 3 principales módulos, «organización del equipo», «recursos humanos» y «cumplimiento y seguridad».

2.1.1. Organización del equipo

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.

¹<https://www.mylenio.com/>

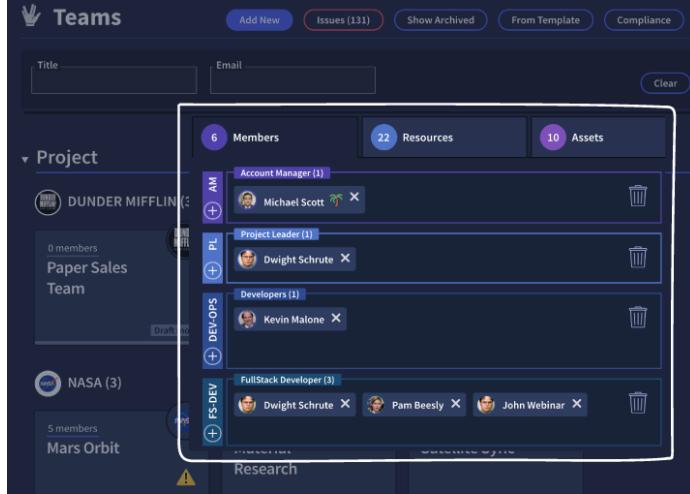


Figura 1: Organización de equipos en MyLenio

2.1.1.1. Manejo de permisos

Dentro de cada equipo se puede 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 fácil el proceso de incorporación de nuevos miembros a los equipos. Entre los SaaS se encuentran Bitbucket, DocuSign, GitHub, GitLab, Google Workspace, Jira, Keeper password, Office 365, Slack y Trello [1].

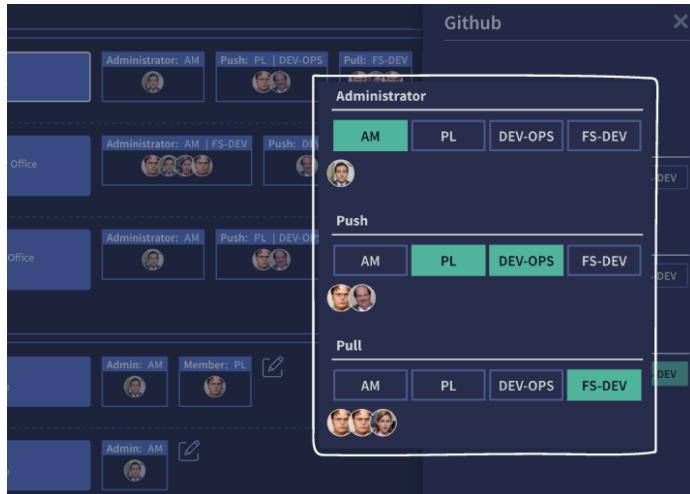


Figura 2: Manejo de permisos en MyLenio

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 a los empleados que aún no la han completado. Análogamente, se le pueden asignar tareas a los empleados y notificarlos para que las terminen [1].

The screenshot displays the MyLenio interface. At the top, there's a summary bar with counts for Owned Flows (5/6), Overdue (16), Pending (2), Pending Requests (3), and Active (1). Below this, a 'Task Requests' section shows 5 pending requests. Further down, there are sections for Holiday Requests (4 pending, 1 active) and a list of tasks. On the right side, there's a detailed view of an 'Onboarding DOC' entry, including fields for Name (Onboarding DOC), Approval required (checked), Label for link, Link Url, and Expiration days (15).

Figura 3: Documentos, capacitaciones y tareas en MyLenio

2.1.2. Recursos humanos

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 Google Workspace 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].

This screenshot shows the 'Onboarding' section of the MyLenio platform. It displays a list of steps for 'Onboarding Argentina Branch - Pablo Fernandez'. The steps are numbered 1 to 4: 1. Send Hire information, 2. Create a Google Account, 3. Create My Lenio Account, and 4. Coordinate to Open Bank Account. Each step has a status indicator (green circle with a checkmark) and a set of icons for edit, delete, message, and info.

Figura 4: Incorporación de empleados en MyLenio

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].

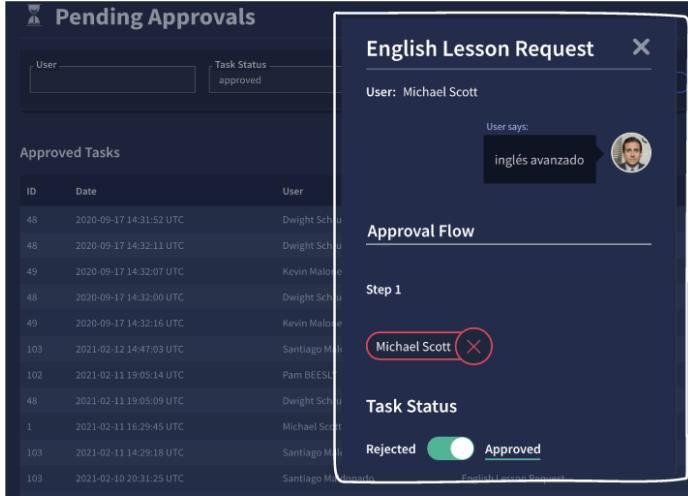


Figura 5: Participación y eficiencia del equipo en MyLenio

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].

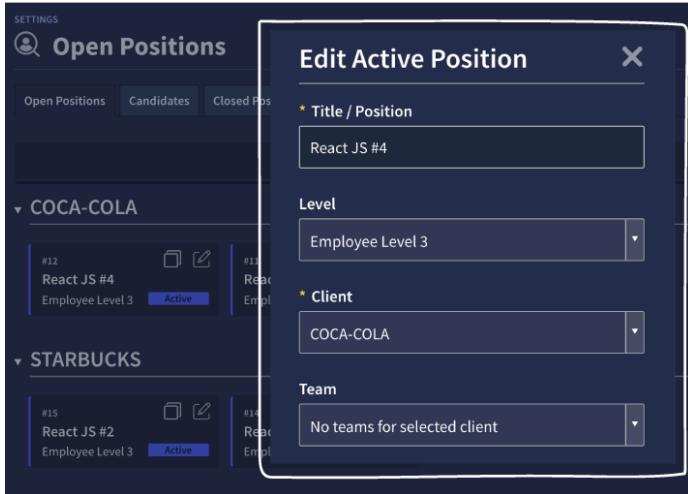


Figura 6: Reclutamiento en MyLenio

2.1.2.4. Información de los empleados

La información de cada empleado es guardada en Google Workspace 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].

The screenshot shows the 'Users' section of the MyLenio interface. On the left, there's a search bar for 'Name' and 'Country', and a dropdown for 'Sort By'. A checkbox for 'Pending Laptop' is checked. Below this is a table with columns 'Name', 'Compliant', and 'Status'. The table lists eight users: AS test, Dwight Schrute, Kevin Malone, Michael Scott, Pam BEESLY, Santiago Maldonado, and Test Prod. Each row shows their UP (1), PC (5), AP (2) counts and their status as ACTIVE. On the right, a large modal window titled 'User Info' displays various details for a selected user. It includes fields for 'gSuite Account: NO', 'Employee: YES', 'Compliant: NO', 'Contract: NO', 'Status: ACTIVE', 'Invited date: 21/12', 'Tenure: < 1 YEAR', and a birthday field set to '12/09/1888'.

Figura 7: Información de los empleados en MyLenio

2.1.3. Cumplimiento y seguridad

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

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 [3].

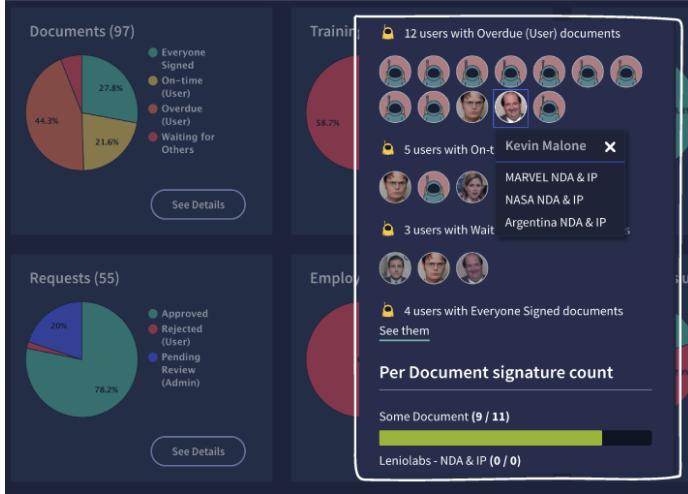


Figura 8: Reporte de cumplimiento en tiempo real en MyLenio

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 [3].

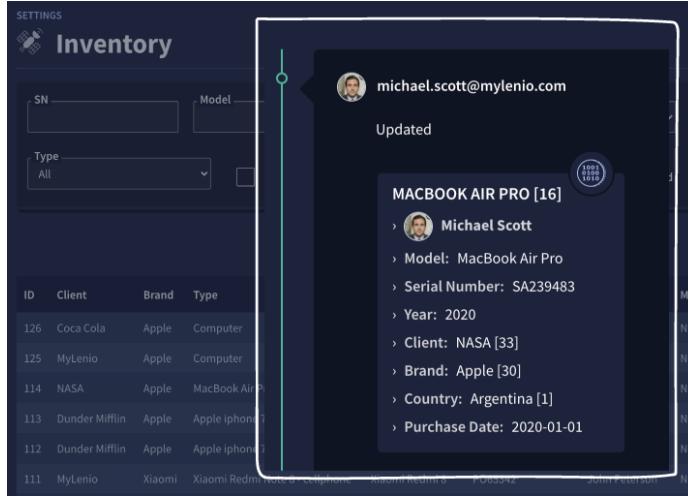


Figura 9: Manejo de Inventario en MyLenio

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 [3].

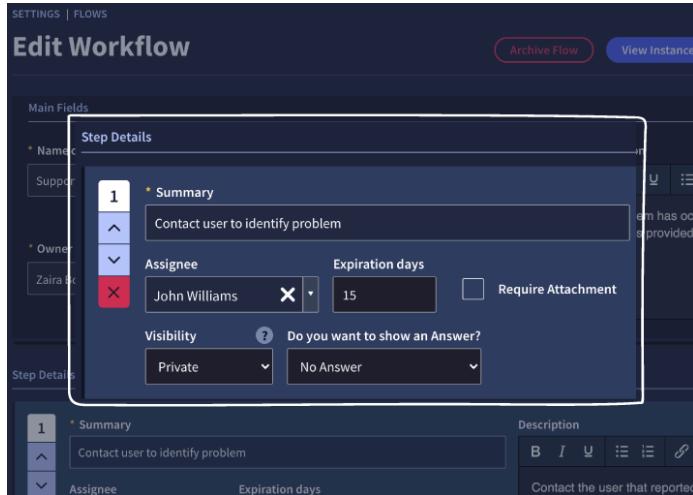


Figura 10: Modelamiento de procesos en MyLenio

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 [3].

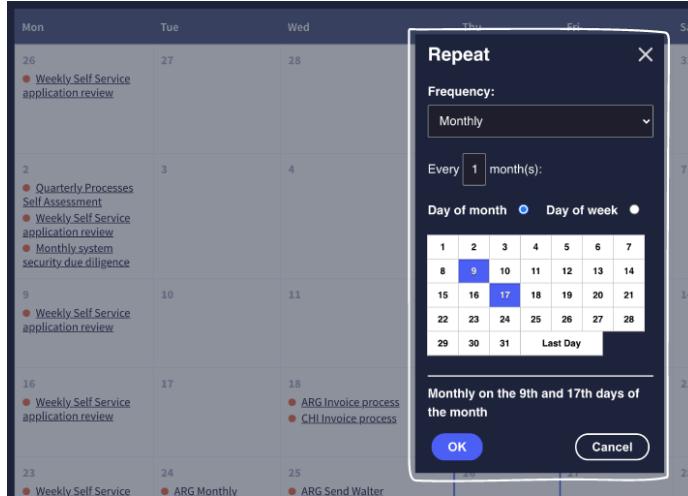


Figura 11: Eventos recurrentes y automatización de cumplimiento en MyLenio

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) [3].

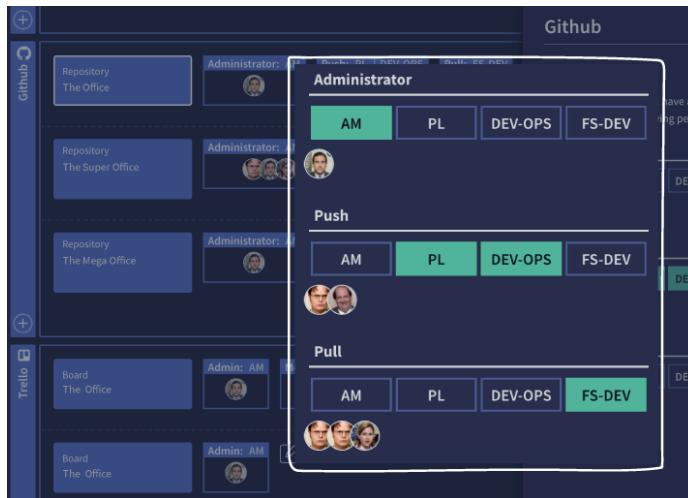


Figura 12: Manejo de riesgos en MyLenio

2.2. Gapps

Gapps² es una plataforma de cumplimiento de seguridad que facilita el seguimiento de su progreso en relación con varios marcos de seguridad. Actualmente, el proyecto se encuentra en modo Alfa, lo que significa que, aunque funciona bien, puede haber algunos cambios importantes a medida que evoluciona. El principal contribuyente al proyecto, Brendan Marshall, desaconseja su uso en entornos de producción [4].

²<https://github.com/bmarsh9/gapps>

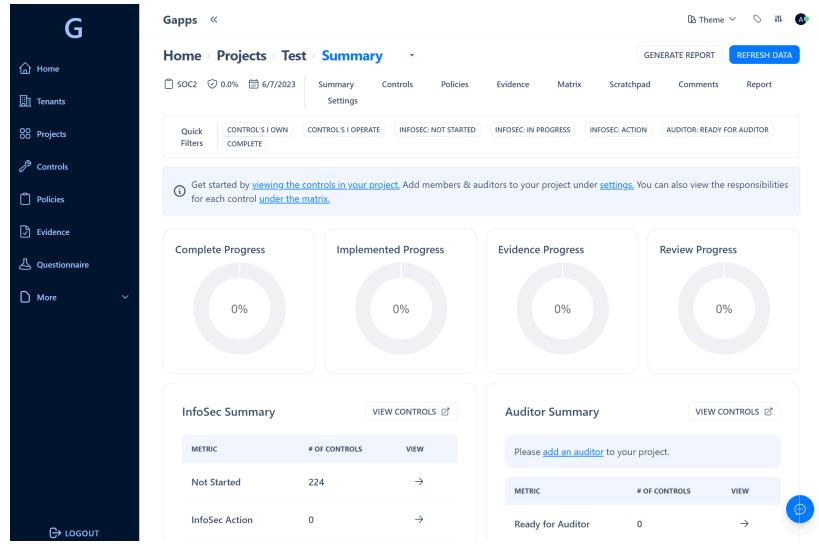


Figura 13: Vista de resumen en Gapps

Gapps ofrece soporte para más de 10 marcos de cumplimiento de seguridad, incluyendo SOC2, CMMC, ASVS, ISO27001, HIPAA, NIST CSF, NIST CSF, NIST 800-53, CSC CIS 18, PCI DSS. Además, cuenta con más de 1500 controles y más de 25 políticas, lo que permite recopilar evidencia para luego visualizarla en un panel de control [4].

