Universidad Siglo 21

Trabajo Final de Grado. Prototipado Tecnológico

Sistema de Gestión de la Seguridad de la Información

Autor: Pablo Ezequiel Córdoba

DNI: 34747470

Legajo: VINF08284

Mendoza, abril de 2022

Índice

Índice de Diagramas

Índice de Tablas

Índice de Ilustraciones

Resumen

La seguridad de la información es una temática que ha ido tomando una relevancia cada vez mayor a lo largo de los años, a tal punto que las organizaciones privadas y entidades públicas han establecido criterios y requerimientos mínimos de seguridad que deben cumplir cualquier tipo de compañía que desee trabajar con ellas. A las pequeñas y medianas empresas que llevan poco tiempo en la implementación de estándares o certificaciones de seguridad, les resulta difícil encontrar un orden y una visión clara de en qué estado se encuentran respecto a estos, lo que suele producir frustraciones, trabajos adicionales y demoras, tanto para ponerlas en práctica como para ver sus resultados. Lo anterior mencionado, sumado a los altos costos que puede tener un servicio de consultoría, fue lo que me llevó a diseñar e implementar una aplicación que organice y brinde información clara y concisa para dichas organizaciones; dándoles una herramienta sólida donde establecer su sistema de gestión de seguridad de la información y que a su vez pueda servir para ver en qué estado se encuentran con respecto las distintas certificaciones, normas o estándares. El objetivo de este proyecto fue alcanzado con el desarrollo de una aplicación web que cumple los requisitos propuestos y permite brindarles a quienes usen la misma, un lugar donde centralizar todos los elementos de estas que están relacionados a la seguridad de la información.

Palabras clave: Seguridad de la Información, Riesgos, Aplicación Web.

Abstract

Information security is a topic that has become increasingly relevant over the years, to the point that private and public organizations have established minimum security requirements and criteria for any company that might want to work with them. Small and medium-sized enterprises that have been implementing security standards or certifications over a short period of time, may find exceedingly difficult to being well organized and have a clear vision on their status in relationship with those standards and certifications, which may result in frustrations, additional re-working, and delays both on the implementation and on the expected results. The mentioned above, and the high costs that consulting services can have, was what made me design and implement an application that can organize and provide clear and concise information for said organizations, giving them a solid tool to establish their information security management system and that allows them to see their real implementation level they have with the mentioned standards, certifications, and regulations. The project's objective was achieved with the development of a web application that meets the proposed requirements and allows to those who utilizes it a place to centralize all the elements that they might have that are related to information security.

Keywords: Information Security, Risks, Web application.

Título

Sistema de Gestión de la Seguridad de la Información

Introducción

A lo largo de los años la preocupación por la protección de la información ha ido incrementando debido a que, gracias a la aparición de herramientas como el internet, ha permitido que la misma sea transmitida con una mayor facilidad y con una reducción considerable de tiempos. Pero ese beneficio, vino con un costo oculto, el de tener que proteger la información para evitar que la misma caiga en manos equivocadas. El problema surge en cómo nos aseguramos de que la misma está correctamente protegida y si se estan siguiendo las recomendaciones, buenas prácticas y requerimientos que tienen los estándares de la industria. De aquí surge la necesidad de una herramienta que nos permita integrar todo lo relacionado al cumplimiento y nos permita afirmar que la información se encuentra dentro de un marco seguro.

Antecedentes

Desde principios de la historia, la información siempre ha tenido un valor importante, porque la misma le otorga cierto poder a quien la tenga por sobre los demás. Es por eso por lo que se ha buscado proteger a la misma utilizando todos los métodos disponibles que van desde intrincados algoritmos de encriptación, hasta protecciones físicas que no permitan su acceso.

No fue hasta los años 80, donde el internet comenzó a utilizarse en mayor medida, y donde comenzaron a surgir algunas buenas prácticas para proteger la información. Así fue el caso del Trusted Computer System Evaluation Criteria (TCSEC) que, si bien planteaba una serie de buenas prácticas requeridas dentro del gobierno de Estados Unidos, también era recomendada para empresas y organizaciones. Aunque la misma nunca tuvo mucho éxito, debido a que era de difícil o costosa aplicación. (Nemati, 2008)

El avance de las tecnologías y la masificación del uso del internet permitió un avance en la comunicación y la transmisión de la información a través de la red, escaló a valores muy altos. Pero esto trajo como problemática el tener que proteger la información, buscando establecer qué medidas y herramientas podían utilizarse para defenderla como lo enuncia Nemati et al. Pero no fue hasta pasados la mitad de los años noventa, que

comenzaron a trabajarse en estándares que permitían reunir una serie de herramientas y medidas a tomar, de forma que podamos proteger a la misma de una forma más estructurada y probada. Casos como el del Consorcio para la Investigación en Políticas y Seguridad de la Información (CRISP), donde el 1998 la NSA contactó a la Universidad de Stanford, con el fin de abordar dichas amenazas y establecer una serie de buenas prácticas. (May & Elliot, 2021)

Ya entrados en los años 2000, y con un incremento prácticamente exponencial de ataques a la seguridad de la información medido año a año, empezaron a surgir una serie de estándares y regulaciones de distintas entidades, que apuntaban a brindar un marco de protección, como lo son la serie ISO 27000, NERC, SSAE 16 (luego llamada SOC), instituciones como el NIST (Instituto Nacional de Estándares y Tecnología, por sus siglas en inglés), que desarrollan no solo estándares sino también recomendaciones y buenas prácticas o regulaciones como la reciente GDRP (Regulación General de Protección de Datos, por sus siglas en inglés) desarrollada en la Unión Europea, que dieron pie a actualizaciones en muchas leyes de países, como en el caso de nuestro país la Ley de Protección de Datos Personales. (Fitzgerald, 2018)

Descripción del Área Problemática

Las pequeñas y medianas empresas, cuando intentan implementar algún estándar, particularmente para el caso, de seguridad suelen encontrarse con muchos problemas para obtener información concreta y precisa de cómo hacerlo, teniendo que recurrir a costosas consultorías, con el fin de orientarse en la obtención de la información.

Sumado al problema mencionado anteriormente, tiende a existir poca organización respecto al manejo de la documentación, los controles, riesgos e incidentes. Causando que exista información desactualizada o poco precisa, falta o sobre controles, errores u omisiones a la hora de gestionar los riesgos e incidentes. Todo esto, produce que para que una empresa pueda realmente implementar dichos estándares deban pasar dos o tres años, solamente en preparación, y al menos un par de años más para comenzar a ver los resultados.

Justificación

Teniendo en cuenta los problemas planteados anteriormente, la herramienta busca dar una solución a las incongruencias, falta de organización y, por consecuente, posibles errores que se tengan a la hora de llevar un Sistema de Gestión de la Seguridad de la Información. Brinda una posibilidad de integración consistente entre todas las aristas que posee la gestión de la seguridad. Dando también un control más estricto de las actividades, tareas o recursos ya utilizados y los que faltan por poner en marcha.

Permite organizar el contenido de forma que el mismo sea de fácil entendimiento, acelerando los procesos y permitiendo realizar ajustes en un menor plazo, pudiendo ver los beneficios de las implementaciones más rápidamente. El resultado de esta es una declaración de la aplicabilidad mucho más clara y dinámica.

