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

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

INFORME FINAL DE CC6909 PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN COMPUTACIÓN

Gabriel Rojas Chamorro

MODALIDAD:
Práctica Extendida

PROFESOR GUÍA:
Eduardo Godoy Vega

SUPERVISOR:
Mauricio Castro García

SANTIAGO DE CHILE
2024

1. Introducción

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 cibernéticas 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 de la norma 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.

Problema y Relevancia

La creciente sofisticación de las amenazas cibernéticas 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 y con el propósito de proteger los activos digitales y salvaguardar la reputación de la empresa en el escenario empresarial 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 poder demostrar el cumplimiento de leyes que se conforman a este paradigma. 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 los requisitos regulatorios, como la ISO 27001, sino que también ofrezcan flexibilidad y capacidad de adaptación a las cambiantes condiciones del entorno digital.

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. Además, plantea la posibilidad de escalar y adaptar la solución para otras organizaciones con necesidades similares, contribuyendo así a la seguridad informática en un ámbito más amplio.

Descripción general de la solución

La solución propuesta adopta un enfoque integral al incorporar módulos especializados para la gestión eficiente de documentos, activos, riesgos y procesos asociados a los controles de ISO 27001. A través de tecnologías sólidas como Django, PostgreSQL y Typescript, se busca ofrecer no solo eficiencia operativa, sino también una base sólida para el desarrollo y la escalabilidad futura, asegurando que la plataforma evolucione al ritmo de las crecientes demandas de seguridad.

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.

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 y Gapps, siendo respectivamente una solución de software y otra de código abierto.

MyLenio

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

2.1.1. Organización del equipo [1]

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

2.1.1.1. Manejo de permisos

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

2.1.1.2. Documentos, capacitaciones y tareas

A cada uno de los miembros de un equipo se les puede asignar documentos, capacitaciones o tareas. Asignar documentos por este medio permite el cumplimiento del sistema de seguridad de la información y le facilita a los empleados firmar, de ser necesario. Asimismo, permite asignar capacitaciones y mostrar el progreso de estas, pudiendo notificar a los empleados que aún no la han completado. Análogamente, se le pueden asignar tareas a los empleados y notificarlos para que las terminen.

2.1.2. Recursos Humanos [2]

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

2.1.2.1. Incorporación de empleados

La integración con 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.

2.1.2.2. Participación y eficiencia del equipo

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

2.1.2.3. Reclutamiento

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

2.1.2.4. Información de los empleados

La información de cada empleado es guardad en 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.

2.1.3. Cumplimiento y Seguridad [3]

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

2.1.3.1. Reporte de Cumplimiento en Tiempo Real

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

2.1.3.2. Manejo de Inventario

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

2.1.3.3. Modelamiento de Procesos

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

2.1.3.4. Eventos Recurrentes y Automatización de Cumplimiento

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

2.1.3.5. Manejo de Riesgos

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

Gapps [4]

Gapps 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.

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.

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.

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.

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

Necesidad de un trabajo novedoso

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

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

Una consideración adicional radica en la viabilidad de comercializar esta aplicación a una amplia gama de clientes, tanto dentro de la misma industria como en otros sectores e incluso entre la competencia. La concepción de un software que no solo satisfaga las necesidades internas de Magnet, sino que también tenga potencial para ser implementado por otras organizaciones, amplía significativamente el alcance y la relevancia del proyecto.

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

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

3. 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 los estándares de la norma ISO 27001. Para lograr esto, se han definido varios módulos, cada uno con su conjunto de funcionalidades específicas. A continuación, se detalla la funcionalidad, historias de usuario y modelo de datos utilizado para cada uno de estos módulos: documentos, activos, riesgos y procesos.

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.

Perfiles de usuario del sistema

3.2.1. 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 marcar como leída las versiones de los documentos. No pueden editar información ni gestionar los datos del sistema.

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.

3.2.2. 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.

Módulo de Documentos

El módulo de documentos es donde se guarda toda la información que define al SGSI. La información se puede dividir en controles, categorías de controles, documentos y evidencia.

3.3.1. Controles

Los controles de seguridad son medidas implementadas para proteger datos e infraestructuras importantes 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.

3.3.2. 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.

3.3.3. 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 mantener 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.

3.3.4. 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.