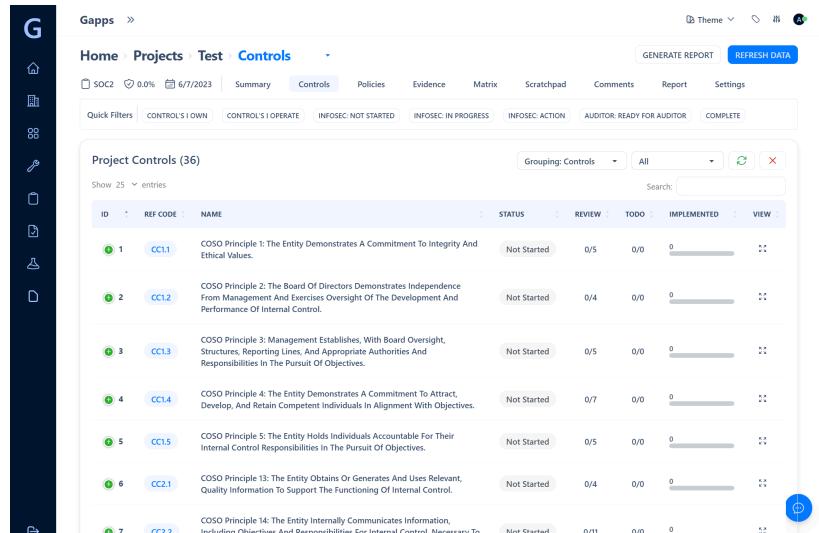


Figura 14: Controles en Gapps

Una característica destacada de Gapps es su capacidad para agregar controles y políticas personalizados. También ofrece un editor de contenido WYSIWYG (What You See Is What You Get, lo que ves es lo que obtienes) y cuestionarios para proveedores. Además, Gapps ha introducido recientemente la capacidad de añadir evidencia directamente a la plataforma [4].

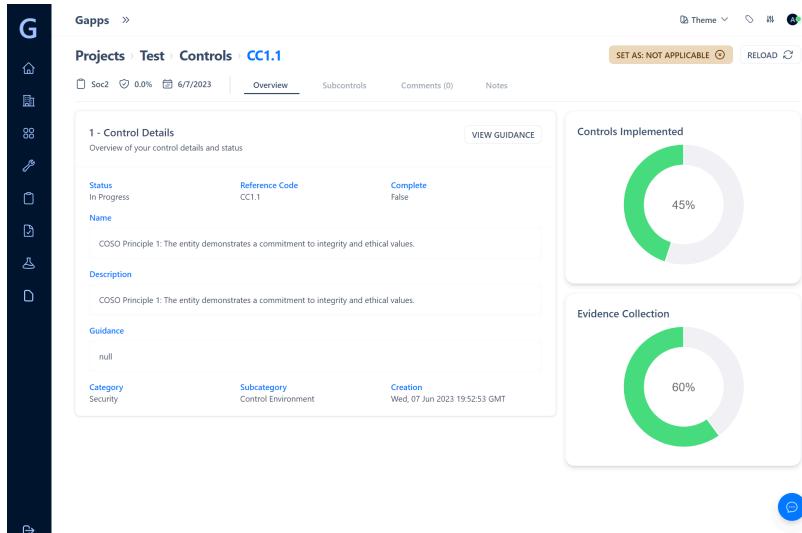


Figura 15: Control en Gapps

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 [4].

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.

2.3. 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 períodos 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 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.

Capítulo 3

Solución

El sistema desarrollado tiene como objetivo principal facilitar la gestión del Sistema de Gestión de Seguridad de la Información (SGSI) de una empresa. Para lograr esto, se han definido varios módulos, cada uno con su conjunto de funcionalidades específicas.

3.1. Tecnologías escogidas

La solución 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.

La elección de Django junto con HTML y CSS se justifica por la naturaleza estática de los datos, donde los cambios no son frecuentes. En este contexto, una biblioteca de frontend como React no aportaría un beneficio significativo, ya que la actualización dinámica de la

interfaz de usuario no es una prioridad, lo que hace que la simplicidad y la eficiencia de HTML y CSS sean suficientes para cumplir con los requisitos del proyecto.

3.2. Django Project Template (DPT)

Django Project Template™ (DPT) está diseñado para ser un punto de partida eficiente para el desarrollo de aplicaciones web en Django dentro de Magnet. La arquitectura de despliegue de DPT está bien definida para asegurar un entorno de desarrollo y producción robusto, especialmente útil para usuarios nuevos o aquellos que migran de versiones anteriores.

3.2.1. Tecnologías Utilizadas en DPT

Django Project Template™ incorpora una variedad de tecnologías para garantizar un desarrollo eficiente y un despliegue robusto. A continuación se describen algunas de las tecnologías clave:

- *Django*: El marco principal para el desarrollo de aplicaciones web. Ofrece una arquitectura robusta y escalable para el backend.
- *Python*: Lenguaje de programación utilizado para desarrollar aplicaciones Django.
- *Docker*: Plataforma para desarrollar, enviar y ejecutar aplicaciones dentro de contenedores, facilitando la gestión y la escalabilidad.
- *Docker Compose*: Herramienta para definir y ejecutar aplicaciones Docker multicontenedor, simplificando la configuración y el despliegue.
- *Nginx*: Servidor web y proxy inverso utilizado para manejar y redirigir las solicitudes HTTP/HTTPS.
- *Gunicorn*: Servidor WSGI que se utiliza para servir aplicaciones Django.
- *Redis*: Almacenamiento en memoria utilizado para la caché y como broker de mensajes para Celery.
- *Celery*: Librería de Python para ejecutar tareas en segundo plano y programadas.
- *PostgreSQL*: Sistema de gestión de bases de datos relacional utilizado para almacenar datos de la aplicación.
- *Amazon S3*: Servicio de almacenamiento en la nube utilizado para almacenar archivos estáticos y de medios.
- *TypeScript*: Un superconjunto de JavaScript que se utiliza para escribir código frontend más robusto y mantenible.
- *Bootstrap*: Framework de diseño frontend utilizado para crear interfaces de usuario responsivas y modernas.

3.2.2. Arquitectura de Infraestructura

La infraestructura de despliegue de DPT se basa en varios componentes containerizados que dependen entre sí. Esto facilita la escalabilidad, la mantenibilidad y el despliegue en entornos de nube. Los componentes principales son:

1. *Nginx*: Actúa como servidor web y proxy inverso, manejando las solicitudes del usuario y redirigiéndolas a la aplicación Django.
2. *Django*: Ejecuta la aplicación web a través del servidor WSGI de Gunicorn.
3. *Redis*: Proporciona servicios de caché y broker de mensajes.
4. *Celery*: Ejecuta tareas en segundo plano y programadas.
5. *PostgreSQL*: Servidor de base de datos.

Estos componentes se comunican a través de una red configurada por Docker Compose, lo que permite una configuración coherente y un despliegue sencillo.

La siguiente figura muestra un diagrama detallado de la arquitectura de despliegue utilizando Docker Compose. En ella se puede observar cómo interactúan entre sí los diferentes componentes, proporcionando una visión clara de cómo se gestionan las solicitudes y tareas dentro del sistema.

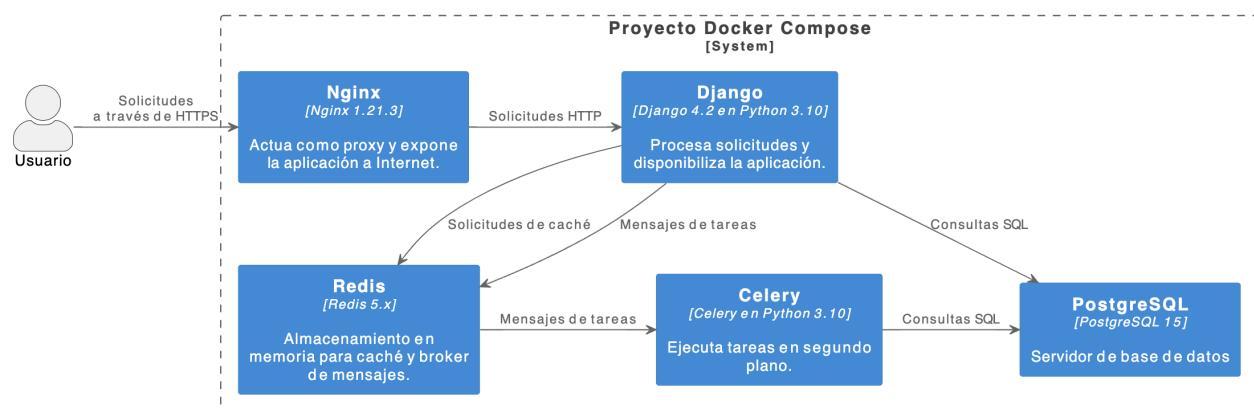


Figura 16: Diagrama de la arquitectura utilizando Docker Compose

3.2.2.1. Despliegue

Para proyectos basados en DPT, la arquitectura de despliegue en DigitalOcean consiste en ejecutar todos los servicios en una sola instancia de Droplet. Además, de ser necesario se puede tener un servicio de almacenamiento de datos en la nube. En este caso se tienen los siguientes elementos:

- *Droplet de DigitalOcean*: Una instancia en la nube donde se ejecutan todos los servicios containerizados (Nginx, Django, Redis, Celery, PostgreSQL).
- *Amazon S3*: Utilizado para almacenar archivos estáticos y de medios, lo que facilita la gestión y el escalado del almacenamiento de archivos.

3.2.2.2. Ventajas de esta Arquitectura

- *Simplicidad*: Ejecutar todos los servicios en un solo Droplet simplifica la gestión y el despliegue.
- *Escalabilidad*: Almacenar archivos en Amazon S3 permite escalar el almacenamiento independientemente de la capacidad del Droplet.
- *Mantenibilidad*: Utilizar Docker Compose facilita la configuración y la actualización de los servicios.

- *Costo-eficiencia:* Mantener una infraestructura sencilla reduce los costos operativos y facilita el monitoreo y la administración.

Esta configuración es ideal para aplicaciones con una carga de tráfico moderada, proporcionando un equilibrio entre simplicidad, eficiencia y escalabilidad.

3.3. Perfiles de usuario del sistema

La plataforma desarrollada para la gestión del Sistema de Gestión de Seguridad de la Información (SGSI) está diseñada para ser utilizada por diferentes perfiles de usuario, cada uno con roles y responsabilidades específicas. Esta organización en perfiles asegura que cada usuario tenga acceso a la información y las funcionalidades que necesita para desempeñar sus tareas, mientras se mantiene la seguridad y la integridad del sistema. Los dos perfiles principales de usuario en el sistema son el perfil de colaborador y el perfil de administrador.

3.3.1. Colaborador

El perfil de colaborador está diseñado para los empleados de la empresa que deben seguir las directrices del SGSI. Los colaboradores tienen acceso para ver toda la información relevante en la aplicación, pero sus permisos de edición están limitados a ciertas acciones específicas como marcar como leídas las versiones de los documentos y participar en los procesos asignados.

1. *Acceso a la Información:* Los colaboradores pueden ver toda la información del SGSI, incluyendo documentos, activos, riesgos y procesos.
2. *Lectura de Documentos:* Los colaboradores pueden acceder y leer los documentos del SGSI. Pueden marcar las versiones de documentos como leídas, registrando que han revisado la información necesaria.
3. *Participación en Procesos:* Los colaboradores pueden participar en los procesos asignados, realizando las actividades correspondientes y generando evidencia según sea necesario.

En resumen, los colaboradores juegan un papel crucial en el cumplimiento del SGSI al mantenerse informados y participar activamente en los procesos, aunque sin permisos para editar o gestionar información del sistema.

3.3.2. Administrador

El perfil de administrador está destinado a los encargados de implementar, mantener y gestionar el SGSI. Los administradores tienen permisos completos dentro del sistema, lo que incluye la creación y edición de documentos, la gestión de activos y riesgos, y la generación de evidencia. Además, los administradores también actúan como colaboradores, siguiendo las mismas directrices y participando en los procesos necesarios.

1. *Gestión de Controles y Categorías:* Los administradores pueden crear y organizar controles de seguridad y sus respectivas categorías.

2. *Subir y Versionar Documentos:* Los administradores pueden subir nuevos documentos, versionar documentos existentes y mantener un registro de las modificaciones.
3. *Aprobar Documentos:* Los administradores tienen la capacidad de aprobar documentos, asegurando su validez y conformidad con los estándares del SGSI.
4. *Gestión de Activos y Riesgos:* Los administradores pueden registrar y clasificar activos, asignar riesgos y definir los controles necesarios para mitigarlos.
5. *Definir y Supervisar Procesos:* Los administradores pueden crear y gestionar procesos, asignar actividades a los colaboradores y supervisar el cumplimiento de los procesos definidos.
6. *Generación y Gestión de Evidencia:* Los administradores pueden crear, modificar y gestionar la evidencia necesaria para demostrar la implementación y efectividad de los controles de seguridad.
7. *Auditoría y Cumplimiento:* Los administradores pueden revisar la evidencia generada, asegurar la conformidad con las políticas de seguridad y preparar el SGSI para auditorías internas y externas.

En resumen, los administradores desempeñan un papel integral en la gestión del SGSI, asegurando que todos los aspectos del sistema sean implementados y mantenidos de acuerdo con los estándares de seguridad establecidos. Además de sus amplias capacidades de gestión, también participan activamente como colaboradores en los procesos definidos.

3.4. Módulo de Usuarios

El módulo de usuarios es donde se guarda la información de los usuarios de la aplicación. Ya que el módulo de usuarios depende del módulo de autenticación proveído por Django, se agregan algunos modelos relacionados acá. Para más detalles sobre la estructura de la base de datos y la relación entre las entidades, consulte la Sección 6.1. del anexo.

3.4.1. Historias de Usuario

1. Como administrador, quiero poder crear, editar, ver y listar los usuarios de la plataforma.
2. Como administrador, quiero poder crear, editar, ver y listar los grupos de la plataforma.
3. Como administrador, deseo tener la capacidad de asignar grupos a los usuarios y, de igual manera, asignar usuarios a grupos.

3.4.2. Interfaz de usuario

La interfaz de usuario del módulo de usuarios está diseñada para ser intuitiva y facilitar la gestión de usuarios y grupos dentro de la aplicación. A continuación, se presenta una descripción del flujo típico que un administrador seguiría al utilizar las vistas más importantes del módulo de usuarios.

El primer paso en el uso de la aplicación es el inicio de sesión. La aplicación presenta una interfaz de inicio de sesión diseñada para ser segura y accesible. Para Magnet, el inicio

de sesión se realiza a través de Google Workspace, proporcionando una integración fluida con los servicios de Google. Esto simplifica el proceso para los usuarios que ya están familiarizados con el entorno de Google. Sin embargo, la flexibilidad de la aplicación permite cambiar el método de autenticación mediante variables de entorno, permitiendo el uso de email y contraseña como alternativa. Esta configuración es útil en entornos donde el uso de Google Workspace no es adecuado o preferido. Además, el registro de usuarios está estrictamente controlado. Solo los administradores de la aplicación pueden crear nuevas cuentas, lo que evita que usuarios externos se registren sin autorización. No obstante, el registro de usuarios externos también puede ser gestionado mediante variables de entorno, permitiendo configuraciones más abiertas si es necesario. Este enfoque garantiza un control preciso sobre quién puede acceder a la aplicación, mejorando la seguridad y la gestión de usuarios.

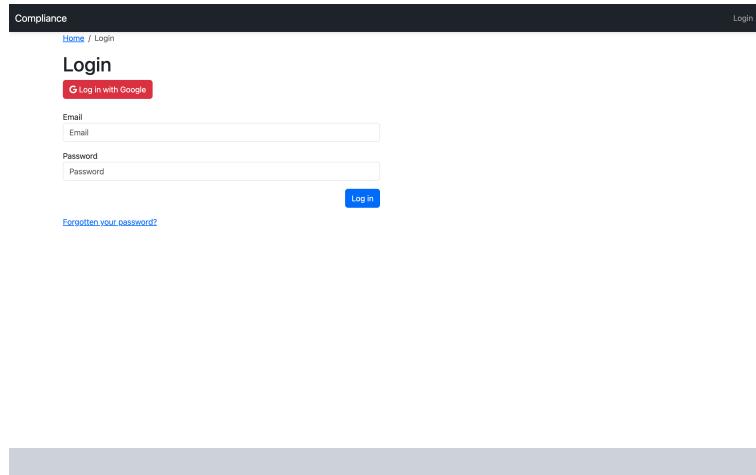


Figura 17: Vista de inicio de sesión

Una vez autenticado, el administrador accede a la vista de listado de usuarios. Esta vista proporciona una tabla con información detallada sobre cada usuario, incluyendo su nombre, dirección de correo electrónico, grupos y estado de la cuenta. Esta vista está diseñada para ser intuitiva y fácil de navegar, permitiendo a los administradores realizar varias acciones importantes: visualización y búsqueda, creación, edición, visualización de detalles y eliminación de usuarios.