Los beneficios que brinda la utilización del desarrollo propuesto son:

- Permite integrar varias herramientas en una sola solución. Teniendo información más clara y concisa en un solo lugar.
- Brinda información precisa respecto al estado actual de la implementación de una certificación. Estableciendo que requerimientos se cumplen, cuales no y qué debería realizarse para los faltantes.
- Llevar un registro organizado de los controles realizados, pendientes y aquellos que deban repetirse, viendo fácilmente aquellos que fallaron.
- Centralizar toda la documentación en un solo repositorio, lo que permite tener un mejor control de esta, validando si se encuentran vigente, y pudiendo determinar cuáles de los mismos deben ser actualizados, o revalidados.
- Una gestión de riesgos e incidentes más ordenada, dándole a los usuarios la posibilidad de ver aquellos que hayan ocurrido, evidenciando que acciones se tomaron para la mitigación de estos y permitiendo un vínculo entre ambos (riesgos e incidentes) con el fin de medir la efectividad de las medidas tomadas.
- Lograr tener un control efectivo de los activos de información que se tienen en la organización, pudiendo caracterizar a los mismos en base a la importancia que tienen y cerciorarse que los mismos están protegidos correctamente.

Objetivo General del Proyecto

Diseñar y desarrollar una aplicación web, que permita a una organización establecer, implementar, mantener y mejorar su Sistema de Gestión de la Seguridad de la Información.

Objetivos Específicos del Proyecto

- Recopilar leyes, normas y estándares, que estén vinculadas o relacionadas a la seguridad de la información.
- Establecer un sistema para la gestión de riesgos e incidentes de una organización.
- Implementar un sistema de blockchain para validar la integridad de la documentación y archivos de la plataforma.
- Establecer un sistema de información que vincule los requerimientos de las normas con los demás artefactos para validar su cumplimiento.
- Desarrollar un sistema para la gestión de documentación de la organización relacionada a la seguridad de la información.

Marco Teórico Referencial

Dominio del Problema

Un Sistema de Gestión de Seguridad de la Información (SGSI, o en inglés ISMS) es definido por ISO (2018) como:

> El conjunto de políticas, procedimientos, lineamientos, actividades y recursos asociados, que son gestionados por una organización con el fin de proteger sus activos de la información. Un SGSI brinda a las organizaciones un enfoque sistemático para establecer, implementar, operar, revisar mantener y mejorar la seguridad de la información de una organización para lograr los objetivos de negocio. Toma como base la evaluación de riesgos y los niveles de aceptación de los riesgos de la organización, para tratar y gestionar efectivamente dichos riesgos. Analizando los requerimientos para la protección de los activos de información y aplicando los controles apropiados para asegurar la protección de dichos activos de información. (p. 11-12)

TICs

En el siguiente apartado, se hará una introducción a los conceptos teóricos que están relacionados a las tecnologías y la comunicación que fueron utilizadas para el desarrollo del proyecto.

El lenguaje de programación elegido para desarrollar esta herramienta fue Python. Dado el dinamismo que se requirió para el proyecto, se ha decidido utilizar un lenguaje que permita un desarrollo rápido de aplicaciones. “Python es un lenguaje de programación interpretado, orientado a objetos de alto nivel con semántica dinámica” (Python Software Foundation, s.f.).

La principal característica de este lenguaje es que su sintaxis ofrece la posibilidad de hacer un código legible fácilmente. Ese es uno de los principales puntos dentro de la filosofía de este. Además, el mismo funciona en múltiples plataformas, por lo que permite una versatilidad a la hora de hacer funcionar una aplicación en distintos dispositivos. Un dato importante para destacar sobre Python es que el mismo tiene licencia de código abierto, es decir que el código está disponible para que cualquier persona pueda consultarlo, estudiarlo y ofrecer modificaciones. Por lo que existen miles de colaboradores alrededor del mundo, que se dedican a verificar, validar y mejorar el lenguaje. (Python Software Foundation, s.f.)

Como entorno de trabajo, el elegido para trabajar fue Django. El mismo está orientado para el desarrollo de sitios web de una manera rápida y ágil.

Cuando hablamos de un entorno de trabajo, nos referimos a una serie de herramientas predefinidas, que nos permiten realizar ciertas actividades y tareas de una manera más sencilla, rápida y eficaz. De esta forma, nos evitamos tener que (re)hacer tareas repetitivas. Agilizando el proceso de programación. (Forcier, Bissex, & Chun, 2008)

Además, posee la capacidad de agregar módulos adicionales, de acuerdo con las necesidades que el proyecto tenga. Aumentando así la versatilidad de la herramienta.

Para guardar la información de la herramienta, se utilizará una base de datos MySQL. Es un gestor de base de datos relacional desarrollado, distribuido y mantenido

por Oracle. Utiliza SQL (Structured Query Language) como lenguaje para el acceso a las bases de datos.

El mismo, así como las otras dos herramientas para desarrollo utilizadas en el proyecto, es de código abierto. Es ampliamente utilizado debido a su versatilidad y facilidad para ser utilizado tanto en entornos en la nube como en entornos on-premise.

Finalmente, para asegurarnos que la documentación y archivos que sean subidos a la plataforma, son almacenados de manera segura y no son modificados o alterados durante su almacenamiento, se utiliza la tecnología blockchain. Según Laurence (2017) un blockchain (cadena de bloques, en inglés) es una estructura de datos que hace posible la creación de una especie de libro contable de datos y compartirlo a través de una red de personas o sistemas independientes. La tecnología blockchain usa la criptografía para permitir a cada participante de la red, gestionar dichos "libros contables" de forma segura, sin tener la necesidad de una autoridad central que aplique las reglas.

Competencia

En el siguiente apartado, se enuncian y comentan herramientas de la competencia.

Eramba es una aplicación de GRC que ayuda con el cumplimiento, gestión de riesgos, prueba de controles, manejo de excepciones, etc. (Eramba, s.f.). Cada uno de estos módulos puede ser trabajado de forma independiente o relacionados entre sí, con el fin de asegurarse el cumplimiento de los estándares definidos por la organización implementadora.

Por otro lado, una herramienta muy similar es KCM-GRC, de la empresa KnowBe4. Esta herramienta posee cuatro módulos principales, que son el de Gestión de cumplimiento, Gestión de Políticas, Gestión de Riesgos y Gestión de riesgos de proveedores. KCM es una plataforma de GRC que ayuda efectiva y eficientemente a manejar riesgos y el cumplimiento dentro de la organización y a través de la seguridad de los proveedores, mientras se visualizan los vacíos dentro del programa interno de seguridad. (KnowBe4, s.f.)

Resulta difícil realmente compararlas, debido a que las organizaciones suelen optar por alternativas desarrolladas internamente o adaptaciones de otras herramientas,

como planillas, Sharepoint, Jira, RedMine, entre otros, que son adaptadas para el uso de esta, sin terminar de ser específicamente desarrolladas para dicho uso.

Diseño Metodológico

Herramientas metodológicas

Para el desarrollo se decidió utilizar como metodología ágil de desarrollo, Scrum. En su definición nos explica que es una estrategia flexible donde todo el equipo de desarrollo, incluyendo al cliente, trabajará buscando un fin en común. (Blockhead, 2016). Su característica es que realiza ciclos con validaciones tempranas con el cliente, con el fin de asegurarnos que lo desarrollado coincide con lo que el cliente está buscando. Cada uno de estos ciclos es llamado Sprint. Usualmente, tienen una duración de entre dos y cuatro semanas.