3.3.5. 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 comité, quiero poder aprobar documentos, para validar su contenido.
7. Como usuario, quiero poder ver el listado de controles.
8. Como usuario, quiero poder ver el detalle de cada control.
9. Como usuario, quiero poder ver el detalle de cada documento.

3.3.6. Modelo de Datos

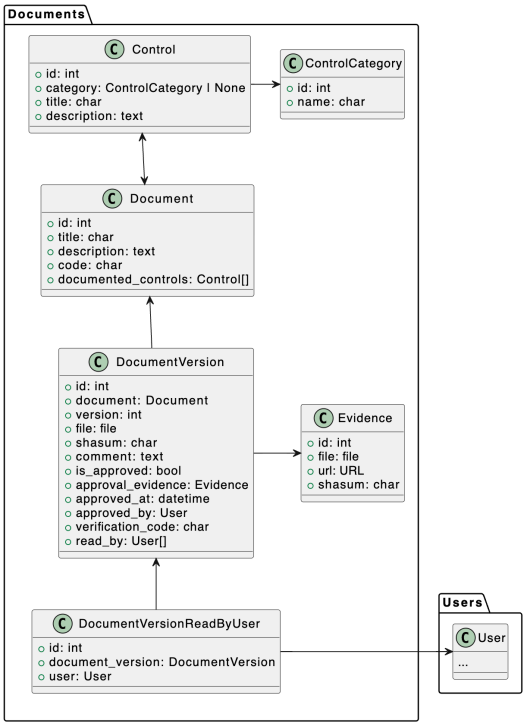

Figura 1: Modelo entidad-relación módulo de documentos

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. **Document**: guarda los datos de un documento.
   - `id`: el identificador único del documento.
   - `title`: el título del documento.
   - `description`: la descripción del documento.
   - `code`: el código del documento.
   - `documented_controls`: los controles que se encuentran documentados en el documento.
4. **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.
   - `file`: el archivo de la versión.
   - `shasum`: el hash (sha256) del archivo de la versión.
   - `comment`: comentario de la versión.
   - `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.
5. **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.
6. **Evidence**: guarda los datos de una evidencia.
   - `id`: el identificador único de la evidencia.
   - `file`: archivo de la evidencia.
   - `url`: URL de la evidencia.
   - `shasum`: el hash (sha256) del archivo o hiperenlace de la evidencia.

3.3.7. Interfaz de usuario

…

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 tipos de activos.

3.4.1. 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.

3.4.2. 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.

3.4.3. Historias de Usuario

1. Como administrador, quiero poder registrar activos de la empresa, para luego definir su riesgo asociado.
2. Como usuario, quiero poder ver el listado de activos.
3. Como usuario, quiero poder ver el detalle de cada activo.

3.4.4. Modelo de Datos

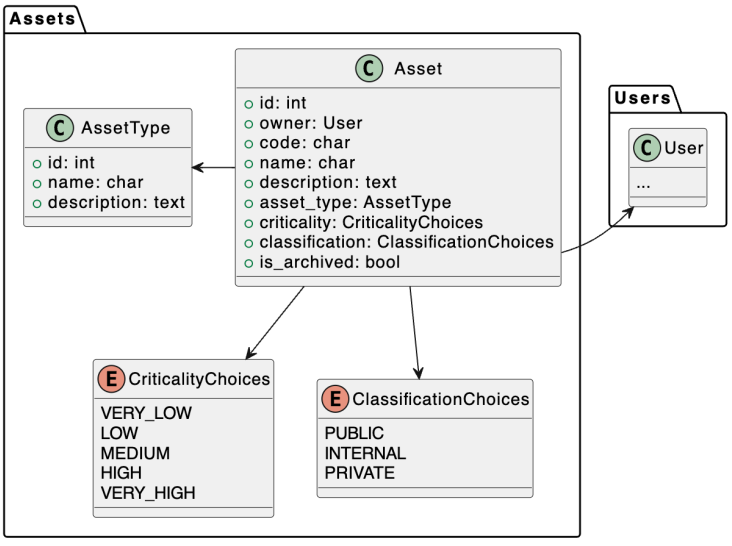

Figura 2: Modelo entidad-relación módulo de activos

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_type`: el tipo de 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.

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.

3.5.1. 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.