Compliance		Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Users							
<h2>Users</h2>							
Name	Email	Is active	Groups				
Gabriel Rojas Chamorro	gabriel.rojas@magnet.cl	Yes	Employee, Administrator				Update user Delete user
1	Showing results from 1 to 1 Total: 1						

Figura 18: Vista de listado de usuarios

Al crear un nuevo usuario, el administrador accede a la vista de creación de usuarios. Esta interfaz incluye campos para ingresar el nombre, apellido, dirección de correo electrónico, estado de actividad y asignación de grupos al usuario. Los botones de acción permiten guardar el nuevo usuario o cancelar la creación y volver a la vista anterior.

Compliance		Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Users / Create user							
<h3>Create user</h3>							
<small>First name (optional)</small>							
<input type="text"/>							
<small>Last name (optional)</small>							
<input type="text"/>							
<small>Email address</small>							
<input type="text"/>							
<small>Active</small>							
<input checked="" type="checkbox"/> Active							
<small>Designates whether this user should be treated as active. Unselect this instead of deleting accounts.</small>							
<small>Groups (optional)</small>							
<input type="text"/> Employee							
<small>The groups this user belongs to. A user will get all permissions granted to each of their groups.</small>							
Save Cancel							

Figura 19: Vista de creación de usuario

La vista de actualización de usuario permite a los administradores editar la información de un usuario existente, como el nombre, apellido, dirección de correo electrónico, estado de actividad y grupos asignados. Los botones de acción permiten guardar los cambios realizados o cancelar la edición y volver a la vista anterior.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Home / Users / gabriel.rojas@magnet.cl / Update gabriel.rojas@magnet.cl

Update gabriel.rojas@magnet.cl

First name (optional)
Gabriel

Last name (optional)
Rojas Chamorro

Email address
gabriel.rojas@magnet.cl

Active

Designates whether this user should be treated as active. Unselect this instead of deleting accounts.

Groups (optional)

Employee Administrator

The groups this user belongs to. A user will get all permissions granted to each of their groups.

Save **Cancel**

Figura 20: Vista de actualización de usuario

Para ver y gestionar información específica de cada usuario, el administrador accede a la vista de detalle de usuario. Esta vista muestra información personal del usuario, como nombre, apellido, correo electrónico y estado de actividad, así como los grupos asignados al usuario. Los botones de acción permiten actualizar la información del usuario, eliminar al usuario de la aplicación, modificar los detalles del grupo asignado o eliminar el grupo de la aplicación.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Home / Users / User: Gabriel.Rojas@magnet.Cl

User: Gabriel.Rojas@magnet.Cl

Update user **Delete user**

First name	Gabriel
Last name	Rojas Chamorro
Email	gabriel.rojas@magnet.cl
Is active	Yes

Assigned groups

Name	Users	Permissions
Employee	1	20
Administrator	1	80

Update group **Delete group**

Update group **Delete group**

Figura 21: Vista de detalle de usuario

Además de gestionar usuarios, los administradores también pueden gestionar los grupos dentro de la aplicación. La vista de listado de grupos permite a los administradores ver y gestionar todos los grupos existentes, incluyendo información sobre el nombre del grupo, el número de usuarios y el número de permisos asociados al grupo. Los botones de acción permiten añadir nuevos grupos, actualizar grupos existentes y eliminar grupos con confirmación para evitar eliminaciones accidentales.

Groups		
Name	Users	Permissions
Administrator	1	68
Employee	1	17
Update group <input checked="" type="checkbox"/> Delete group Update group <input checked="" type="checkbox"/> Delete group		
Showing results from 1 to 2 Total: 2		

Figura 22: Vista de listado de grupos

Para más detalles sobre las demás vistas del módulo de usuarios consulte la Sección 6.2. del anexo.

3.5. Módulo de Documentos

El módulo de documentos es el repositorio central donde se guarda toda la información que define al SGSI. La información se puede dividir en controles, documentos y evidencia. Para más detalles sobre la estructura de la base de datos y la relación entre las entidades, consulte la Sección 6.3. del anexo.

3.5.1. Controles

Los controles de seguridad son medidas implementadas para proteger datos e infraestructuras críticas para una organización. Cualquier tipo de salvaguarda o contramedida utilizada para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad se considera un control de seguridad. Estos pueden incluir medidas técnicas como firewalls y antivirus, así como procedimientos y políticas como la formación de empleados y la gestión de accesos.

3.5.2. Categorías de Controles

Las categorías de controles son grupos de controles relacionados entre sí. Estas categorías permiten organizar y gestionar los controles de manera más efectiva, facilitando la identificación de áreas específicas de seguridad que necesitan ser abordadas. Ejemplos de categorías incluyen controles organizacionales, controles de personas, controles físicos y controles tecnológicos. Cada categoría abarca una serie de controles que cumplen con objetivos específicos dentro del SGSI.

3.5.3. Documentos

Los documentos son información registrada que respalda la implementación y gestión del SGSI. Pueden incluir políticas de seguridad, procedimientos operativos, registros de auditoría, planes de continuidad del negocio y cualquier otra información necesaria para mante-

ner y mejorar la seguridad de la información dentro de la organización. La correcta gestión de estos documentos es crucial para asegurar la conformidad con normas y regulaciones y para facilitar la revisión y mejora continua del SGSI.

3.5.4. Tipos de Documentos

Los tipos de documentos son categorías utilizadas para organizar la información dentro del SGSI. Cada tipo cumple un propósito específico, facilitando la gestión y asegurando la conformidad con los estándares de seguridad. Ejemplos de tipos de documentos incluyen políticas, procedimientos, registros, informes y manuales. La correcta clasificación y gestión de estos documentos es crucial para la eficacia del SGSI y la conformidad con normas y regulaciones.

3.5.5. Evidencia

La evidencia se refiere a la documentación y pruebas tangibles que demuestran la implementación y efectividad de los controles de seguridad. Puede incluir registros de auditoría, informes de incidentes, resultados de pruebas de seguridad, registros de capacitación del personal, entre otros. La recopilación y gestión adecuada de la evidencia es esencial para demostrar la conformidad con los requisitos del SGSI y para proporcionar una base sólida para auditorías internas y externas.

3.5.6. Historias de Usuario

1. Como administrador, quiero poder crear categorías de controles para agrupar controles relacionados.
2. Como administrador, quiero poder crear controles para definir mi marco de SGSI.
3. Como administrador, quiero poder cargar todas las categorías y controles de ISO 27001 a partir de una plantilla, para tener una base al momento de implementar cada control.
4. Como administrador, quiero poder subir documentos a cada control, para definir mi implementación de dicho control.
5. Como administrador, quiero que los documentos queden versionados, para saber qué versiones han sido leídas por los usuarios y mantener un registro de modificaciones.
6. Como administrador, quiero poder aprobar documentos, para validar su contenido.
7. Como usuario, quiero poder ver el listado de documentos.
8. Como usuario, quiero poder ver el detalle de cada documento.
9. Como usuario, quiero poder ver el listado de controles.
10. Como usuario, quiero poder ver el detalle de cada control.
11. Como usuario, quiero poder ver el detalle de cada documento.
12. Como usuario, quiero poder marcar como leída una versión de un documento.
13. Como administrador, necesito poder generar enlaces de solo lectura para las versiones de documentos utilizando el código del documento y su número de versión.
14. Como usuario, quiero poder ver el listado de tipos de documentos.
15. Como usuario, quiero poder ver el detalle de cada tipo de documento.
16. Como administrador, quiero poder crear nuevos tipos de documentos.
17. Como administrador, quiero poder editar los tipos de documentos existentes.

18. Como administrador, quiero poder eliminar tipos de documentos que ya no son necesarios.

3.5.7. Interfaz de Usuario

El flujo típico de un usuario en el módulo de documentos comienza con la vista de listado de controles, donde puede visualizar todos los controles de seguridad definidos en el SGSI. Esta vista es fundamental para mantener una organización clara y accesible de los controles, facilitando su gestión y revisión.

The screenshot shows a web-based application interface for managing controls. At the top, there is a navigation bar with links for Compliance, Accounts, Documents, Assets, Risks, and Processes. A user is logged in as gabriel.rojas@magnet.cl. Below the navigation, the URL is Home / Controls. The main title is 'Controls'. On the right, there is a button labeled 'Add control +'. The table below lists one control entry:

Name	Category	Updated at	Updated by
Control_1	Control_Category_1	May 29, 2024, 12:33 p.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

At the bottom of the table, there are buttons for 'Update control' and 'Delete control'. Below the table, a message indicates 'Showing results from 1 to 1 Total: 1'.

Figura 23: Vista de listado de controles

Desde aquí, un administrador puede acceder a la vista de creación de controles, donde puede definir nuevos controles de seguridad dentro del SGSI. Esta función es fundamental para asegurar que todas las medidas necesarias para proteger la información de la organización estén claramente documentadas y gestionadas.

The screenshot shows a 'Create control' form. At the top, there is a navigation bar with links for Compliance, Accounts, Documents, Assets, Risks, and Processes. A user is logged in as gabriel.rojas@magnet.cl. Below the navigation, the URL is Home / Controls / Create control. The main title is 'Create control'. The form has three input fields: 'Category (optional)' with a dropdown menu, 'Title' with a text input field, and 'Description (optional)' with a large text area. At the bottom, there are two buttons: 'Save' (blue) and 'Cancel' (red).

Figura 24: Vista de creación de controles

Una vez creado un control, los usuarios pueden ver toda la información relevante sobre un control específico en la vista de detalle de controles. Esta vista incluye secciones para mostrar los documentos, riesgos relacionados y evidencias asociadas al control.

Compliance Accounts Documents Assets Risks Processes

Logged in as gabriel.rojas@magnet.cl

[Home](#) / [Controls](#) / Control: Control 1

Control: Control 1

Category	Control_Catgeory_1
Title	Control 1
Description	
Created at	May 29, 2024, 12:33 p.m.
Created by	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)
Updated at	May 29, 2024, 12:33 p.m.
Updated by	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Documented in

Name	Last approved version	Last version	Updated at	Updated by
------	-----------------------	--------------	------------	------------

Related risks

Name	Updated at	Updated by
------	------------	------------

Evidences

Name	Evidence	Created at	Created by
------	----------	------------	------------

Figura 25: Vista de detalle de controles

Si es necesario actualizar la información de un control existente, el administrador puede acceder a la vista de actualización de controles, donde puede editar los detalles del control.

Compliance Accounts Documents Assets Risks Processes

Logged in as gabriel.rojas@magnet.cl

[Home](#) / [Controls](#) / [Control 1](#) / Update Control 1

Update Control 1

Category (optional)	Control_Catgeory_1
Title	Control 1
Description (optional)	

Save **Cancel**

Figura 26: Vista de actualización de controles

Para gestionar las categorías de controles, el administrador puede utilizar la vista del listado de categorías de controles, que proporciona una tabla con información sobre cada categoría de control.

Compliance		Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Control Categories							
<h2>Control Categories</h2>							

Name	Updated at	Updated by	
Control Category_1	May 29, 2024, 12:33 p.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)	Update control category  Delete control category 

Showing results from 1 to 1
Total: 1

1

Figura 27: Vista de listado de categorías de controles

Desde esta vista, puede acceder a la creación de nuevas categorías de controles o editar las existentes, facilitando la organización y gestión de los controles.

Compliance	Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Control categories / Create control category						
<h3>Create control category</h3>						
<input type="text" value="Name"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>						

Figura 28: Vista de creación de categorías de controles

La gestión de documentos es otro aspecto crucial del SGSI. Los usuarios pueden comenzar con la vista del listado de documentos, que proporciona una tabla con información sobre cada documento, incluyendo su nombre, la última versión aprobada, la última versión, la fecha de actualización y el usuario que realizó la última actualización.

Compliance					Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Documents										
<h2>Documents</h2>										Add document +
<hr/>										
Name	Last approved version	Last version	Updated at	Updated by						
Document1	Document1 - V1	Document1 - V2	May 29, 2024, 10:49 a.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)	Update document	Delete document				
1										Showing results from 1 to 1 Total: 1

Figura 29: Vista de listado de documentos

Para añadir nuevos documentos, el administrador puede acceder a la vista de creación de documentos, donde se pueden ingresar detalles como el título, código, tipo de documento, descripción, carpeta en Drive y controles documentados.

Compliance		Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Documents / Create document							
<h3>Create document</h3>							
Title	<input type="text"/>						
Code	<input type="text"/>						
Document type (optional)	<input type="text"/> -----						
Description (optional)	<input type="text"/>						
Drive folder (optional)	<input type="text"/>						
Documented controls (optional)	<input type="text"/>						
Save Cancel							

Figura 30: Vista de creación de documentos

Una vez creado un documento, los usuarios pueden ver y el administrador gestionar toda la información específica del documento en la vista de detalle de documentos, asegurando que esté actualizado y correctamente gestionado.

Document: Document 1

Name	Author	Is Approved read	Updated at	Updated by
Document 1 - Gabriel Rojas Chamorro V2	(gabriel.rojas@magnet.cl)	No	June 17, 2024, 1:36 a.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)
Document 1 - Gabriel Rojas Chamorro V1	(gabriel.rojas@magnet.cl)	Yes	June 14, 2024, 10:56 a.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Figura 31: Vista de detalle de documentos

Para mantener un registro actualizado y detallado de todas las versiones de los documentos, el administrador puede utilizar la vista de creación de versiones de documentos, donde se pueden añadir nuevas versiones a un documento existente.

Create document version

Author:

File (optional): Choose File No file chosen

File url (optional):

Comment (optional):

Figura 32: Vista de creación de versiones de documentos

El detalle de cada versión del documento también puede ser gestionado en la vista de detalle de versión de documentos, proporcionando información específica sobre cada versión, como el autor, comentarios, estado de aprobación y usuarios que han leído la versión.

The screenshot shows a detailed view of a document version. At the top, there's a header with 'Compliance' and other navigation links. Below it, the document title is 'Document Version: Document 1 - V1'. A 'Mark as read' button is visible. The main content includes a table with document metadata like 'Author' (Gabriel Rojas Chamorro), 'Version' (1), and 'File' (disc1.pdf). It also lists approval history with columns for 'Approved by' (Gabriel Rojas Chamorro) and 'Evidence for Document 1 - V1' (link). A 'Read by' section follows, with columns for 'Name' and 'Email'.

Figura 33: Vista de detalle de versión de documentos

Para aprobar una versión específica de un documento, el administrador puede acceder a la vista de aprobación de versiones de documentos, donde puede subir un archivo de evidencia, ingresar una URL o un texto como evidencia de la aprobación.

This screenshot shows the 'Approve document version' interface. It has a title 'Approve document version' and a sub-header 'Approve document version'. There are three input fields: 'Evidence file (optional)' with a 'Choose File' button, 'Evidence URL (optional)' with a text input field, and 'Text (optional)' with a text area. Below the fields are 'Approve' and 'Cancel' buttons.

Figura 34: Vista de aprobación de versión de documentos

Adicionalmente, la vista del listado de tipos de documentos muestra una tabla con los tipos de documentos existentes en el sistema. Los campos más relevantes incluyen el nombre del tipo de documento y la cantidad de documentos asociados a este tipo.