Herramientas de desarrollo

Para el desarrollo de esta aplicación se utilizó el lenguaje de programación Python, trabajando el mismo utilizando el framework Django. Sumado a este framework, se lo acompañó de Flask para la utilización de blockchain. Y finalmente se utilizó el motor de base de datos de MySQL para el acceso a los datos.

Elementos de la recolección de datos

Con el fin de obtener un listado de cuáles son los estándares más implementados, se consultó a tres responsables de las áreas de seguridad de distintas organizaciones. Dos de ellas relacionadas al Software y una de ellas al segmento bancario. Con la información provista por los expertos y sumando la documentación de apoyo de estándares y certificaciones, como son ISO 27001, SOC 2, FedRAMP, Microsoft 365 y leyes o reglamentaciones como GDPR, LGPD y la Ley de Protección de Datos argentina, sirvieron como base para la obtención de los distintos requerimientos y objetivos que deben ser cumplidos por las organizaciones para asegurar y proteger la seguridad de la información.

Planificación del proyecto

El proyecto fue planificado utilizando un diagrama de Gantt, el cual permite visualizar las tareas fácilmente.

ID	Title	Start Time	End Time	Predecessor
1	Selección de la temática	03/22/2021	04/09/2021	
2	Introducción	04/09/2021	04/12/2021	1
3	Justificación	04/12/2021	04/14/2021	2
4	Objetivo General del Proyecto	04/14/2021	04/15/2021	3
5	Objetivos Específicos del Proyecto	04/15/2021	04/17/2021	4
6	Marco Teórico Referencial	04/17/2021	04/22/2021	5
7	Diseño Metodológico	04/22/2021	04/25/2021	6
8	Relevamiento	04/25/2021	04/28/2021	3
9	Procesos de Negocio	04/28/2021	05/02/2021	8
10	Diagnóstico	05/03/2021	5/5/2021	7,4,5
11	Propuesta	05/06/2021	5/9/2021	8
12	Objetivo General del sistema	5/10/2021	5/11/2021	9
13	Límites	5/12/2021	05/14/2021	10
14	Alcances	05/15/2021	05/17/2021	10
15	Historias de usuarios	05/18/2021	05/23/2021	10,11,12
16	Diagramas	05/23/2021	05/24/2021	10,11,12
17	Seguridad	05/25/2021	05/31/2021	14
18	Riesgos	6/1/2021	6/6/2021	13,14
19	Costos	6/7/2021	6/10/2021	16
20	Conclusiones	6/11/2021	06/13/2021	17
21	Codificación del prototipo	6/1/2021	7/4/2021	17

Diagrama 1 - Fuente: Elaboración propia

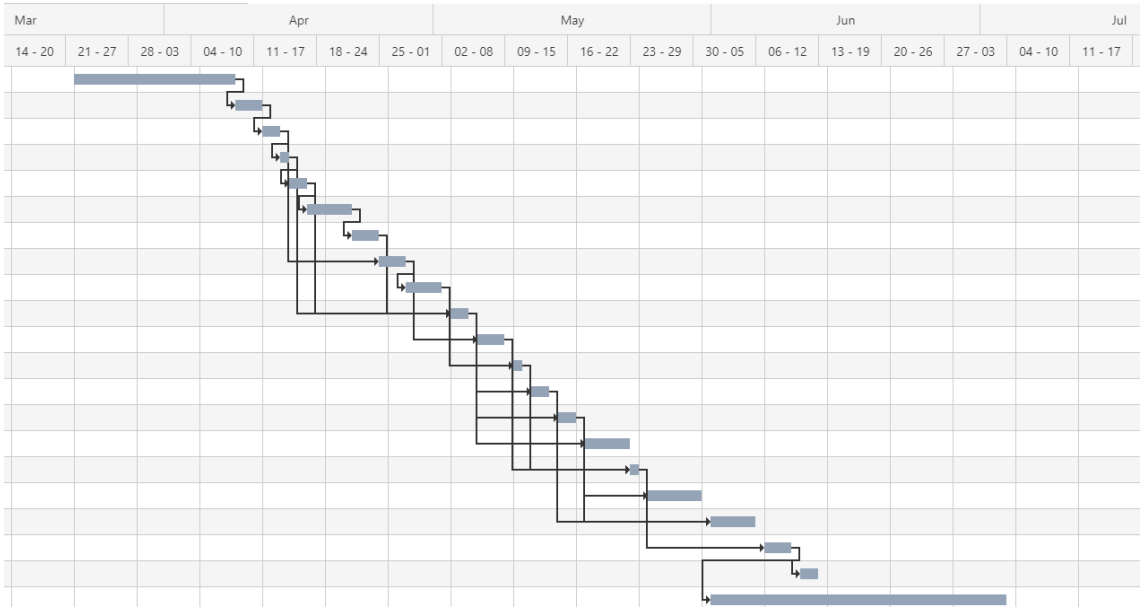


Diagrama 2- Fuente: Elaboración Propia

Relevamiento

Relevamiento Estructural

Debido a que el proyecto que no está dirigido específicamente para una organización en particular no es posible fijar una localización ni componentes de esta. Este tipo de herramientas es aplicado en aquellas que ya hayan certificado o implementado algún estándar de seguridad o tengan intenciones de hacerlo.

En el relevamiento realizado, se pudo observar que en general estas empresas poseen grupos reducidos de personas (entre 2 a 6 personas) y que trabajan con el soporte o colaboración de otras áreas. Usualmente, el nombre que recibe el área que utiliza la herramienta, posee el nombre de Cumplimiento (Compliance, en inglés).

Relevamiento Funcional

Al tratarse de una aplicación que puede ser aplicada en distintas instituciones y que no todas siguen la misma estructura jerárquica, se presenta a continuación un organigrama de la estructura estándar que suelen estar presente en la gran mayoría de ellas.

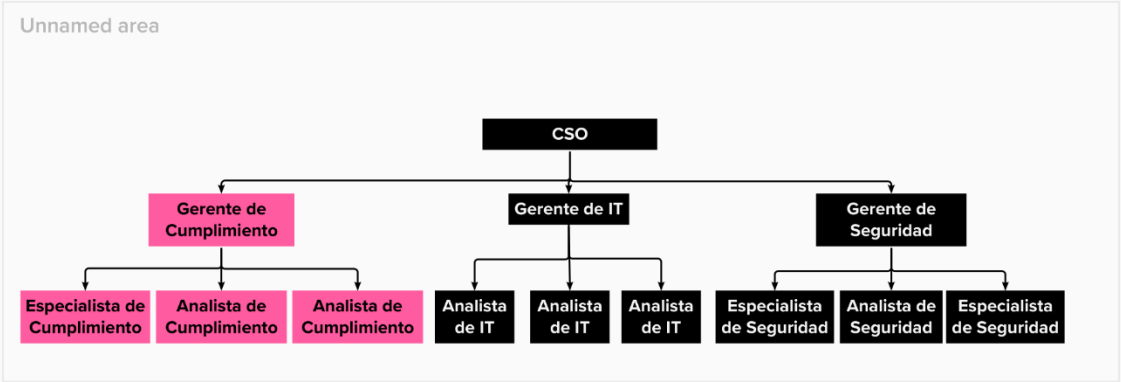


Diagrama 3 - Fuente: Elaboración Propia

Funciones del área implicada:

El área de compliance o cumplimiento, suele tener asignadas diversas tareas entre las que se incluyen: asegurarse del cumplimiento normativo existente en la organización, gestión de los procesos, políticas y procedimientos implementados en la organización para dicho cumplimiento, la identificación, gestión y prevención de riesgos e incidentes, realización y monitoreo de los controles existentes en la organización con el fin de informar desviaciones existentes respecto a los procesos y finalmente, la tarea de ser punto de consultas respecto a las distintas normas, estándares y regulaciones existentes que puedan impactar a la organización.