3.5.2. Historias de Usuario

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

3.5.3. Modelo de Datos

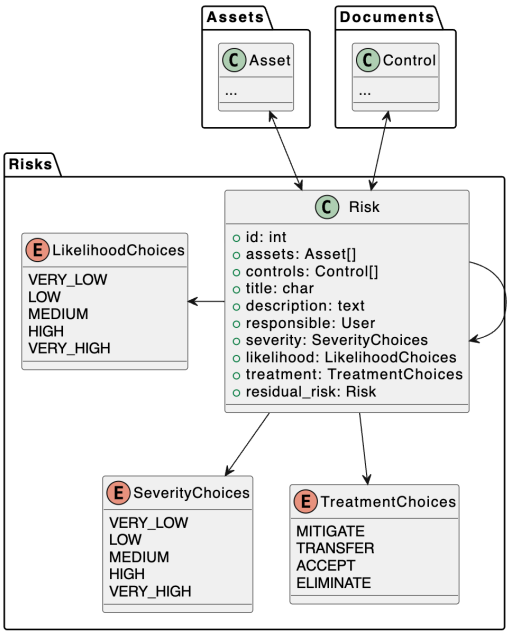

Figura 3: Modelo entidad-relación módulo de riesgos

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.

3.5.4. Interfaz de usuario

...

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.

3.6.1. Procesos

Los procesos son

3.6.2. Actividades

Las actividades son

3.6.3. Historias de Usuario

1. Como administrador, quiero poder definir procesos manuales para generar evidencia de cierto control.
2. Como administrador, quiero poder definir procesos recurrentes para generar evidencia de cierto control de manera periódica.
3. Como administrador, quiero poder asignar procesos a los usuarios directamente o indirectamente a través de grupos para generar evidencia de los controles.
4. Como usuario, quiero ser notificado al tener un nuevo proceso asignado para poder completarlo rápidamente.

3.6.4. Modelo de Datos

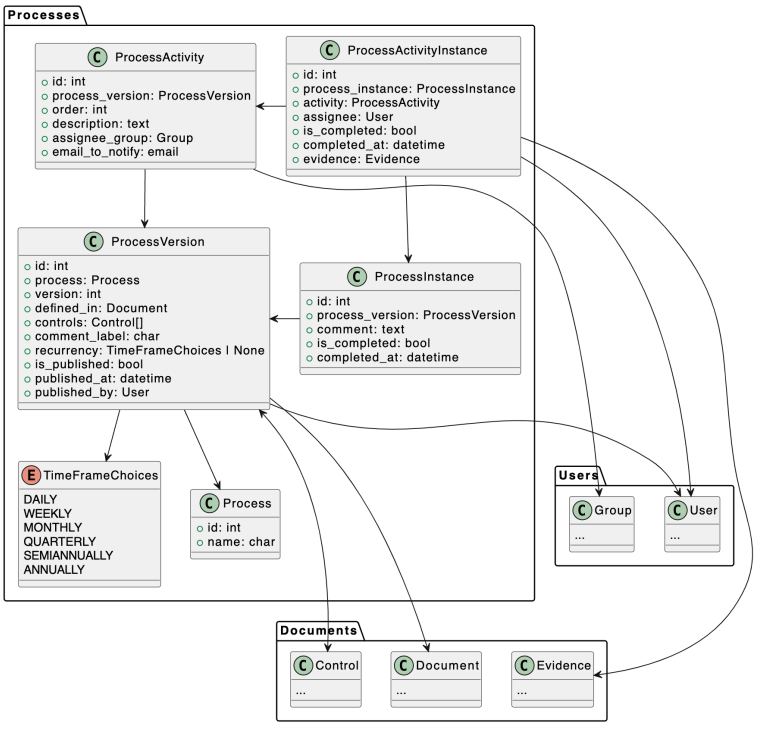

Figura 4: Modelo entidad-relación módulo de procesos

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 sé instancia el proceso, que puede ser `diariamente`, `semanalmente`, `mensualmente`, `trimestralmente`, `semi anualmente` o `anualmente`.
   - `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 publico 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.
   - `description`: la descripción de la actividad a realizar.
   - `asignee_group`: el grupo de usuarios entre los cuales se puede asignar la actividad cuando se inicia una instancia de esta.
   - `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 instance 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.
   - `asignee`: 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.

3.6.5. Interfaz de usuario

...

4. Evaluación

5. Conclusiones

Trabajo Futuro

Referencias

[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