Compliance	Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Document Types						Add document type +
Document Types						

Name	Related documents	Actions
Document type 1	1	Update document type Delete document type

Showing results from 1 to 1
Total: 1

Figura 35: Vista de listado de tipos de documentos

Para agregar un nuevo tipo de documento, el administrador puede acceder a la vista de creación de tipos de documentos, donde se puede ingresar el nombre del tipo de documento.

Compliance	Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Document types / Create document type						Add document type +
Create document type						

Name	<input type="text"/>
------	----------------------

[Save](#) [Cancel](#)

Figura 36: Vista de creación de tipos de documentos

La vista de detalle de un tipo de documento muestra información específica sobre un tipo de documento en particular, facilitando la gestión de estos.

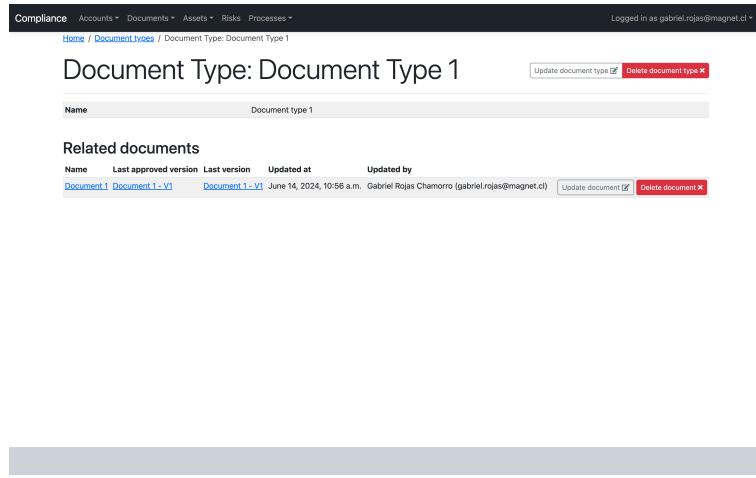


Figura 37: Vista de detalle de tipos de documentos

Para editar un tipo de documento existente, el administrador puede utilizar la vista de actualización de tipos de documentos, donde puede modificar el nombre del tipo de documento seleccionado.

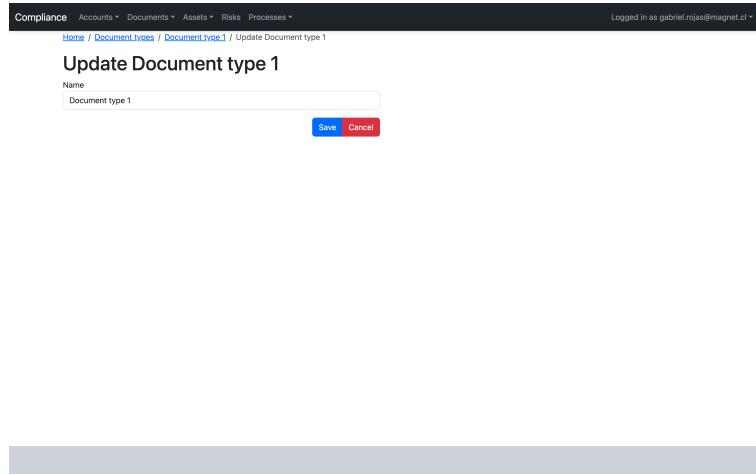


Figura 38: Vista de actualización de tipos de documentos

Finalmente, para gestionar la evidencia, los usuarios pueden acceder a la vista de detalle de evidencia, donde se muestra toda la información relevante de una evidencia.

The screenshot shows a software interface for managing compliance documents. At the top, there's a navigation bar with links for Compliance, Accounts, Documents, Assets, Risks, Processes, and Home/Evidence. The main title is "Evidence: Evidence For Document 1 - V1". Below the title, there's a table with the following data:

Approved document version	Document 1 - V1
Evidence	evidence
ShaSum	e3b0c42398fc1c149afbf4c899fb92427ae41e4649b934ca9599fb7852b855
Created at	June 14, 2024, 10:56 a.m.
Created by	gabriel.rojas@magnet.cl

Figura 39: Vista de detalle de evidencia

Este flujo de trabajo asegura que todos los documentos, controles y evidencias del SGSI estén organizados y gestionados de manera eficiente, facilitando la conformidad con las normas y regulaciones de seguridad de la información.

Para más detalles sobre otras vistas del módulo de documentos consulte la Sección 6.4. del anexo.

3.6. Módulo de Activos

El módulo de activos es donde se preserva un inventario con todos los activos de la empresa pertinentes a la seguridad de la información. Su principal componente son los activos y los roles de los activos. Para más detalles sobre la estructura de la base de datos y la relación entre las entidades, consulte la Sección 6.5. del anexo.

3.6.1. Activos

Los activos son cualquier recurso que sea valioso para la organización y que necesite protección. Pueden incluir hardware, software, datos, personas, instalaciones y cualquier otro elemento que pueda tener un impacto en la seguridad de la información.

3.6.2. Tipos de activos

Los tipos de activos son para poder clasificar a los activos por su tipo, por ejemplo, aplicaciones, equipos informáticos, oficinas, entre otros.

3.6.3. Roles de Activos

Los roles de activos son asignaciones específicas que definen las responsabilidades y permisos de los usuarios en relación con un activo particular. Este concepto permite una gestión granular y detallada de quién puede acceder y manejar cada activo, asegurando que solo las personas autorizadas tengan los permisos necesarios para interactuar con ellos.

3.6.4. Historias de Usuario

1. Como administrador, quiero poder registrar activos de la empresa, para luego definir su riesgo asociado.
2. Como administrador, quiero poder editar activos.
3. Como usuario, quiero poder ver el listado de activos.
4. Como usuario, quiero poder ver el detalle de cada activo.
5. Como administrador, quiero poder crear tipos de activos.
6. Como administrador, quiero poder editar tipos de activos.
7. Como usuario, quiero poder ver el listado de tipos de activos.
8. Como usuario, quiero poder ver el detalle de cada tipo de activo.
9. Como administrador, quiero poder crear roles de activos.
10. Como administrador, quiero poder editar roles de activos.
11. Como usuario, quiero poder ver el listado de roles de activos.
12. Como usuario, quiero poder ver el detalle de cada rol de activo.

3.6.5. Interfaz de usuario

El flujo típico de un usuario comienza con la vista de listado de activos, donde se pueden visualizar todos los activos registrados en el sistema. Esta vista es fundamental para mantener una organización clara y accesible de los activos, facilitando su gestión y revisión. Desde aquí, los administradores pueden agregar nuevos activos, actualizar los existentes o archivar aquellos que ya no son relevantes.

Figura 40: Vista de listado de activos

Al agregar un nuevo activo, el administrador ingresa información detallada como el nombre, código, propietario, tipo, criticidad y clasificación del activo. Esta información es esencial para mantener un registro completo y detallado de todos los activos de la organización.

The screenshot shows the 'Create asset' form in the Compliance application. It includes fields for Name, Code, Owner, Description (optional), Type, Criticality, and Classification. At the bottom are 'Save' and 'Cancel' buttons.

Figura 41: Vista de creación de activos

Una vez registrado, los usuarios pueden ver toda la información relevante sobre el activo en la vista de detalle de activos. Esta vista proporciona un desglose completo del activo, incluyendo su código, nombre, propietario, tipo, criticidad y clasificación.

The screenshot shows the 'Asset: Asset 1 - Gabriel Rojas Chamorro' detail view. It includes sections for General Information (Archived: No, Code: AS1, Name: Asset 1, Owner: Gabriel Rojas Chamorro, Description: -), Types (Asset type 1), Criticality (Medium), Classification (Internal), and History (Created at: June 17, 2024, 12:18 a.m., Created by: Gabriel Rojas Chamorro, Updated at: June 17, 2024, 12:18 a.m., Updated by: Gabriel Rojas Chamorro). It also shows Roles (Asset) and Related risks (No data to show).

Figura 42: Vista de detalle de activos

Si es necesario actualizar la información de un activo, el administrador accede a la vista de modificación de activos, donde puede editar los detalles existentes. Esta funcionalidad es crucial para asegurar que la información de los activos esté siempre actualizada y precisa.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Update Asset 1 - Gabriel Rojas Chamorro

Name
Asset 1

Code
AS1

Owner
Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Description (optional)

Types
Asset type 1

Criticality
Medium

Classification
Internal

Save **Cancel**

Figura 43: Vista de modificación de activos

Para gestionar los tipos de activos, los usuarios pueden utilizar la vista de listado de tipos de activos, que proporciona una tabla con información sobre cada tipo de activo. Desde esta vista, el administrador puede acceder a la creación de nuevos tipos de activos o a la edición de los existentes, facilitando la organización y clasificación de los activos.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Asset Types

Add asset type +

Name	Updated at	Updated by
Asset type 1	May 31, 2024, 9:38 a.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Showing results from 1 to 1
Total: 1

Update asset type **Delete asset type**

Figura 44: Vista de listado de tipos de activos

Al agregar un nuevo tipo de activo, el administrador ingresa el nombre del tipo de activo. Esta clasificación ayuda a organizar y gestionar los activos de manera más eficiente.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

[Home](#) / [Asset types](#) / Create asset type

Create asset type

Name

Description (optional)

Save Cancel

Figura 45: Vista de creación de tipos de activos

La vista de detalle de tipos de activos proporciona información específica sobre un tipo de activo en particular, permitiendo al administrador ver y gestionar todos los aspectos relacionados con ese tipo.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

[Home](#) / [Asset types](#) / Asset Type: Asset Type 1

Asset Type: Asset Type 1

[Update asset type](#) [Delete asset type](#)

Name	Asset type 1
Description	
Created at	June 17, 2024, 12:16 a.m.
Created by	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)
Updated at	June 17, 2024, 12:16 a.m.
Updated by	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Related assets

Code	Name	Owner	Types	Criticality	Classification	Archived	Updated at	Updated by	Action
A51	Asset 1	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)	Asset	Medium	Internal	No	June 17, 2024, 12:18 a.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)	Archive

[Update asset](#)

Figura 46: Vista de detalle de tipos de activos

Para actualizar un tipo de activo existente, el administrador accede a la vista de modificación de tipos de activos, donde puede cambiar el nombre del tipo de activo según sea necesario.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

[Home](#) / [Asset types](#) / [Asset type 1](#) / Update Asset type 1

Update Asset type 1

Name
Asset type 1

Description (optional)

Save Cancel

Figura 47: Vista de modificación de tipos de activos

La vista de roles de activos permite definir y asignar roles específicos a los activos dentro del sistema, lo que es esencial para establecer las responsabilidades y permisos adecuados para cada activo. Esta funcionalidad asegura que solo los usuarios autorizados puedan gestionar los activos.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

[Home](#) / Asset Roles

Asset Roles

Add asset role +

Name	Asset
Asset 1 - Asset role 1	Asset 1 - Gabriel Rojas Chomorlo

1

Showing results from 1 to 1
Total: 1

Update asset role Delete asset role

Figura 48: Vista de listado de roles de activos

Al agregar un nuevo rol de activo, el administrador selecciona el activo al cual se asignará el rol, ingresa el nombre del rol y, opcionalmente, asigna grupos de usuarios relacionados con este rol.

Figura 49: Vista de creación de roles de activos

La vista de detalle de roles de activos proporciona información detallada sobre un rol específico asignado a un activo, incluyendo los usuarios que tienen asignado dicho rol, lo que facilita la gestión de las responsabilidades y permisos.

Figura 50: Vista de detalle de roles de activos

Si es necesario modificar la información de un rol de activo, el administrador accede a la vista de actualización de roles de activos, donde puede cambiar el nombre del rol y actualizar la lista de usuarios asignados.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Home / Asset roles / Asset 1 - Asset role 1 / Update Asset 1 - Asset role 1

Update Asset 1 - Asset role 1

Name
Asset role 1

Users
gabriel.rojas@magnet.cl

Save Cancel

Figura 51: Vista de actualización de roles de activos

Para eliminar un rol de activo, la vista de eliminación de roles de activos permite confirmar la acción, asegurando que solo se realicen eliminaciones intencionales y evitando así errores.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Home / Asset roles / Asset 1 - Asset role 1 / Delete Asset 1 - Asset role 1

Delete Asset 1 - Asset role 1

Are you sure you want to delete "Asset 1 - Asset role 1"?

Confirm Cancel

Figura 52: Vista de eliminación de roles de activos

Este flujo de trabajo asegura que todos los activos, sus tipos y roles estén organizados y gestionados de manera eficiente, facilitando la conformidad con las normas y regulaciones de seguridad de la información.

Para más detalles sobre otras vistas del módulo de activos, consulte la Sección 6.6. del anexo.

3.7. Módulo de Riesgos

El módulo de riesgos es donde se gestiona y asigna un riesgo a cada uno de los activos, evaluando su gravedad y probabilidad. Su único componente es el riesgo. Para más detalles sobre la estructura de la base de datos y la relación entre las entidades, consulte la Sección 6.7. del anexo.

3.7.1. Riesgos

Los riesgos sirven para relacionar a los activos con los controles. En los controles se definen los posibles riesgos y acá se relacionan con un activo real, detallando más a fondo cuál es el riesgo en sí y como este afecta a la información de la empresa.

3.7.2. Historias de Usuario

1. Como administrador, quiero poder asignar un riesgo a cada uno de los activos.
2. Como administrador, quiero poder editar un riesgo.
3. Como usuario, quiero poder ver el listado de riesgos.
4. Como usuario, quiero poder ver el detalle de cada riesgo.

3.7.3. Interfaz de usuario

El flujo de trabajo de un usuario en el módulo de riesgos comienza con la vista de listado de riesgos. Aquí, el usuario puede ver todos los riesgos registrados en el sistema, con detalles como el nombre del riesgo, la fecha y hora de la última actualización, y el usuario que realizó la última actualización. Desde esta vista, los administradores pueden agregar nuevos riesgos, actualizar los existentes o eliminar aquellos que ya no son relevantes.

Name	Updated at	Updated by
Risk_1	June 3, 2024, 11:42 a.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Figura 53: Vista de listado de riesgos

Cuando se necesita agregar un nuevo riesgo, el administrador accede a la vista de creación de riesgos. En esta interfaz, se ingresan los detalles necesarios para registrar el riesgo, como el activo y el control asociados, el título del riesgo, el responsable, la severidad, la probabilidad y el tratamiento del riesgo. Esta información es crucial para asegurar una gestión detallada y precisa de los riesgos en la organización.

The screenshot shows the 'Create risk' form in the Compliance application. It has fields for Asset, Control, Title, Description (optional), Responsible, Severity, Likelihood, Treatment, and Residual risk for (optional). At the bottom are 'Save' and 'Cancel' buttons.

Figura 54: Vista de creación de riesgos

Una vez que el riesgo está registrado, se puede acceder a la vista de detalle de riesgos para ver toda la información relevante sobre un riesgo en particular. Esta vista muestra un desglose completo del riesgo, incluyendo el título, el responsable, la severidad, la probabilidad, el tratamiento, la fecha de creación y la última actualización. Además, se listan los activos, controles y riesgos residuales relacionados con el riesgo.

The screenshot shows the 'Risk: Risk 1' detail view. It includes sections for General information (Title: Risk 1, Description: Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)), Assets (Asset 1: Asset type 1, Medium, Internal, No, June 17, 2024, 12:18 a.m., Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)), Controls (Control 1: Control category 1, June 14, 2024, 10:41 a.m., Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)), and Residual risks.

Figura 55: Vista de detalle de riesgos

Si es necesario actualizar la información de un riesgo, el administrador accede a la vista de modificación de riesgos. Aquí, puede editar los detalles existentes del riesgo registrado en el sistema, asegurando que la información esté siempre actualizada y precisa.