Respecto a los procesos que lleva el área, es posible identificar los siguientes:

1. Gestión de documentación
2. Gestión de riesgos
3. Gestión de incidentes
4. Ejecución de controles
5. Cumplimiento de normas, estándares y regulaciones implementadas o a implementar.

Proceso: Gestión de la documentación

- **Roles:**
    - Personal de Compliance (PC)
    - Personal de otras áreas (POA)
    - Repositorio de documentación (RD)
- **Pasos:**

El personal de compliance revisa en la RD si existe ya existe un documento anterior que deba ser modificado o si debe realizarse uno nuevo. El PC se reúne con el POA y establecen los lineamientos que debe tener el nuevo documento o las modificaciones a realizar. El documento es realizado por el PC o el POA, dependiendo de quién es el responsable del documento y, una vez finalizado se sube a la RD (por ejemplo, Sharepoint, Google Drive, etc.). Se establece cuándo se revisará nuevamente y se repite el proceso.

Proceso: Gestión de Riesgos

- **Roles:**
    - Personal de compliance (PC)
    - Responsables de otras áreas (ROA)
    - Planilla de riesgos (PR)
- **Pasos:**

Anualmente, el PC se reúne con cada ROA y definen los riesgos que impactan en la misma. De cada riesgo, se define: Probabilidad, Impacto y Exposición. Junto con esto, se definen que acciones, controles, políticas y procedimientos son utilizados para minimizar ya sea el impacto o la probabilidad. Una vez definidos los riesgos del área, los mismos son registrados en la PR (usualmente una planilla de Excel o Google Drive).

Proceso: Gestión de Incidentes

- **Roles:**
    - Personal de Compliance (PC)
    - Personal de otras áreas (POA)
    - Planilla de incidentes (PI)
- **Pasos:**

Cada vez que ocurre un incidente, el mismo es reportado por POA y se reúnen junto con el PC y documentan el incidente en la PI, con los datos: Tipo de incidente, fecha que ocurrió, Descripción del incidente, Impacto, Responsable, Acciones Correctivas y Acciones Preventivas.

Proceso: Validación de controles

- **Roles:**
    - Personal de Compliance (PC)
    - Personal de otras áreas (POA)
    - Planilla de Listado de controles (PLC)
    - Herramienta a controlar (HC)
- **Pasos:**

El PC revisa de la PLC que controles deben ser realizados, y se reúne con el POA para solicitarle las evidencias, registros, capturas o documentación de la HC que permita realizar el control. El PC recibe la evidencia y valida el cumplimiento del control. Una vez realizado el mismo, se registra en la PLC: La herramienta revisada, quién fue el POA con el que se realizó, la evidencia registrada y el resultado del control. Dependiendo del resultado, se evalúa cuándo se realizará nuevamente el control. La evidencia queda almacenada en algún repositorio de la organización (por ejemplo: Google Drive, Sharepoint, Dropbox, etc.).

Proceso: Cumplimiento de Normas, Estándares y Regulaciones

- **Roles:**
    - Personal de Compliance (PC)
    - Declaración de Aplicabilidad o similar (DA)
    - Estándar, Norma o Regulación (ENR)
- **Pasos:**

El Personal de Compliance consulta el/los ENR que la organización ha implementado o desea implementar y genera un documento de DA donde tenga registrados los requerimientos o controles que deben ser cumplidos y registra las políticas, procesos, controles y herramientas que permitan cumplir dichos requerimientos o controles. Usualmente la DA suele ser una planilla.

Relevamiento de Documentación

A continuación, lista los documentos relevados en los procesos previamente mencionados:

- **Planilla de Riesgos:** Es el documento donde se registran los riesgos de una organización. (Anexo 1)
- **Planilla de incidentes:** Es utilizada para registrar los incidentes y las acciones tomadas sobre los mismos. (Anexo 2)
- **Planilla de listado de controles:** Es el listado de los controles que deben realizarse para cierto período. (Anexo 3)
- **Declaración de Aplicabilidad:** Permite identificar los controles o requerimientos de normas, estándares y regulaciones y asociarlos a las políticas, procedimientos, procesos y controles que tiene la organización. (Anexo 4)

Procesos del Negocio

A continuación, se presenta el diagrama 4, el cual muestra el modelado de los procesos mencionados en el relevamiento funcional.