The screenshot shows a web-based application interface for managing risks. At the top, there's a navigation bar with links for Compliance, Accounts, Documents, Assets, Risks, and Processes. A user is logged in as gabriel.rojas@magnet.cl. Below the navigation, the URL is Home / Risks / Risk 1 / Update Risk 1. The main content area is titled "Update Risk 1". It contains several input fields: "Asset" dropdown set to "Asset 1 - Gabriel Rojas Chamorro", "Control" dropdown set to "Control 1", "Title" input field containing "Risk 1", "Description (optional)" input field (empty), "Responsible" dropdown set to "Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)", "Severity" dropdown set to "Medium", "Likelihood" dropdown set to "Medium", "Treatment" dropdown set to "Accept", and "Residual risk for (optional)" input field (empty). There are also "Save" and "Cancel" buttons at the bottom.

Figura 56: Vista de modificación de riesgos

Para eliminar un riesgo, la vista de eliminación de riesgos permite confirmar la acción de eliminar un riesgo específico del sistema. Esta vista muestra un mensaje de confirmación con el nombre del riesgo a eliminar, asegurando que solo se realicen eliminaciones intencionales y evitando así errores.

The screenshot shows a confirmation dialog box. The title is "Delete Risk 1". Inside the dialog, a message asks "Are you sure you want to delete 'Risk 1'?" At the bottom right are two buttons: "Confirm" (in red) and "Cancel".

Figura 57: Vista de eliminación de riesgos

Este flujo de trabajo asegura que todos los riesgos estén organizados y gestionados de manera eficiente, facilitando la conformidad con las normas y regulaciones de seguridad de la información.

3.8. Módulo de Procesos

El módulo de procesos es donde se definen y gestionan los procesos. El principal propósito de los procesos es generar evidencia de que los procesos definidos en los controles del SGSI se están cumpliendo y así poder cumplir con leyes u obtener certificaciones, al momento de ser auditados. Para más detalles sobre la estructura de la base de datos y la relación entre las entidades, consulte la Sección 6.8. del anexo.

3.8.1. Procesos

Los procesos son conjuntos de actividades que se deben realizar para cumplir con los controles del SGSI. Cada proceso puede tener varias versiones, y cada versión puede definir una serie de actividades específicas. Los procesos son fundamentales para estructurar y organizar el cumplimiento de los requisitos del SGSI.

3.8.2. Actividades

Las actividades son acciones específicas que deben llevarse a cabo como parte de un proceso. Cada actividad tiene un objetivo claro y puede requerir la generación de entregables o evidencia de su cumplimiento. Las actividades están asignadas a grupos y sus instancias a usuarios específicos y pueden tener una recurrencia definida, es decir, pueden ser actividades recurrentes que se deben realizar periódicamente.

3.8.3. Historias de Usuario

1. Como administrador, quiero poder definir procesos, para generar evidencia de cierto control.
2. Como administrador, necesito la capacidad de versionar los procesos y establecer un flujo de publicación para gestionar adecuadamente las actualizaciones y revisiones.
3. Como usuario, quiero poder crear instancias de procesos en los cuales alguno de mis grupos esté asignado a la primera actividad.
4. Como usuario, quiero que se me notifique al tener una actividad de una instancia de un proceso asignado.
5. Como usuario, quiero que en la página principal se muestren los procesos en los cuales estoy asignado a la primera actividad.
6. Como usuario, quiero que en la página principal se muestren los procesos en los cuales alguno de mis grupos esté asignado a la primera actividad.
7. Como usuario, deseo que en la página principal se muestren las instancias de proceso en las cuales estoy asignado a al menos una instancia de actividad.

3.8.4. Interfaz de usuario

El flujo de trabajo de un usuario en el módulo de procesos comienza con la vista de listado de procesos, que presenta una lista completa de todos los procesos existentes en el sistema. Aquí, los usuarios pueden ver información relevante como el nombre del proceso, la última versión publicada, la última versión en general, la fecha y hora de la última actualización, y el usuario que realizó dicha actualización. Desde esta vista, los administradores tienen la opción de iniciar un nuevo proceso, añadir una nueva versión del proceso, actualizar la información del proceso existente o eliminarlo si ya no es necesario.

Processes					
Name					
Process_1	Process_1V1	Process_1V2	June 14, 2024, 11:59 a.m.	gabriel.rojas@magnet.cl	
<small>Showing results from 1 to 1 Total: 1</small>					

Figura 58: Vista de listado de procesos

Cuando un administrador necesita crear un nuevo proceso, accede a la vista de creación de procesos. En esta interfaz, el administrador ingresa el nombre del nuevo proceso y guarda la información para registrarla en el sistema.

Compliance	Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Processes / Create process						
Create process <input type="text" value="Name"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>						

Figura 59: Vista de creación de proceso

Una vez que un proceso ha sido creado, se puede acceder a su vista de detalle. Esta vista proporciona información detallada sobre el proceso, como su nombre, la fecha y hora de creación, el usuario que lo creó, la fecha y hora de la última actualización, y el usuario que realizó la última actualización. Además, desde esta vista, los usuarios pueden iniciar el proceso, actualizar su información o eliminarlo.

The screenshot shows a process detail view. At the top, there's a navigation bar with links for Compliance, Accounts, Documents, Assets, Risks, and Processes. A user is logged in as gabriel.rojas@magnet.cl. Below the navigation, the URL is Home / Processes / Process: Process 1. The main title is "Process: Process 1". There are three tabs at the top right: "Start process +", "Update process", and "Delete process X".

Name	Process 1
Created at	June 14, 2024, 11:44 a.m.
Created by	gabriel.rojas@magnet.cl
Updated at	June 14, 2024, 11:44 a.m.
Updated by	gabriel.rojas@magnet.cl

Below this is a section titled "Versions". It lists two versions:

Version	Published	Defined in	Updated at	Updated by
V1	Yes	Document 1	June 14, 2024, 11:46 a.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)
V2	No	Document 1	June 14, 2024, 11:59 a.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

At the bottom right of the version table are buttons for "Publish", "Update process version", and "Delete process version X".

Figura 60: Vista de detalle de proceso

Si es necesario actualizar un proceso, la vista de actualización permite modificar su nombre y guardar los cambios realizados.

The screenshot shows an update process view. The URL is Home / Processes / Process 1 / Update Process 1. The title is "Update Process 1". There is a single input field labeled "Name" containing "Process 1". At the bottom are "Save" and "Cancel" buttons.

Figura 61: Vista de actualización de proceso

Para eliminar un proceso, la vista de eliminación presenta un mensaje de confirmación para asegurar que la acción es intencional. El administrador puede confirmar o cancelar la eliminación según sea necesario.

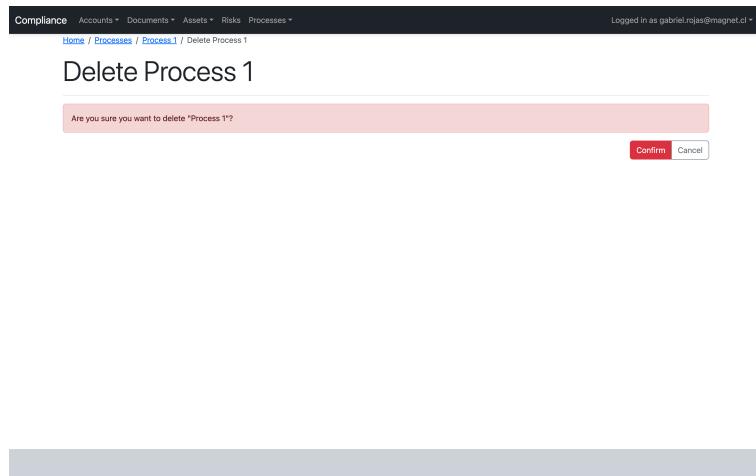


Figura 62: Vista de eliminación de proceso

Cuando se requiere crear una nueva versión de un proceso, los administradores acceden a la vista de creación de versiones de proceso. Aquí, se definen detalles como el documento en el que se basa la versión, los controles asociados, la recurrencia y el correo para notificaciones de finalización. Esta funcionalidad permite mantener el proceso actualizado y alineado con las políticas de la organización.

A screenshot of a 'Create process version' form. The top navigation bar is identical to Figure 62. The main form has a title 'Create process version'. It contains several input fields: 'Defined in' (with a dropdown menu showing '-----'), 'Controls' (with a dropdown menu showing '-----'), 'Comment label (optional)' (an input field), 'Recurrency (optional)' (with a dropdown menu showing '-----'), and 'Email to notify completion (optional)' (an input field). At the bottom right of the form are two buttons: 'Save' (in blue) and 'Cancel'.

Figura 63: Vista de creación de versión de proceso

Una vez creada, la versión de un proceso se puede ver en detalle, mostrando información relevante como el proceso al que pertenece, el documento que la define, el estado de publicación, la recurrencia y el correo de notificación. Además, desde esta vista, los administradores pueden publicar la versión, agregar actividades, actualizar la información o eliminar la versión si es necesario.

Process Version: Process 1 V2

Process
Defined in [Document 1](#)
Published No
Recurcency -
Email to notify completion June 14, 2024, 12:20 p.m.
Created at June 14, 2024, 12:20 p.m.
Created by Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)
Updated at June 14, 2024, 12:20 p.m.
Updated by Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Controls

Name	Category	Updated at	Updated by
Control 1	Control category 1	June 14, 2024, 10:41 a.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Activities

Title	Description	Assignee groups	Updated at	Updated by
Activity 1	Activity 1 description	Employee, Administrator	June 14, 2024, 12:20 p.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

[Update process activity](#) [Delete process activity](#)

Figura 64: Vista de detalle de versión de proceso

Para mantener la versión del proceso actualizada, la vista de actualización permite modificar detalles específicos como el documento definido, los controles asociados y la recurrencia.

Update Process 1 V2

Defined in [Document 1](#)

Controls [Control 1](#)

Comment label (optional)

Recurcency (optional)

Email to notify completion (optional)

[Save](#) [Cancel](#)

Figura 65: Vista de actualización de versión de proceso

La publicación de una versión de proceso se confirma a través de una vista de publicación que asegura que el administrador desea proceder con la acción.

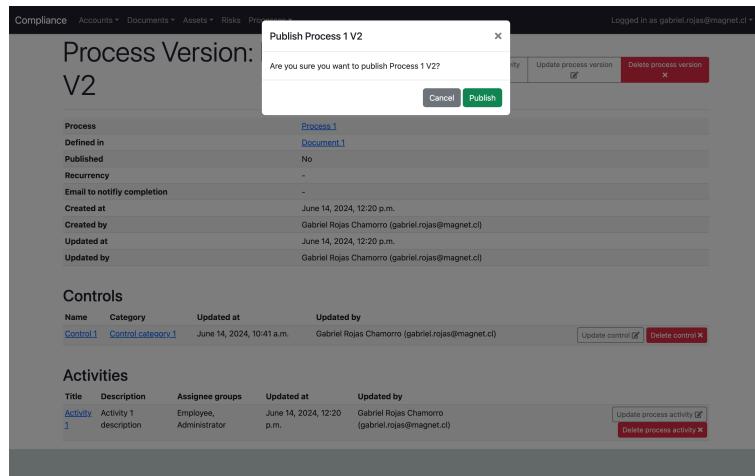


Figura 66: Vista de publicación de versión de proceso

La eliminación de una versión de proceso también se confirma mediante una vista que pregunta si realmente se desea eliminar la versión especificada, asegurando así que no se realicen eliminaciones accidentales.

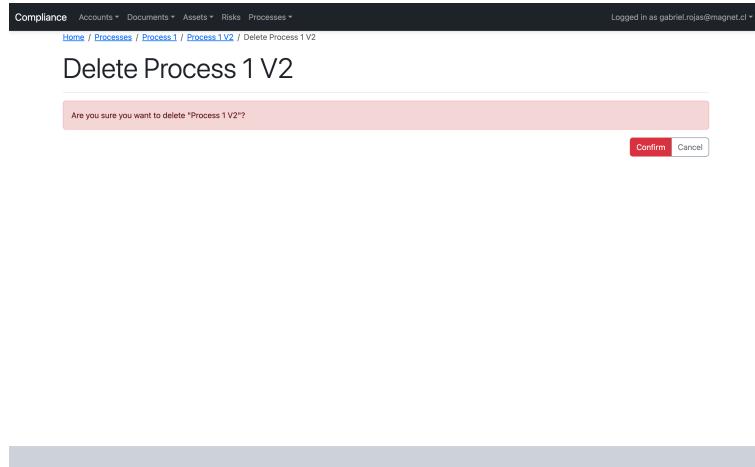


Figura 67: Vista de eliminación de versión de proceso

La creación de actividades dentro de una versión de proceso es un paso crucial. En la vista de creación de actividades, se definen los detalles necesarios como el título, la descripción, los entregables, los grupos asignados y el correo para notificaciones.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Create process activity

Title

Description

Deliverables (optional)

Assignee groups

Email to notify (optional)

Save **Cancel**

Figura 68: Vista de creación de actividad de versión de proceso

La vista de detalle de una actividad proporciona una visión completa de una actividad específica, incluyendo su título, descripción, entregables, grupos asignados y estado de finalización. Además, los administradores pueden actualizar o eliminar la actividad desde esta vista.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Process Activity: Activity 1

Process version Process 1V2

Description Activity 1 description

Deliverables -

Assignee groups Employee, Administrator

Email to notify -

Created at June 14, 2024, 12:20 p.m.

Created by Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Updated at June 14, 2024, 12:20 p.m.

Updated by Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Update process activity **Delete process activity**

Figura 69: Vista de detalle de actividad de versión de proceso

Si es necesario actualizar una actividad, la vista de actualización permite modificar la información existente, asegurando que todos los detalles sean precisos y estén actualizados.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

[Home](#) / [Processes](#) / [Process.1](#) / [Process.1.V2](#) / [Activity.1](#) / Update Activity 1

Update Activity 1

Title
Activity 1

Description
Activity 1 description

Deliverables (optional)

Assignee groups
 Employee A Administrator

Email to notify (optional)

[Save](#) [Cancel](#)

Figura 70: Vista de actualización de actividad de versión de proceso

La eliminación de una actividad se confirma mediante una vista que pregunta si se desea eliminar la actividad seleccionada, proporcionando una capa adicional de seguridad para evitar eliminaciones accidentales.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

[Home](#) / [Activity.1](#) / Delete Activity 1

Delete Activity 1

Are you sure you want to delete "Activity 1"?

[Confirm](#) [Cancel](#)

Figura 71: Vista de eliminación de actividad de versión de proceso

Finalmente, la vista de listado de instancias de procesos muestra todas las instancias creadas, permitiendo a los usuarios ver detalles como el nombre, comentarios, fecha de actualización y estado de finalización. Desde esta vista, se pueden iniciar nuevas instancias o eliminar las existentes.

Compliance	Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Process Instances						
Process Instances						
Name	Comment	Updated at	Updated by	Completed	Completed at	
Process 1 V1 Instance	-	June 16, 2024, 8:57 p.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)	No	-	Delete process instance X
Showing results from 1 to 1 Total: 1						

Figura 72: Vista de listado de instancias de procesos

La creación de una nueva instancia de proceso se realiza en una vista donde se selecciona el proceso y se añaden comentarios opcionales.

Compliance	Accounts	Documents	Assets	Risks	Processes	Logged in as gabriel.rojas@magnet.cl
Home / Process Instances / Create process instance						
Create process instance						
Process	-----					
Comment (optional)						
Save Cancel						

Figura 73: Vista de creación de instancia de proceso

La vista de detalle de la instancia de un proceso proporciona una visión completa de una instancia específica, mostrando detalles sobre la versión del proceso, comentarios, fecha de creación, actividades y su estado de finalización. Desde aquí, los administradores pueden eliminar la instancia o completar actividades.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Home / Process instances / Process Instance: Process 1 V1 Instance

Process Instance: Process 1 V1 Instance

Process version Process 1 V1

Comment -

Created at June 16, 2024, 8:57 p.m.

Created by Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Updated at June 16, 2024, 8:57 p.m.

Updated by Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Completed No

Completed at -

Activities

Title	Description	Assignee	Completed	Completed at
Activity 1	Activity 1 description	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)	No	-

Activity 1

Description: Activity 1 description

Deliverables: -

Evidence file (optional)
Choose File | No file chosen File with the evidence of the activity completion.