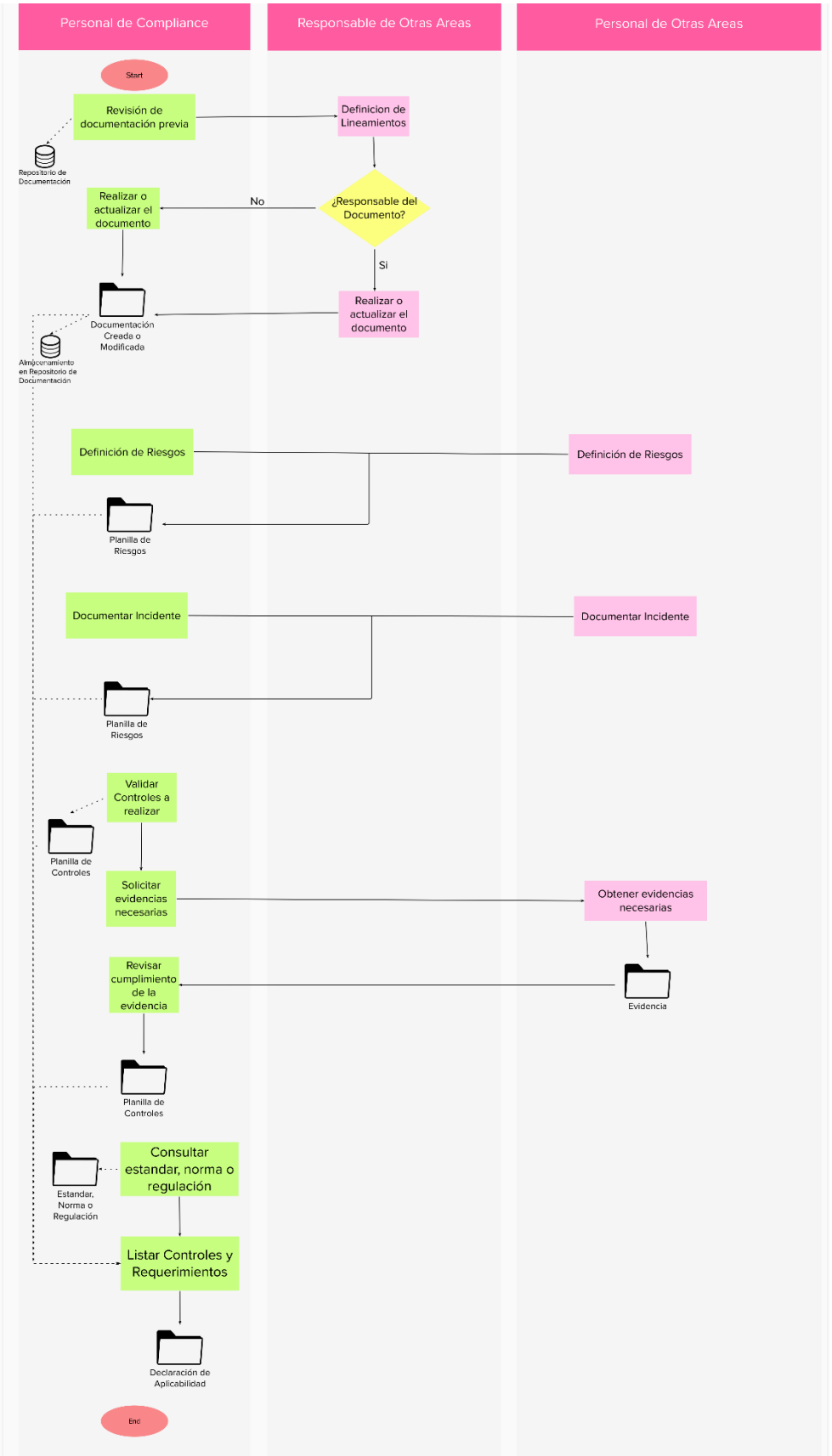


Diagrama 4 - Fuente: Elaboración Propia

Diagnóstico y Propuesta

Tabla 1 - Fuente: Elaboración Propia

Nombre del proceso: Gestión de la documentación	
Problemas	***Causas***
Pueden existir documentos que no hayan tenido revisiones periódicas	Debido a la existencia de una gran cantidad de documentación o alguna forma de establecer recordatorios para cada documento
Los documentos pueden ser modificados sin la autorización o aprobación de su responsable	Debido a que no todos los sistemas donde se almacena la documentación tienen los registros de las fechas que éstos han sido modificados

Tabla 2 - Fuente: Elaboración Propia

Nombre del proceso: Gestión de riesgos	
Problemas	***Causas***
Existen riesgos que pueden no ser revisados periódicamente	Al no tener una clara muestra de cuándo han sido agregados o actualizados los riesgos, no es posible saber si deben ser revisados o no
Pueden existir riesgos que no posean acciones para minimizar su impacto o probabilidad	Si bien existe una columna en la planilla para completarlo, no es posible saber si dichas acciones siguen vigentes o no
No es posible medir la efectividad de las medidas tomadas	Al realizar revisiones anuales, la medición de los riesgos se realiza a modo de “foto” en el momento que fue obtenido y no modificado hasta la próxima evaluación.
No es posible saber si alguien realizó cambios en la planilla	No existe un registro de los cambios y/o modificaciones que se realizaron a la misma

Tabla 3 - Fuente: Elaboración Propia

Nombre del proceso: Gestión de Incidentes	
Problemas	***Causas***
Los incidentes pueden no ser actualizados con nueva información	Si existió nueva información sobre los incidentes, o había información faltante, puede no ser llenada nunca
No es posible saber si alguien realizó cambios en la planilla	No existe un registro de los cambios y/o modificaciones que se realizaron a la misma
Las acciones correctivas y preventivas pueden no ser efectivas	No se mide la efectividad de las acciones tomadas
No se puede saber si los incidentes ocurridos ya han sido registrados como riesgos que tengan medidas para que no se produzcan	No existe vinculación entre los incidentes y los riesgos

Tabla 4 - Fuente: Elaboración Propia

Nombre del proceso: Validación de controles	
Problemas	***Causas***
Pueden existir controles que se estén realizando para mitigar un riesgo que ya no existe.	No existe vinculación entre los riesgos y controles que se estén realizando.

Tabla 5 - Fuente: Elaboración Propia

Nombre del proceso: Cumplimiento de Normas, Estándares y Regulaciones	
Problemas	***Causas***
Los controles, herramientas, procesos y políticas pueden ya no estar siendo utilizados.	Existencia de información no actualizada en las distintas herramientas
Falta de cumplimientos de requerimientos de las normas.	Falta de claridad en los listados de requerimientos, y la existencia de información no existente.

Propuesta

Se realizó la propuesta de una herramienta con el fin de resolver los problemas que fueron mencionados. La misma consiste en una aplicación que integre todos estos procesos en una sola aplicación, permitiendo administrar desde la misma su Sistema de Gestión de la Seguridad de la Información. De esta forma, teniendo todo agrupado en un solo sitio, nos permite no solo no depender de tantas herramientas, sino que también tener un mejor control de los distintos procesos. Permite la configuración de alertas que puedan solicitar la revisión de dicha información que se encuentre cargada luego de un período de tiempo para que la misma se mantenga actualizada. La aplicación permite la vinculación entre la información existente entre cada uno de los procesos permitiendo visualizar fácilmente cuando dicha información ya no se encuentra existente.

La gestión de la documentación logra la integridad de esta, utilizando la tecnología de blockchain para tener un registro fehaciente de los cambios realizados en la documentación, certificando y validando el o la responsable de los cambios realizados y la fecha de estos. Esta tecnología también es utilizada para la información que se almacena en los controles, asegurándonos que la misma no ha sido modificada sin la autorización correspondiente. Las alertas mencionadas anteriormente, también pueden ser utilizadas en los controles, con el fin de establecer fechas limitantes para la realización de estos y que dicha fecha no llegue a su vencimiento.

Permite la administración de riesgos e incidentes de forma sistemática, logrando que se pueda evitar omisiones no intencionales. Además, con la vinculación entre ambos es posible medir la efectividad de las acciones tomadas.

Finalmente, toda esta información se vincula con los distintos puntos de las normas que posee el sistema, teniendo así mayor claridad respecto a qué requerimientos o controles de las normas se están cumpliendo y cuáles no. Dándonos como resultado una declaración de la aplicabilidad con información clara y actualizada.

Objetivos, límites y alcances del prototipo

Objetivos

Desarrollar un sistema que permita establecer y administrar un Sistema de Gestión de la Seguridad de la Información.

Limites

El sistema se encuentra delimitado desde la administración de documentación, activos de información, riesgos, incidentes y controles hasta la vinculación de dichos objetos con las normas.

Alcance

El prototipo contempla los siguientes procesos:

- Gestión de la documentación
- Gestión de riesgos
- Gestión de incidentes
- Gestión de controles
- Gestión de activos de información
- Cumplimiento de normas, estándares y Regulaciones
- Administración de usuarios

No contempla

Los siguientes procesos no son contemplados:

- Sistema de notificaciones
- Implementación de Blockchain para validar documentos y archivos subidos.

Descripción del sistema

Product Backlog

Tomando en consideración todas las historias de usuarios que pertenecen al prototipo de la aplicación, se elaboró el product backlog. La siguiente tabla enumera cada una de las actividades a realizar, con un número de identificación, su nombre, la prioridad que posee, los puntos estimados siguiendo una sucesión de Fibonacci y finalmente las posibles dependencias que existan entre las mismas.

Tabla 6 - Product Backlog

ID	Historia de Usuario	Prioridad	Puntos de Historia	Dependencias
US-001	ABM Usuarios	Alta	5	
US-002	Ingreso de usuario	Alta	1	US-001
US-003	Creación de documentación	Alta	3	
US-004	Modificación documentación	Media	1	US-003
US-005	Eliminación de documentación	Media	1	US-003
US-006	Listado de documentos	Media	1	US-003
US-007	Creación de nuevo riesgo	Alta	3	
US-008	Modificación de riesgo	Media	1	US-008
US-009	Eliminación de riesgo	Media	1	US-008
US-010	Visualización de listado de riesgos	Media	1	US-008
US-011	Creación de nuevo incidente	Alta	3	
US-012	Modificación de incidente	Media	1	US-012
US-013	Eliminación de incidente	Media	1	US-012
US-014	Visualización de listado de incidentes	Media	1	US-012
US-015	Vinculación riesgo-incidente	Baja	1	US-012, US-009
US-016	Creación de nuevo activo de información	Media	3	
US-017	Modificación de activo de información	Baja	1	US-017
US-018	Eliminación de activo de información	Baja	1	US-017
US-019	Visualización de listado de activos de información	Baja	1	US-017
US-020	Vinculación activo - incidente	Baja	1	US-017, US-013

US-021	Vinculación activo - riesgo	Baja	1	US-017, US-009
US-022	Creación de nuevo control	Alta	3	
US-023	Modificación de control	Alta	1	US-023
US-024	Visualización de listado de controles	Alta	1	US-023
US-025	Realización del control	Alta	3	US-023, US-024
US-026	Carga de archivos en controles	Media	3	US-023, US-024
US-027	Asignación de controles a usuarios	Baja	1	US-023, US-024, US-001
US-028	Vinculación control - riesgo	Media	1	US-023, US-008
US-029	Calculo exposición riesgo	Alta	3	US-023, US-024
US-030	Listado de normas	Baja	1	
US-031	Listado de controles de normas/estándar	Baja	1	
US-032	Detalle de controles de normas/estándar	Baja	1	
US-033	Vinculación control de normas - Control	Baja	1	US-023, US-036
US-034	Vinculación control de normas - Documentación	Baja	1	US-023, US-036
US-035	Vinculación control de normas - Activo	Baja	1	US-023, US-036
US-036	Detalle de cumplimiento de norma/estándar	Baja	1	US-036, US-037, US-038

Historias de Usuario

Tabla 7 - Fuente: Elaboración Propia

ID	US-001	**Nombre**	ABM Usuarios
Descripción	Como usuario administrador quiero crear, modificar o eliminar a otros usuarios para que puedan usar la plataforma o quitarles el acceso		
Criterios de Aceptación	1. Dado un usuario administrador, cuando cargo un usuario que ya se encuentra existente, entonces el sistema muestra un error 2. Dado un usuario administrador, cuando la contraseña no cumple los requisitos de: 8 o más caracteres, una mayúscula, una minúscula y un alfanumérico especial, entonces el sistema muestra un error. 3. Dado un usuario administrador, cuando completo los datos, si falta un campo al registrar el usuario o al modificarlo, entonces el sistema mostrará un error que todos deben ser completados. 4. Dado un usuario administrador, cuando exista un error al eliminar un usuario, entonces el sistema mostrará el error encontrado. 5. Dado un usuario administrador, cuando el usuario es creado o modificado correctamente, entonces el sistema muestra un mensaje.		
Prioridad	Alta	**Puntos de historia estimados**	5

Tabla 8 - Fuente: Elaboración Propia

ID	US-002	**Nombre**	Ingreso de usuarios
Descripción	Como usuario quiero iniciar sesión para utilizar el sistema		
Criterios de Aceptación	1. Dado un usuario, cuando el mismo es inexistente o ingresa una contraseña errónea, entonces el sistema muestra error de usuario o contraseña inválidos. 2. Dado un usuario existente, cuando se ingresa el usuario y la contraseña son correctos entonces accederá al sistema.		
Prioridad	Alta	**Puntos de historia estimados**	1

Tabla 9 - Fuente: Elaboración Propia

ID	US-003	**Nombre**	Creación de documentación
Descripción	Como usuario, quiero cargar en el sistema una documentación de la organización para agregarla a la biblioteca		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado, cuando no se adjunta un archivo, entonces el sistema muestra un error. 3. Dado un usuario logueado, cuando se completan todos los campos y se adjunta un archivo, entonces el sistema muestra un mensaje confirmando que el documento fue creado.		
Prioridad	Alta	**Puntos de historia estimados**	3

Tabla 10 - Fuente: Elaboración Propia

ID	US-004	**Nombre**	Modificación documentación
Descripción	Como usuario, quiero modificar una documentación de la organización ya agregada anteriormente para actualizarla		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado, cuando no se adjunta un archivo, entonces el sistema muestra un error. 3. Dado un usuario logueado, cuando se completan todos los campos y se adjunta un archivo, entonces el sistema muestra un mensaje confirmando que el documento fue modificado.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 11 - Fuente: Elaboración Propia

ID	US-005	**Nombre**	Eliminación de la documentación
Descripción	Como un usuario logueado, quiero eliminar un documento en existente en la plataforma para que no pueda ser accesible.		
Criterios de Aceptación	1. Dado un usuario logueado y un documento cargado, cuando se elimina el documento, el sistema muestra un mensaje de éxito en la operación. 2. Dado un usuario logueado y un documento cargado, cuando no fue posible eliminar el documento, el sistema muestra un mensaje de error.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 12 - Fuente: Elaboración Propia

ID	US-006	**Nombre**	Listado de documentos
Descripción	Como usuario, quiero consultar el listado de documentos para acceder a ellos		
Criterios de Aceptación	1. Dado un usuario logueado, cuando existe al menos un documento cargado, entonces se muestra el nombre de cada documento existente. 2. Dado un usuario logueado, cuando no existe ningún documento cargado, entonces se muestra un mensaje indicando la inexistencia de documentos cargados.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 13 - Fuente: Elaboración Propia

ID	US-007	**Nombre**	Creación de nuevo riesgo
Descripción	Como usuario, quiero agregar un nuevo riesgo en la plataforma para darle seguimiento		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado, cuando se completan todos los campos, el sistema muestra un mensaje confirmando que el riesgo fue creado.		
Prioridad	Alta	**Puntos de historia estimados**	3

Tabla 14 - Fuente: Elaboración Propia

ID	US-008	**Nombre**	Modificación de riesgo
Descripción	Como usuario, quiero modificar un riesgo existente en la plataforma para actualizar su información		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, el sistema muestra un error. 2. Dado un usuario logueado, cuando se completan todos los campos, el sistema muestra un mensaje confirmando que el riesgo fue modificado.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 15 - Fuente: Elaboración Propia

ID	US-009	**Nombre**	Eliminación de riesgo
Descripción	Como usuario, quiero eliminar un riesgo existente en la plataforma para que no se tenga más acceso a él		
Criterios de Aceptación	1. Dado un usuario logueado y un riesgo cargado, cuando se elimina el riesgo y se muestra un mensaje de éxito en la operación. 2. Dado un usuario logueado y un riesgo cargado, cuando no se elimina el riesgo se muestra un mensaje de error.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 16 - Fuente: Elaboración Propia