Evidence URL (optional)
URL to the evidence of the activity completion.

Text (optional)
Text as evidence of the activity completion.

Email to notify (optional)

Save **Cancel**

Figura 74: Vista de detalle de instancia de proceso

Para completar una actividad dentro de una instancia de proceso, la vista de finalización permite registrar la evidencia necesaria, asegurando que todas las actividades se cumplan según los requisitos establecidos.

Compliance Accounts ▾ Documents ▾ Assets ▾ Risks Processes ▾

Logged in as gabriel.rojas@magnet.cl ▾

Home / Processes / Process 1 V1 Instance / Activity 1

Activity 1

Description: Activity 1 description

Deliverables: -

Evidence file (optional)
Choose File | No file chosen File with the evidence of the activity completion.

Evidence URL (optional)
URL to the evidence of the activity completion.

Text (optional)
Text as evidence of the activity completion.

Email to notify (optional)

Save **Cancel**

Figura 75: Vista de finalización de actividad de una instancia de proceso

Con este flujo de trabajo, se asegura que todos los procesos y actividades estén organizados, gestionados y cumplidos de manera eficiente, facilitando la conformidad con las normas y regulaciones de seguridad de la información.

Para más detalles sobre otras vistas del módulo de procesos, consulte la Sección 6.9. del anexo.

Capítulo 4

Evaluación

La evaluación de la solución desarrollada se ha llevado a cabo mediante la aplicación en un contexto real dentro de la empresa Magnet y mediante una encuesta de usabilidad dirigida a los usuarios finales, utilizando la System Usability Scale (SUS)³. El objetivo de esta evaluación es demostrar cuán eficaz es la solución propuesta para resolver los problemas planteados y cumplir con los objetivos establecidos.

4.1. Uso en un Contexto Real

La plataforma fue implementada y utilizada en Magnet para la gestión del Sistema de Gestión de Seguridad de la Información (SGSI) según el estándar ISO 27001. Durante su uso, se recopiló información sobre su desempeño y efectividad en la gestión de documentos, activos, riesgos y procesos.

4.1.1. Resultados del Uso Real

- *Gestión de Documentos:* Se logró centralizar y versionar la documentación relevante, facilitando el acceso y asegurando la conformidad con las políticas de la empresa.
- *Gestión de Activos:* La clasificación y seguimiento de activos mejoró la visibilidad y control sobre los recursos críticos de la empresa.
- *Gestión de Riesgos:* La identificación y evaluación de riesgos permitió una respuesta más ágil y eficiente ante posibles amenazas.
- *Gestión de Procesos:* La definición y seguimiento de procesos aseguró la generación de evidencia necesaria para auditorías, cumpliendo con los requisitos de ISO 27001.

³«https://en.wikipedia.org/wiki/System_usability_scale»

4.2. Encuesta de Usabilidad

Para complementar la evaluación, se realizó una encuesta de usabilidad entre los usuarios de la plataforma, utilizando la System Usability Scale (SUS). La encuesta se basó en una escala del 1 al 5, donde 1 representa «totalmente en desacuerdo» y 5 representa «totalmente de acuerdo». A continuación, se presentan los resultados de la encuesta y el puntaje SUS calculado.

4.2.1. Resultados de la Encuesta

El puntaje SUS se calcula mediante la siguiente fórmula:

1. Para cada pregunta impar (1, 3, 5, 7, 9), se resta 1 del puntaje.
2. Para cada pregunta par (2, 4, 6, 8, 10), se resta el puntaje de 5.
3. Se suman todos los valores obtenidos y se multiplica por 2.5 para obtener el puntaje SUS.

Los resultados individuales y el puntaje promedio se muestran a continuación:

Pregunta	Respuesta Usuario 1	Respuesta Usuario 2	Promedio
Me gustaría usar este sistema frecuentemente	3	5	4
Encontré el sistema innecesariamente complejo	1	2	1.5
Pensé que el sistema era fácil de usar	5	4	4.5
Creo que necesitaría el soporte de una persona técnica para poder usar este sistema	1	2	1.5
Encontré que las diversas funciones en este sistema estaban bien integradas	4	5	4.5
Pensé que había demasiada inconsistencia en este sistema	2	2	2
Imagino que la mayoría de las personas aprendería a usar este sistema muy rápidamente	5	4	4.5
Encontré el sistema muy engorroso de usar	2	2	2
Me sentí muy seguro usando el sistema	5	5	5

Pregunta	Respuesta Usuario 1	Respuesta Usuario 2	Promedio
Necesitaba aprender muchas cosas antes de poder comenzar a usar este sistema	1	1	1
Puntaje SUS	87.5	85	86.25

4.3. Análisis de la Encuesta

El puntaje promedio SUS de 86.25 indica una excelente usabilidad del sistema, ya que un puntaje SUS por encima de 68 se considera bueno y un puntaje por encima de 80.3 se considera excelente [5]. Este resultado refleja que los usuarios encuentran la plataforma fácil de usar, bien integrada y confiable.

4.4. Conclusiones de la Evaluación

La evaluación demuestra que la solución propuesta ha sido efectiva en la gestión del SGSI en Magnet, cumpliendo con los estándares de ISO 27001. Los resultados de la encuesta de usabilidad indican una alta aceptación y satisfacción por parte de los usuarios, con una interfaz intuitiva y bien integrada que facilita su uso sin necesidad de soporte técnico significativo.

La implementación en un contexto real y la retroalimentación positiva obtenida de los usuarios finales validan la eficacia de la solución desarrollada, asegurando su capacidad para mejorar la gestión de la seguridad de la información en la empresa. Esta plataforma no solo resuelve los problemas planteados, sino que también proporciona una base sólida para futuras mejoras y escalabilidad.

Capítulo 5

Conclusiones

5.1. Resumen del Trabajo Realizado

Este trabajo se centró en el desarrollo e implementación de una plataforma para la gestión del Sistema de Gestión de Seguridad de la Información (SGSI) en Magnet, conforme al estándar ISO 27001. La solución propuesta abarcó la gestión de documentos, activos, riesgos y procesos, utilizando tecnologías como Django, PostgreSQL, Docker y TypeScript.

5.2. Objetivos Alcanzados y No Alcanzados

5.2.1. Objetivos Alcanzados

- *Centralización de Documentos:* Se logró centralizar la gestión de documentos y asegurar su versionado y conformidad.
- *Gestión de Activos:* Se implementó una eficiente clasificación y seguimiento de activos críticos.
- *Evaluación de Riesgos:* La plataforma permitió una identificación y evaluación sistemática de riesgos.
- *Gestión de Procesos:* Se definieron y gestionaron procesos que generan evidencia de conformidad con los controles del SGSI.

5.2.2. Objetivos No Alcanzados

Todos los objetivos iniciales del proyecto fueron alcanzados, aunque se identificaron áreas de mejora para futuras iteraciones.

5.3. Análisis Crítico de los Resultados

Los resultados obtenidos fueron altamente satisfactorios, principalmente debido a la correcta elección de tecnologías y la adaptación de las mejores prácticas en el desarrollo del software. La participación activa de los usuarios finales en el proceso de evaluación también contribuyó a la validación y refinamiento de la solución.

5.4. Relevancia e Impacto del Trabajo Realizado

La implementación de esta plataforma tiene un impacto significativo en la capacidad de Magnet para gestionar su SGSI de manera autónoma y eficaz, mejorando su postura de seguridad informática y facilitando el cumplimiento con los estándares de ISO 27001. Además, la solución desarrollada ofrece potencial de comercialización, pudiendo ser adaptada y utilizada por otras organizaciones.

5.5. Lecciones Aprendidas

Durante el desarrollo del proyecto, se aprendieron varias lecciones importantes:

- *Importancia de la Usabilidad:* Una interfaz intuitiva y bien diseñada es crucial para la aceptación del sistema por parte de los usuarios.
- *Interacción con los Usuarios:* La retroalimentación constante de los usuarios finales es vital para el éxito de cualquier proyecto de software.

5.6. Trabajo Futuro

Para mejorar aún más la solución y abordar las áreas de mejora identificadas, se proponen los siguientes trabajos futuros:

- *Integración con Más Sistemas:* Ampliar la integración con otros sistemas y servicios utilizados por Magnet y otras organizaciones.
- *Automatización Avanzada:* Implementar características avanzadas de automatización para reducir aún más la carga de trabajo manual en la gestión del SGSI.
- *Análisis de Datos:* Desarrollar módulos de análisis de datos para proporcionar informes y estadísticas más detalladas sobre la gestión de la seguridad de la información.
- *Expansión de Funcionalidades:* Añadir nuevas funcionalidades basadas en las necesidades emergentes de la empresa y las tendencias en seguridad de la información.

En conclusión, la plataforma desarrollada no solo cumple con los objetivos establecidos, sino que también abre nuevas oportunidades para la mejora continua y la expansión, beneficiando tanto a Magnet como a otras organizaciones en su gestión de la seguridad de la información.

Bibliografía

- [1] Mylenio, «Team Organization». 2022. Accedido: 20 de mayo de 2024. [En línea]. Disponible en: <https://www.mylenio.com/team-organization>
- [2] Mylenio, «Human Resources - HR People Love». 2022. Accedido: 20 de mayo de 2024. [En línea]. Disponible en: <https://www.mylenio.com/human-resources-hr>
- [3] Mylenio, «Compliance & Security - Become Compliance». 2022. Accedido: 20 de mayo de 2024. [En línea]. Disponible en: <https://www.mylenio.com/compliance-and-security>
- [4] Brendan Marshall, «bmarsh9/gapps: Security compliance platform - SOC2, CMMC, ASVS, ISO27001, HIPAA, NIST CSF, NIST 800-53, CSC CIS 18, PCI DSS, SSF tracking. <https://gapps.darkbanner.com>». Accedido: 20 de mayo de 2024. [En línea]. Disponible en: <https://github.com/bmarsh9/gapps>
- [5] Nathan Thomas, «How To Use The System Usability Scale (SUS) To Evaluate The Usability Of Your Website - Usability Geek». Accedido: 1 de julio de 2024. [En línea]. Disponible en: <https://usabilitygeek.com/how-to-use-the-system-usability-scale-sus-to-evaluate-the-usability-of-your-website/>
- [6] Django Software Foundation, «The contenttypes framework | Django documentation». Accedido: 27 de mayo de 2024. [En línea]. Disponible en: <https://docs.djangoproject.com/en/4.2/ref/contrib/contenttypes/>

Capítulo 6

Anexo

6.1. Modelo de datos módulo de Usuarios

1. User: guarda los datos de los usuarios registrados.
 - `id`: identificador único del usuario.
 - `email`: el email del usuario.
 - `first_name`: el(los) nombre(s) del usuario.
 - `last_name`: el(los) apellido(s) del usuario.
 - `is_active`: indica si el usuario está activo en la aplicación.
 - `is_staff`: indica si el usuario tiene la capacidad de loguearse al sitio de administración.
 - `is_superuser`: indica si el usuario tiene todos los permisos, sin tener que asignarselos.
 - `date_joined`: fecha en la cual el usuario fue registrado.
 - `groups`: los grupos asignados al usuario.
 - `user_permissions`: los permisos asignados al usuario.
2. Group: guarda los datos de los grupos de la aplicación.
 - `id`: identificador único del grupo.
 - `name`: el nombre del grupo.
 - `permissions`: los permisos asociados al grupo.
3. Permission: guarda los datos de los permisos de la aplicación.
 - `id`: identificador único del permiso.
 - `content_type`: el tipo de contenido al cual está relacionado el permiso, donde estos son modelos de Django [6].
 - `name`: el nombre del permiso.
 - `codename`: el código del permiso.

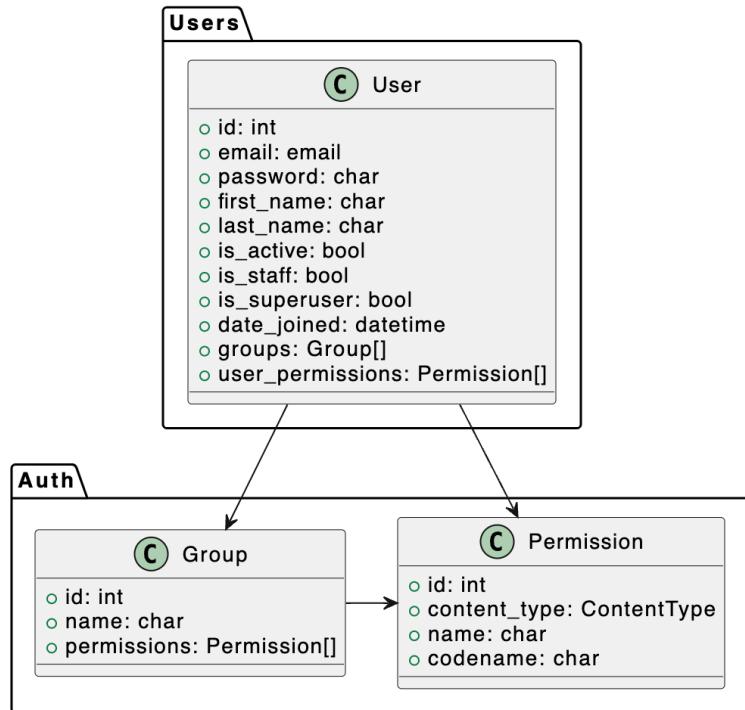


Figura 76: Modelo entidad-relación módulo de usuarios

6.2. Vistas módulo de Usuarios

6.2.1. Eliminación de Usuario

La vista de eliminación de usuario permite a los administradores borrar una cuenta de usuario existente del sistema. Esta acción es crítica y debe realizarse con precaución, ya que la eliminación de un usuario no puede deshacerse.

Confirmación de Eliminación: Se muestra un mensaje de confirmación para asegurar que la eliminación del usuario es intencional y evitar la eliminación accidental de datos importantes.

Acciones disponibles:

- *Confirmar:* Permite proceder con la eliminación del usuario.
- *Cancelar:* Permite cancelar la operación de eliminación.

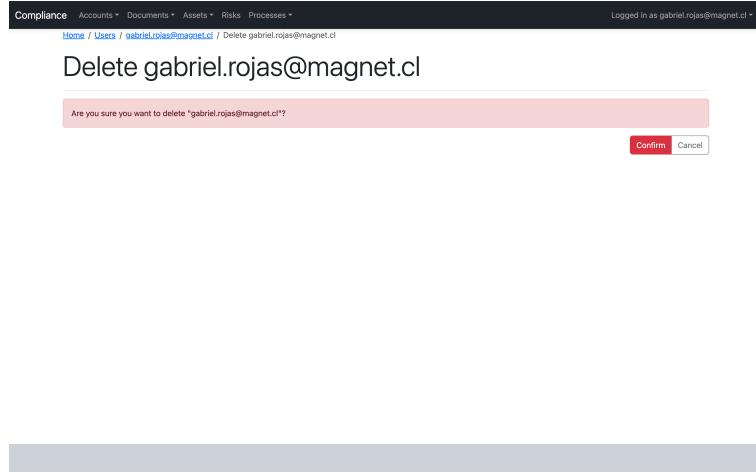


Figura 77: Vista de eliminación de usuario

6.2.2. Creación de grupo

La vista de creación de grupos permite a los administradores añadir nuevos grupos al sistema. Esta interfaz incluye los siguientes campos y opciones:

- *Nombre*: Ingrese el nombre del grupo.
- *Usuarios (opcional)*: Asigne uno o más usuarios al grupo.
- *Permisos (opcional)*: Asigne uno o más permisos al grupo.

Botones de acción:

- *Guardar*: Guarda el nuevo grupo.
- *Cancelar*: Cancela la creación y vuelve a la vista anterior.

Figura 78: Vista de creación de grupo

6.2.3. Detalle de grupo

La vista de detalle de grupo muestra información detallada sobre un grupo específico. Incluye:

- *Usuarios*: Lista de usuarios que pertenecen al grupo, junto con su nombre y correo electrónico.