ID	US-010	**Nombre**	Visualización de listado de riesgos
Descripción	Como usuario quiero ver el listado de todos los riesgos existentes en la plataforma para consultarlos		
Criterios de Aceptación	1. Dado un usuario logueado y al menos un riesgo cargado, cuando quiero ver los riesgos existentes, entonces el sistema muestra el nombre de cada riesgo existente. 2. Dado un usuario logueado y ningún riesgo cargado, cuando quiero ver los riesgos existentes, entonces el sistema muestra un mensaje indicando la inexistencia de riesgos cargados.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 17 - Fuente: Elaboración Propia

ID	US-011	**Nombre**	Creación de un nuevo incidente
Descripción	Como usuario, quiero crear un nuevo incidente en la plataforma para darle seguimiento		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado, cuando se completan todos los campos, entonces el sistema muestra un mensaje confirmando que el riesgo fue creado.		
Prioridad	Alta	**Puntos de historia estimados**	3

Tabla 18 - Fuente: Elaboración Propia

ID	US-012	**Nombre**	Modificación de un incidente
Descripción	Como usuario, quiero modificar un incidente existente en la plataforma para actualizar su información		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado, cuando se completan todos los campos, entonces el sistema muestra un mensaje confirmando que el riesgo fue modificado.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 19 - Fuente: Elaboración Propia

ID	US-013	**Nombre**	Eliminación de incidente
Descripción	Como usuario, quiero eliminar un incidente existente en la plataforma para que no se tenga más acceso a él		
Criterios de Aceptación	1. Dado un usuario logueado y un riesgo cargado, cuando se elimina el incidente, entonces el sistema muestra un mensaje de éxito en la operación. 2. Dado un usuario logueado y un riesgo cargado, cuando no se puede eliminar el incidente, entonces el sistema muestra un mensaje de error.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 20 - Fuente: Elaboración Propia

ID	US-014	**Nombre**	Visualización de listado de incidentes
Descripción	Como usuario quiero ver el listado de todos los incidentes existentes en la plataforma para consultarlos		
Criterios de Aceptación	1. Dado un usuario logueado y al menos un incidente cargado, cuando quiero consultar el listado de incidentes, entonces el sistema muestra el nombre de cada riesgo existente. 2. Dado un usuario logueado y ningún riesgo existente, cuando quiero consultar el listado de incidentes, entonces el sistema muestra un mensaje indicando la inexistencia de riesgos cargados.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 21 - Fuente: Elaboración Propia

ID	US-015	**Nombre**	Vinculación Riesgo-Incidente
Descripción	Como usuario quiero actualizar un incidente cargado para vincularlo con un riesgo cargado		
Criterios de Aceptación	1. Dado un usuario logueado, un incidente y un riesgo cargado, cuando ambos son asociados, entonces el sistema vincula el riesgo con el incidente.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 22 - Fuente: Elaboración Propia

ID	US-016	**Nombre**	Creación de un nuevo Activo de Información
Descripción	Como usuario, quiero crear un nuevo activo de información en la plataforma para darle seguimiento		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado, cuando se completan todos los campos, entonces el sistema muestra un mensaje confirmando que el activo fue creado.		
Prioridad	Media	**Puntos de historia estimados**	3

Tabla 23 - Fuente: Elaboración Propia

ID	US-017	**Nombre**	Modificación de un activo de información
Descripción	Como usuario, quiero modificar un activo de información existente en la plataforma para actualizar su información		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado, cuando se completan todos los campos, entonces el sistema muestra un mensaje confirmando que el activo fue modificado.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 24 - Fuente: Elaboración Propia

ID	US-018	**Nombre**	Eliminación de activo de información
Descripción	Como usuario, quiero eliminar un activo de información existente en la plataforma para que no se tenga más acceso a él		
Criterios de Aceptación	1. Dado un usuario logueado y un activo de información cargado, quiero eliminar el incidente, entonces el sistema muestra un mensaje de éxito en la operación. 2. Dado un usuario logueado y un activo de información cargado, cuando no se elimina el activo de información, entonces el sistema se muestra un mensaje de error.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 25 - Fuente: Elaboración Propia

ID	US-019	**Nombre**	Visualización de listado de activo de información
Descripción	Como usuario quiero ver el listado de activos de información para consultarlos		
Criterios de Aceptación	1. Dado un usuario logueado y al menos un activo de información cargado, cuando quiero ver el listado, entonces el sistema muestra el nombre de cada activo de información existente. 2. Dado un usuario logueado y ningún activo de información existente, cuando quiero consultar el listado de activos, entonces el sistema muestra un mensaje indicando la inexistencia de activos de información cargados.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 26 - Fuente: Elaboración Propia

ID	US-020	**Nombre**	Vinculación Activo-Incidente
Descripción	Como usuario quiero actualizar un Incidente cargado para vincularlo con un Activo cargado		
Criterios de Aceptación	1. Dado un usuario logueado, un activo y un incidente cargado, cuando quiero asociar el activo con el incidente, entonces el sistema asocia el activo con el incidente.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 27 - Fuente: Elaboración Propia

ID	US-021	**Nombre**	Vinculación Activo-Riesgo
Descripción	Como usuario quiero actualizar un Riesgo cargado para vincularlo con un Activo cargado		
Criterios de Aceptación	1. Dado un usuario logueado, un activo y un riesgo cargado, cuando quiero asociar el activo con el riesgo, entonces el sistema asocia el activo con el riesgo.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 28 - Fuente: Elaboración Propia

ID	US-022	**Nombre**	Creación de un nuevo Control
Descripción	Como usuario, quiero crear un nuevo control en la plataforma para darle seguimiento		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado, cuando se completan todos los campos, entonces el sistema muestra un mensaje confirmando que el control fue creado.		
Prioridad	Alta	**Puntos de historia estimados**	3

Tabla 29 - Fuente: Elaboración Propia

ID	US-023	**Nombre**	Modificación de un control
Descripción	Como usuario, quiero modificar un control existente en la plataforma para actualizar su información		
Criterios de Aceptación	1. Dado un usuario logueado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado, cuando se completan todos los campos, entonces el sistema muestra un mensaje confirmando que el control fue modificado.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 30 - Fuente: Elaboración Propia

ID	US-024	**Nombre**	Visualización de listado de controles
Descripción	Se muestra el listado de todos los controles existentes en la plataforma		
Criterios de Aceptación	1. Dado un usuario logueado y al menos un control cargado, se muestra el nombre de cada control existente. 2. Dado un usuario logueado y ningún control existente, Se muestra un mensaje indicando la inexistencia de controles cargados.		
Prioridad	Alta	**Puntos de historia estimados**	1

Tabla 31 - Fuente: Elaboración Propia

ID	US-025	**Nombre**	Realización de controles
Descripción	Como usuario quiero realizar un control planificado para actualizar su información		
Criterios de Aceptación	1. Dado un usuario logueado y al menos un control cargado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado y ningún control existente, cuando se completan todos los campos, entonces el sistema muestra un mensaje confirmando que el control fue realizado y se crea un control realizado.		
Prioridad	Alta	**Puntos de historia estimados**	3