- *Permisos asignados:* Una lista detallada de los permisos asignados al grupo, incluyendo el nombre del permiso, el nombre de código y la aplicación/modelo asociado.

Botones de acción:

- *Actualizar grupo:* Permite editar la información del grupo.
- *Eliminar grupo:* Permite eliminar el grupo, con confirmación para evitar eliminaciones accidentales.

Name	Codename	App label	Model
Can view control	view_control	documents	control
Can view control category	view_contrcategory	documents	contrcategory
Can view document	view_document	documents	document
Can view document version	view_documentversion	documents	documentversion
Can add document version read by user	add_documentversionreadbyuser	documents	documentversionreadbyuser
Can view document version read by user	view_documentversionreadbyuser	documents	documentversionreadbyuser
Can view evidence	view_evidence	documents	evidence
Can view asset	view_asset	information_assets	asset
Can view asset type	view_assettype	information_assets	assettype
Can view process	view_process	processes	process
Can view process activity	view_processactivity	processes	processactivity
Can change process activity instance	change_processactivityinstance	processes	processactivityinstance
Can view process activity instance	view_processactivityinstance	processes	processactivityinstance
Can add process instance	add_processinstance	processes	processinstance
Can view process instance	view_processinstance	processes	processinstance
Can view process version	view_processversion	processes	processversion

Figura 79: Vista de detalle de grupo

6.2.4. Actualización de grupo

La vista de actualización de grupo permite a los administradores editar la información de un grupo existente. Incluye los siguientes campos y opciones:

- *Nombre:* Editar el nombre del grupo.
- *Usuarios (opcional):* Asignar o cambiar los usuarios que pertenecen al grupo.
- *Permisos (opcional):* Asignar o cambiar los permisos del grupo.

Botones de acción:

- *Guardar:* Guarda los cambios realizados en el grupo.
- *Cancelar:* Cancela la operación y vuelve a la vista anterior sin guardar los cambios.

Figura 80: Vista de actualización de grupo

6.2.5. Eliminación de Grupos

La vista de eliminación de grupos permite eliminar un grupo específico del sistema, garantizando que los usuarios y roles asociados se manejen adecuadamente antes de la eliminación final. Esta funcionalidad es esencial para mantener la estructura organizativa actualizada y precisa dentro del SGSI.

Confirmación de Eliminación: Se muestra un mensaje de confirmación para asegurar que la eliminación del grupo es intencional y evitar la eliminación accidental de datos importantes.

Acciones disponibles:

- *Confirmar:* Permite proceder con la eliminación del grupo seleccionado.
- *Cancelar:* Permite cancelar el proceso de eliminación y regresar a la vista anterior sin realizar cambios.

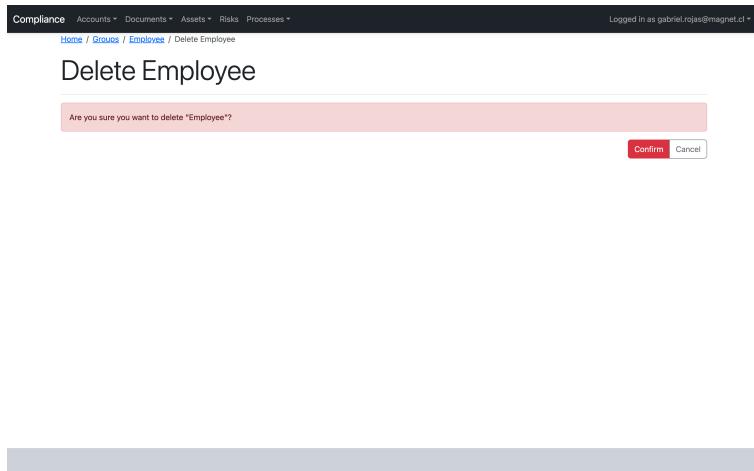


Figura 81: Vista de eliminación de grupo

6.3. Modelo de Datos módulo de Documentos

1. ControlCategory: guarda los datos de las categorías de controles.
 - **id:** el identificador único de la categoría.
 - **name:** el nombre de la categoría.
2. Control: guarda los datos de los controles.
 - **id:** el identificador único del control.
 - **category:** la categoría del control.
 - **title:** el título del control.
 - **description:** la descripción del control.
3. DocumentType: guarda los datos de los tipos de documentos.
 - **id:** el identificador único del tipo.
 - **name:** el nombre del tipo.

4. Document: guarda los datos de un documento.
 - **id**: el identificador único del documento.
 - **title**: el título del documento.
 - **document_type**: el tipo de documento.
 - **description**: la descripción del documento.
 - **code**: el código del documento.
 - **drive_folder**: la URL a la carpeta de drive para el documento.
 - **documented_controls**: los controles que se encuentran documentados en el documento.
5. DocumentVersion: guarda los datos de las versiones de un documento.
 - **id**: el identificador único de la versión de un documento.
 - **document**: el documento al cual pertenece la versión.
 - **version**: el número de la versión.
 - **author**: el autor del documento.
 - **shasum**: el hash (sha256) del archivo de la versión.
 - **comment**: comentario de la versión.
 - **file**: el archivo de la versión.
 - **file_url**: el URL a la versión del documento.
 - **is_approved**: booleano indicando si la versión se encuentra aprobada.
 - **approval_evidence**: la evidencia de aprobación de la versión.
 - **approved_at**: la fecha y hora en la cual fue aprobada la versión.
 - **approved_by**: el usuario que aprobó la versión.
 - **verification_code**: código utilizado para verificar la lectura de una versión.
 - **read_by**: los usuarios que han marcado como leída la versión.
6. DocumentVersionReadByUser: relaciona usuarios y versiones de documentos, marcando una versión de un documento como leída.
 - **id**: el identificador único de la relación entre usuario y versión de documento.
 - **document_version**: la versión leída por el usuario.
 - **user**: el usuario que leyó la versión.
7. Evidence: guarda los datos de una evidencia.
 - **id**: el identificador único de la evidencia.
 - **file**: archivo de la evidencia.
 - **url**: URL de la evidencia.
 - **text**: texto de la evidencia.
 - **shasum**: el hash (sha256) del archivo, URL o texto de la evidencia.

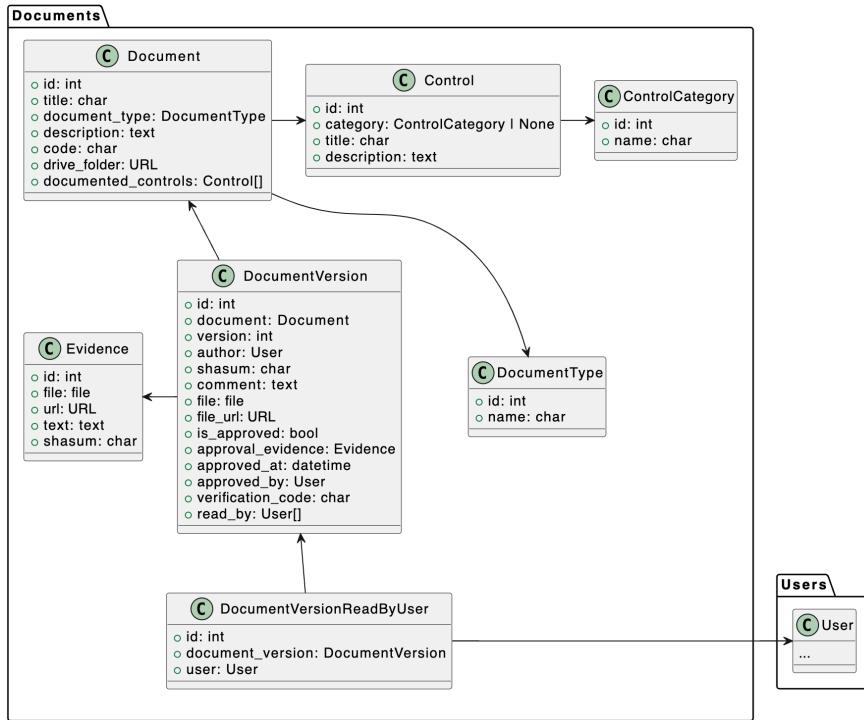


Figura 82: Modelo entidad-relación módulo de documentos

6.4. Vistas modulo de Documentos

6.4.1.1. Eliminación de Controles

La vista de eliminación de controles permite a los administradores eliminar un control específico de forma segura y definitiva.

- *Confirmación:* Se presenta un mensaje claro preguntando si realmente se desea eliminar el control especificado, mostrando su nombre para asegurar que se está eliminando el control correcto.

Botones de acción:

- *Confirmar:* Elimina definitivamente el control.
- *Cancelar:* Cancela la operación y vuelve a la vista anterior sin realizar cambios.

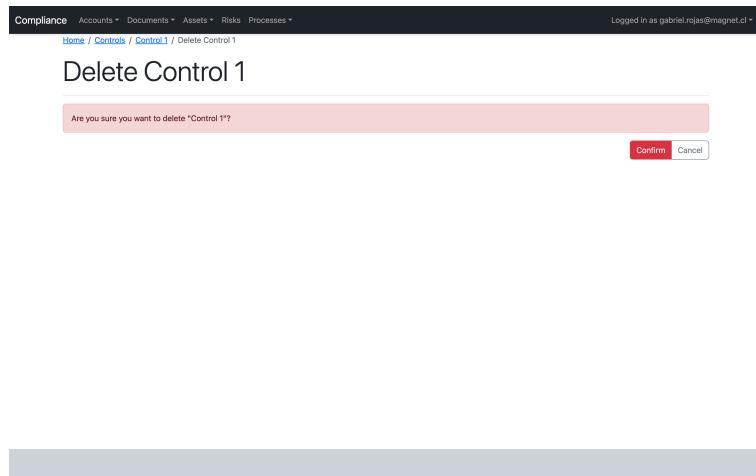


Figura 83: Vista de eliminación de controles

6.4.1.2. Detalle de Categorías de Controles

La vista de detalle de categorías de controles permite a los administradores ver y gestionar información específica de cada categoría de control. Los campos más relevantes incluyen:

- *Nombre*: Nombre de la categoría de control.
- *Creado por*: Usuario que creó la categoría de control.
- *Actualizado por*: Usuario que realizó la última actualización.

Además, la vista muestra los controles relacionados con esta categoría.

Botones de acción:

- *Actualizar Categoría de Control*: Permite editar la información de la categoría de control.
- *Eliminar Categoría de Control*: Permite eliminar la categoría de control.

Name	Control Category 1
Created at	May 29, 2024, 12:33 p.m.
Created by	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)
Updated at	May 29, 2024, 12:33 p.m.
Updated by	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Related controls			
Name	Category	Updated at	Updated by
Control_1	Control Category_1	May 29, 2024, 12:33 p.m.	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)

Figura 84: Vista de detalle de categorías de controles

6.4.1.3. Actualización de Categorías de Controles

La vista de actualización de categorías de controles permite a los administradores editar la información de una categoría de control existente. Esta interfaz incluye:

- *Nombre*: Campo para editar el nombre de la categoría de control.

Botones de acción:

- *Guardar*: Guarda los cambios realizados en la categoría de control.
- *Cancelar*: Cancela la operación y vuelve a la vista anterior sin realizar cambios.

The screenshot shows a web interface for updating a control category. At the top, there's a navigation bar with links for Compliance, Accounts, Documents, Assets, Risks, and Processes. The user is logged in as 'gabriel.rojas@magnet.cl'. The main content area has a title 'Update Control Category 1'. Below the title is a form with a single input field labeled 'Name' containing the value 'Control Category 1'. At the bottom of the form are two buttons: 'Save' (in blue) and 'Cancel' (in red).

Figura 85: Vista de actualización de categorías de controles

6.4.1.4. Eliminación de Categorías de Controles

La vista de eliminación de categorías de controles permite a los administradores eliminar una categoría específica de control de forma segura y definitiva.

- *Confirmación*: Se presenta un mensaje claro preguntando si realmente se desea eliminar la categoría de control especificada, mostrando su nombre para asegurar que se está eliminando la categoría correcta.

Botones de acción:

- *Confirmar*: Elimina definitivamente la categoría de control.
- *Cancelar*: Cancela la operación y vuelve a la vista anterior sin realizar cambios.

The screenshot shows a confirmation dialog for deleting a control category. The URL is 'Home / Control categories / Control Category.1 / Delete Control Category 1'. The page title is 'Delete Control Category 1'. A red message box contains the text 'Are you sure you want to delete *Control Category 1*?'. At the bottom are two buttons: 'Confirm' (in red) and 'Cancel'.

Figura 86: Vista de eliminación de categorías de controles

6.4.1.5. Eliminación de Documentos

La vista de eliminación de documentos permite a los administradores eliminar un documento específico de la aplicación de forma segura y definitiva.

- *Confirmación:* Se presenta un mensaje claro preguntando si realmente se desea eliminar el documento especificado, mostrando su nombre para asegurar que se está eliminando el documento correcto.

Botones de acción:

- *Confirmar:* Elimina definitivamente el documento de la aplicación.
- *Cancelar:* Cancela la operación y vuelve a la vista anterior sin realizar cambios.

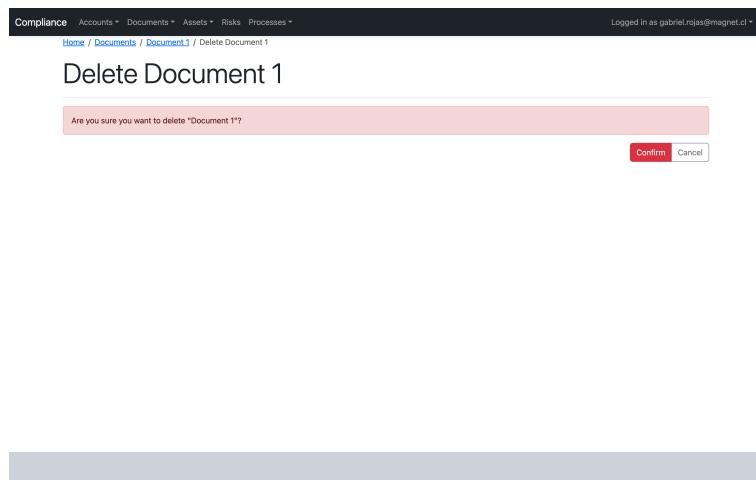


Figura 87: Vista de eliminación de documentos

6.4.1.6. Actualización de Versión de Documentos

La vista de actualización de versiones de documentos permite a los administradores actualizar la información de una versión específica de un documento. Los campos más relevantes incluyen:

- *Autor:* Autor de la versión del documento.
- *Archivo actual:* Enlace al archivo de la versión actual del documento.
- *Cambiar archivo:* Opción para subir un nuevo archivo si es necesario.
- *URL del archivo (opcional):* Enlace opcional al archivo de la versión del documento.
- *Comentario (opcional):* Campo para agregar comentarios sobre la actualización de la versión del documento.

Botones de acción:

- *Guardar:* Permite guardar los cambios realizados en la versión del documento.
- *Cancelar:* Permite cancelar la operación de actualización y volver a la vista anterior sin realizar cambios.

Figura 88: Vista de actualización de versión de documentos

6.4.1.7. Eliminación de Versión de Documentos

La vista de eliminación de versiones de documentos permite a los administradores eliminar una versión específica de un documento de forma segura y definitiva.

- *Confirmación:* Se presenta un mensaje claro preguntando si realmente se desea eliminar la versión especificada del documento, mostrando su nombre para asegurar que se está eliminando la versión correcta.

Botones de acción:

- *Confirmar:* Elimina definitivamente la versión del documento.
- *Cancelar:* Cancela la operación y vuelve a la vista anterior sin realizar cambios.

Figura 89: Vista de eliminación de versiones de documentos

6.4.1.8. Eliminación de Tipos de Documentos

La vista de eliminación de un tipo de documento permite confirmar la eliminación del tipo de documento seleccionado. Esta vista incluye la siguiente información relevante:

- *Confirmación:* Se solicita la confirmación del usuario para eliminar el tipo de documento seleccionado.

Acciones disponibles:

- *Confirmar*: Permite confirmar la eliminación del tipo de documento.
- *Cancelar*: Permite cancelar la eliminación y volver a la vista anterior sin realizar cambios.

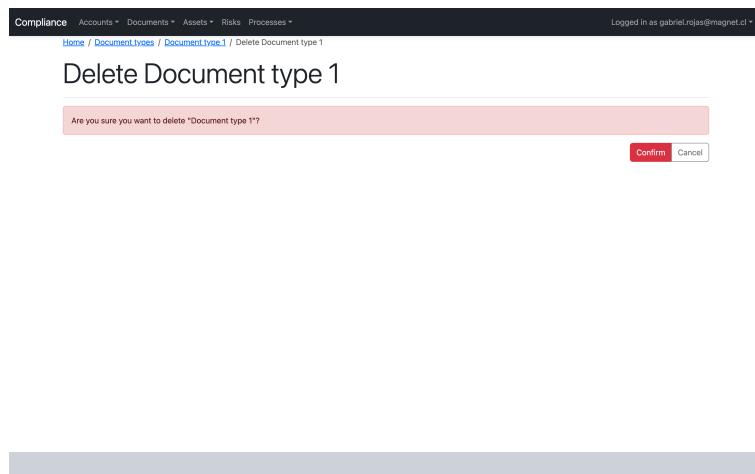


Figura 90: Vista de eliminación de tipos de documentos

6.5. Modelo de Datos módulo de Activos

1. AssetType: guarda los datos de un tipo de activo.
 - **id**: el identificador único.
 - **name**: el nombre del tipo de activo.
 - **description**: la descripción del tipo de activo.
2. Asset: guarda los datos de un activo.
 - **id**: el identificador único.
 - **owner**: el dueño del activo.
 - **code**: el código único del activo.
 - **name**: el nombre del activo.
 - **description**: la descripción del activo.
 - **asset_types**: los tipos del activo.
 - **criticality**: la criticidad del activo, que puede ser **muy baja**, **baja**, **media**, **alta** o **muy alta**.
 - **classification**: la clasificación del activo, que puede ser **pública**, **interna** o **privada**.
 - **is_archived**: indica si el activo está actualmente archivado.
3. AssetRole: guarda los datos de un rol de un activo.
 - **id**: el identificador único.
 - **asset**: el activo del rol.
 - **name**: el nombre del rol.
 - **users**: los usuarios asignados al rol.

- AssetRoleUser: guarda los datos de roles asignados a usuarios.
 - id**: el identificador único.
 - role**: el rol asignado al usuario.
 - user**: el usuario asignado al rol.

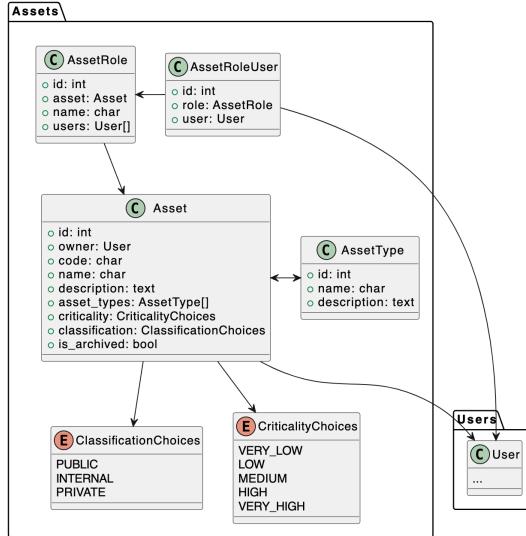


Figura 91: Modelo entidad-relación módulo de activos

6.6. Vistas modulo de Activos

6.6.1.1. Archivado de Activos

La vista de archivado de un activo permite confirmar la acción de archivar un activo específico. Los campos más relevantes y acciones disponibles son los siguientes:

- Mensaje de confirmación*: Indica si el usuario está seguro de querer archivar el activo seleccionado.
- Nombre del Activo*: Se muestra el nombre del activo a archivar.

Acciones disponibles:

- Archivar*: Confirma la acción de archivar el activo.
- Cancelar*: Cancela la acción de archivado y regresa a la vista anterior.

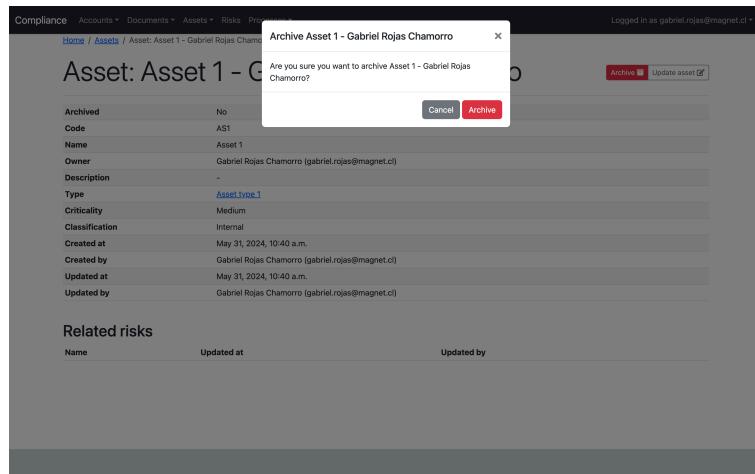


Figura 92: Vista de archivado de activos

6.6.1.2. Eliminación de Tipos de Activos

La vista de eliminación de un tipo de activo confirma la eliminación del tipo de activo seleccionado. Esta vista presenta un mensaje de confirmación para asegurar que el usuario desea proceder con la acción de eliminación. Los elementos incluidos son:

- *Mensaje de confirmación*: Pregunta al usuario si está seguro de querer eliminar el tipo de activo.
- *Botón Confirmar*: Procede con la eliminación del tipo de activo.
- *Botón Cancelar*: Cancela la acción de eliminación y regresa a la vista anterior.

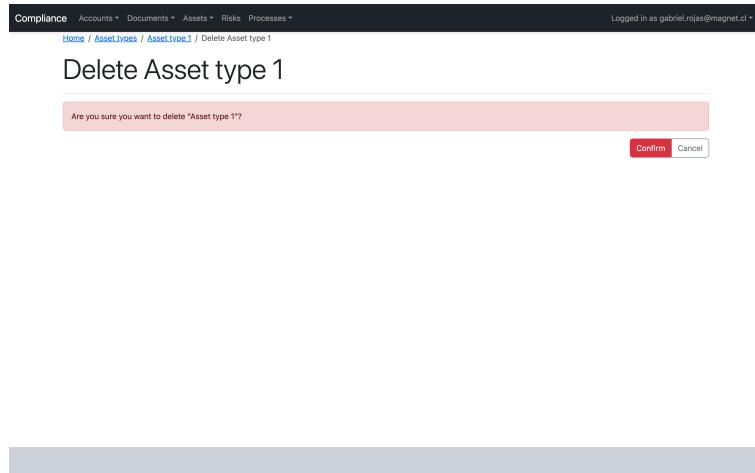


Figura 93: Vista de eliminación de tipos de activos

6.7. Modelo de Datos módulo de riesgos

1. Risk: guarda los datos de un riesgo.
 - **id**: el identificador único.
 - **assets**: los activos para el cual existe el riesgo.
 - **controls**: los controles asociados al riesgo.

- **title**: el título del riesgo.
- **description**: la descripción del riesgo.
- **responsible**: el responsable del riesgo.
- **severity**: la gravedad del riesgo, que puede ser **muy baja**, **baja**, **media**, **alta** o **muy alta**.
- **likelihood**: la probabilidad de que se materialice el riesgo, que puede ser **muy baja**, **baja**, **media**, **alta** o **muy alta**.
- **treatment**: el tratamiento que se le dará al riesgo, que puede ser **mitigar**, **transferir**, **aceptar** o **eliminar**.
- **residual_risk**: el riesgo residual del riesgo.

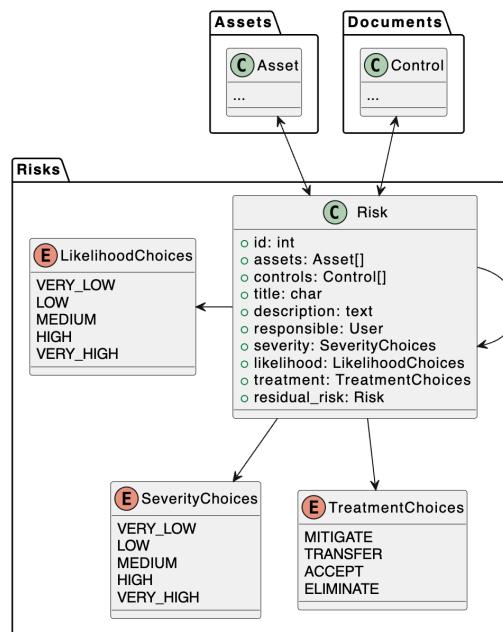


Figura 94: Modelo entidad-relación módulo de riesgos

6.8. Modelo de Datos módulo de procesos

1. **Process**: guarda los datos de un proceso.
 - **id**: el identificador único.
 - **name**: el nombre de la definición de un proceso.
2. **ProcessVersion**: guarda los datos de una versión de un proceso.
 - **id**: el identificador único.
 - **process**: el proceso al cual pertenece la versión.
 - **version**: el número de la versión del proceso.
 - **defined_in**: el documento en el cual está definido el proceso.
 - **controls**: los controles para los cuales se genera la evidencia al completar las actividades de la versión.
 - **comment_label**: la etiqueta para el comentario de una instancia del proceso.

- **recurrency**: la periodicidad con la cual se instancia el proceso, que puede ser diariamente, semanalmente, mensualmente, trimestralmente, semi anualmente o anualmente.
- **email_to_notify**: la dirección de correo electrónico a notificar al finalizar el proceso.
- **is_published**: indica si la versión está publicada.
- **published_at**: la fecha y hora en la cual se publicó la versión.
- **published_by**: el usuario que publicó la versión.

3. **ProcessActivity**: guarda los datos de una actividad.

- **id**: el identificador único.
- **process_version**: la versión del proceso a la cual pertenece la actividad.
- **order**: el orden respecto a otras actividades de una versión de un proceso.
- **title**: el título de la actividad.
- **description**: la descripción de la actividad a realizar.
- **assignee_group**: el grupo de usuarios entre los cuales se puede asignar la actividad cuando se inicia una instancia de esta.
- **deliverables**: los entregables de la actividad.
- **email_to_notify**: el email al cual se debe notificar cuando se inicie una instancia de la actividad.

4. **ProcessInstance**:

- **id**: el identificador único.
- **process_version**: la versión del proceso usada para su instancia.
- **comment**: el comentario con el cual se inició la instancia del proceso.
- **is_completed**: booleano que representa si la instancia del proceso fue completada.
- **completed_at**: fecha y hora en la cual fue completada la instancia del proceso.

5. **ProcessActivityInstance**:

- **id**: el identificador único.
- **process_instance**: la instancia de un proceso a la cual esta asociada la instancia de la actividad.
- **activity**: la actividad de la versión del proceso usada para su instancia.
- **assignee**: el usuario encargado de realizar la actividad.
- **is_completed**: booleano que representa si la actividad fue completada.
- **completed_at**: fecha y hora en la cual fue completada la actividad.
- **evidence**: la evidencia generada a partir de la actividad.

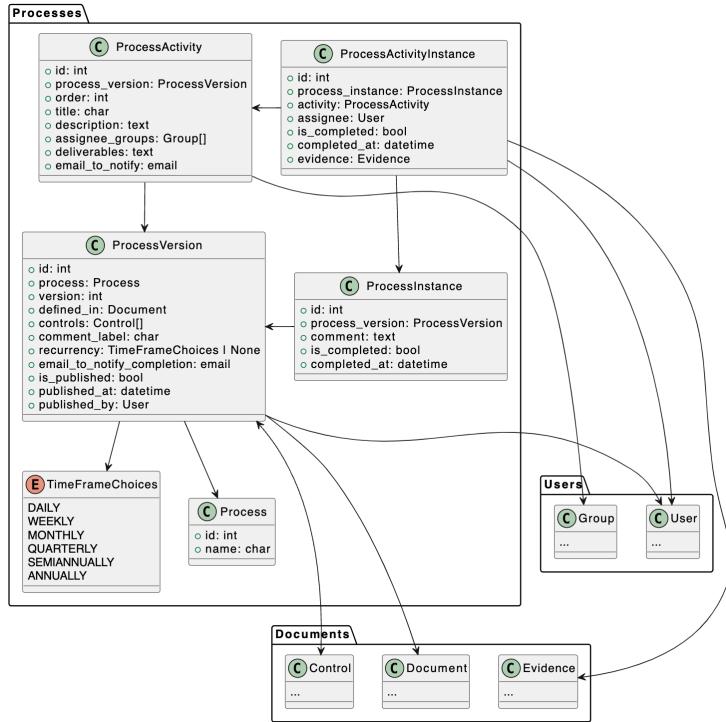


Figura 95: Modelo entidad-relación módulo de procesos

6.9. Vistas modulo de procesos

6.9.1.1. Eliminación de la Instancia de un Proceso

La vista de eliminación de la instancia de un proceso permite al usuario confirmar la eliminación de una instancia específica de un proceso. Los puntos más importantes de esta vista son:

- *Confirmación de Eliminación:* Mensaje de confirmación para asegurar que el usuario realmente desea eliminar la instancia del proceso seleccionada.

Acciones disponibles:

- *Confirmar:* Permite eliminar la instancia de proceso seleccionada.
- *Cancelar:* Permite cancelar la eliminación de la instancia de proceso.

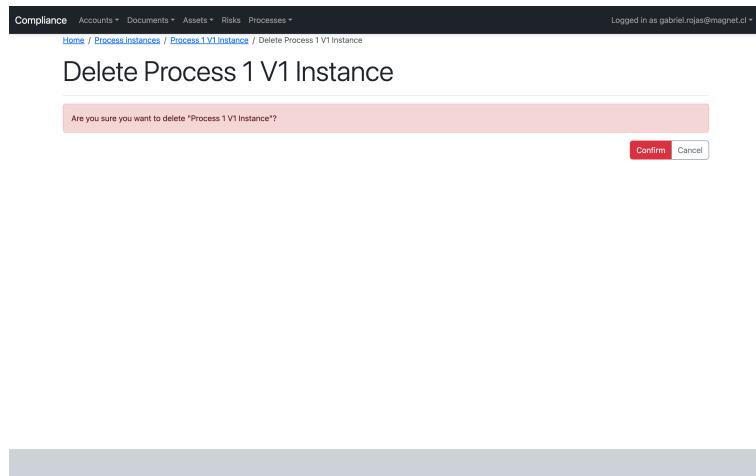


Figura 96: Vista de eliminación de instancia de proceso

6.9.1.2. Detalle de la Actividad de una Instancia de Proceso

La vista de detalle de la actividad de una instancia de proceso muestra la información relevante de una actividad específica dentro de una instancia de proceso. Los puntos más importantes de esta vista son:

- *Proceso Instancia*: Muestra la instancia de proceso a la que pertenece la actividad.
- *Actividad*: Nombre de la actividad.
- *Responsable*: Persona asignada para realizar la actividad.
- *Descripción*: Detalles y descripción de la actividad.
- *Entregables*: Lista de entregables relacionados con la actividad (si los hay).
- *Completado*: Estado de la actividad, indicando si está completada o no.
- *Completado en*: Fecha y hora en que se completó la actividad (si está completada).

Acciones disponibles:

- *Completar Actividad*: Permite marcar la actividad como completada.
- *Eliminar Actividad*: Permite eliminar la actividad de la instancia de proceso.

Process Activity Instance: Activity 1	
Process instance	Process 1 V1 Instance
Activity	Activity 1
Assignee	Gabriel Rojas Chamorro (gabriel.rojas@magnet.cl)
Description	Activity 1 description
Deliverables	-
Completed	No
Completed at	-

Figura 97: Vista de detalle de la actividad de una instancia de proceso