Tabla 32 - Fuente: Elaboración Propia

ID	US-026	**Nombre**	Carga de archivos en controles
Descripción	Como usuario quiero cargar un documento en la realización de un control para que quede registrado		
Criterios de Aceptación	1. Dado un usuario logueado y al menos un control cargado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado y ningún control existente, cuando se completan todos los campos, entonces el sistema muestra un mensaje confirmando que el control fue realizado.		
Prioridad	Media	**Puntos de historia estimados**	3

Tabla 33 - Fuente: Elaboración Propia

ID	US-027	**Nombre**	Asignación de controles a usuarios
Descripción	Como usuario como usuario, quiero actualizar el control para asignarme a mi o a otro usuario la realización de un control		
Criterios de Aceptación	1. Dado un usuario logueado y al menos un control cargado, cuando no son completados todos los campos necesarios, entonces el sistema muestra un error. 2. Dado un usuario logueado y ningún control existente, cuando se completan todos los campos, entonces el sistema muestra un mensaje confirmando que la asignación fue realizada.		
Prioridad	Media	**Puntos de historia estimados**	3

Tabla 34 - Fuente: Elaboración Propia

ID	US-028	**Nombre**	Vinculación Control - Riesgo
Descripción	Como usuario quiero actualizar un Riesgo cargado para vincularlo con un Control cargado		
Criterios de Aceptación	1. Dado un usuario logueado, un control y un riesgo cargado, cuando quiero asociar el riesgo y el control, los vinculo entre sí, entonces el sistema asocia el control con el riesgo.		
Prioridad	Media	**Puntos de historia estimados**	1

Tabla 35 - Fuente: Elaboración Propia

ID	US-029	**Nombre**	Calculo exposición riesgo
Descripción	Como sistema quiero modificar un riesgo para actualizar automáticamente la exposición que tiene un riesgo		
Criterios de Aceptación	1. Dado uno o más controles o uno o más documentos existentes, un riesgo cargado y estos asociados entre sí, cuando actualizo el riesgo, entonces se disminuye el valor de la exposición teniendo en cuenta los valores residuales y la sucesión de Fibonacci. 2. Dado uno o más incidentes existentes, un riesgo cargado y estos asociados entre sí, cuando actualizo el riesgo, entonces se aumenta el valor de la exposición teniendo en cuenta los valores residuales y la sucesión de Fibonacci.		
Prioridad	Alta	**Puntos de historia estimados**	3

Tabla 36 - Fuente: Elaboración Propia

ID	US-030	**Nombre**	Listado de normas
Descripción	Como usuario quiero ver el listado de todas las normas, certificaciones y estándares que posee la plataforma para consultarlas		
Criterios de Aceptación	1. Dado un usuario logueado y al menos una certificación, norma o estándar cargado, cuando consulto el listado, entonces el sistema muestra el nombre de cada una de ellas existente. 2. Dado un usuario logueado y ninguna una certificación, norma o estándar existente, cuando consulto el listado, el sistema muestra un mensaje indicando la inexistencia de las mismas cargadas.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 37 - Fuente: Elaboración Propia

ID	US-031	**Nombre**	Listado de controles de normas/estándar
Descripción	Como usuario quiero ver el listado de controles asociados a una norma, certificación o estándar que posee la plataforma para consultarlo		
Criterios de Aceptación	1. Dado un usuario logueado y al menos una certificación, norma o estándar cargado, cuando consulto el listado de controles, entonces el sistema muestra el nombre de cada una de ellas existente. 2. Dado un usuario logueado y ninguna una certificación, norma o estándar existente, cuando consulto el listado de controles, entonces el sistema muestra un mensaje indicando la inexistencia de las mismas cargadas.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 38 - Fuente: Elaboración Propia

ID	US-032	**Nombre**	Detalle de controles de normas/estándar
Descripción	Como usuario quiero ver el detalle de requerimientos de un control de una norma, estándar o certificación para consultarlo		
Criterios de Aceptación	1. Dado un usuario logueado, al menos una certificación, norma o estándar cargado y un control cargado de la norma, certificación o estándar cuando consulto el detalle del control, entonces el sistema muestra la información de este.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 39 - Fuente: Elaboración Propia

ID	US-033	**Nombre**	Vinculación control normas – control
Descripción	Como usuario quiero vincular un control cargado con un control de la norma cargado para asociarlos		
Criterios de Aceptación	1. Dado un usuario logueado, un control y un control de la norma cargado, cuando quiero actualizar el control, entonces el sistema los asocia entre sí.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 40 - Fuente: Elaboración Propia

ID	US-034	**Nombre**	Vinculación control normas – Documentación
Descripción	Como usuario quiero vincular una documentación cargada con un control de la norma cargado para asociarlos		
Criterios de Aceptación	1. Dado un usuario logueado, una documentación y un control de la norma cargado, cuando actualizo el control entonces el sistema los asocia entre sí.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 41 - Fuente: Elaboración Propia

ID	US-035	**Nombre**	Vinculación control normas – activo
Descripción	Como usuario quiero vincular un activo de información cargado con un control de la norma cargado para asociarlos		
Criterios de Aceptación	1. Dado un usuario logueado, un activo de información y un control de la norma cargado, cuando actualizo el control entonces el sistema los asocia entre sí.		
Prioridad	Baja	**Puntos de historia estimados**	1

Tabla 42 - Fuente: Elaboración Propia

ID	US-036	**Nombre**	Detalle de cumplimiento de norma/estándar
Descripción	Como sistema quiero calcular el estado de cumplimiento de las distintas normas, para actualizar dicho valor		
Criterios de Aceptación	1. Dado un usuario logueado y al menos una norma, certificación o estándar, cuando actualizo el valor de acuerdo a los controles y documentos asociados, entonces el sistema actualiza el estado de cumplimiento de la misma		
Prioridad	Baja	**Puntos de historia estimados**	1

Sprint Backlog

El primer sprint se definió teniendo en cuenta una duración de dos semanas y considerando el listado de historias de usuario mencionado en la sección anterior.

Tabla 43 - Fuente: Elaboración Propia

SPRINT 1							
ID	Historia de Usuario	Tarea	Estimado	Estado	Prioridad	Puntos de Historia	Dependencias
US-001	ABM Usuarios	Codificar Módulo	3 días	Pendiente	Alta	5	
		Diseñar interfaz gráfica	0,5 día	Pendiente			
		Implementación e integración	0,5 día	Pendiente			
		Pruebas del módulo	1 día	Pendiente			
US-002	Ingreso de usuario	Codificar Módulo	1 día	Pendiente	Alta	1	US-001
		Diseñar interfaz gráfica	0,5 día	Pendiente			
		Implementación e integración	0,5 día	Pendiente			
		Pruebas del módulo	1 día	Pendiente			
US-008	Creación de nuevo riesgo	Codificar Módulo	2 días	Pendiente	Alta	3	
		Diseñar interfaz gráfica	0,5 día	Pendiente			
		Implementación e integración	0,5 día	Pendiente			
		Pruebas del módulo	1 día	Pendiente			
US-012	Creación de nuevo incidente	Codificar Módulo	2 días	Pendiente	Alta	3	
		Diseñar interfaz gráfica	0,5 día	Pendiente			
		Implementación e integración	0,5 día	Pendiente			
		Pruebas del módulo	1 día	Pendiente			

Estructura de datos

Para presentar la estructura de la aplicación, se presenta un diagrama de clases y de un diagrama de base de datos para mostrar las relaciones en la misma.

Diagrama de Base de Datos

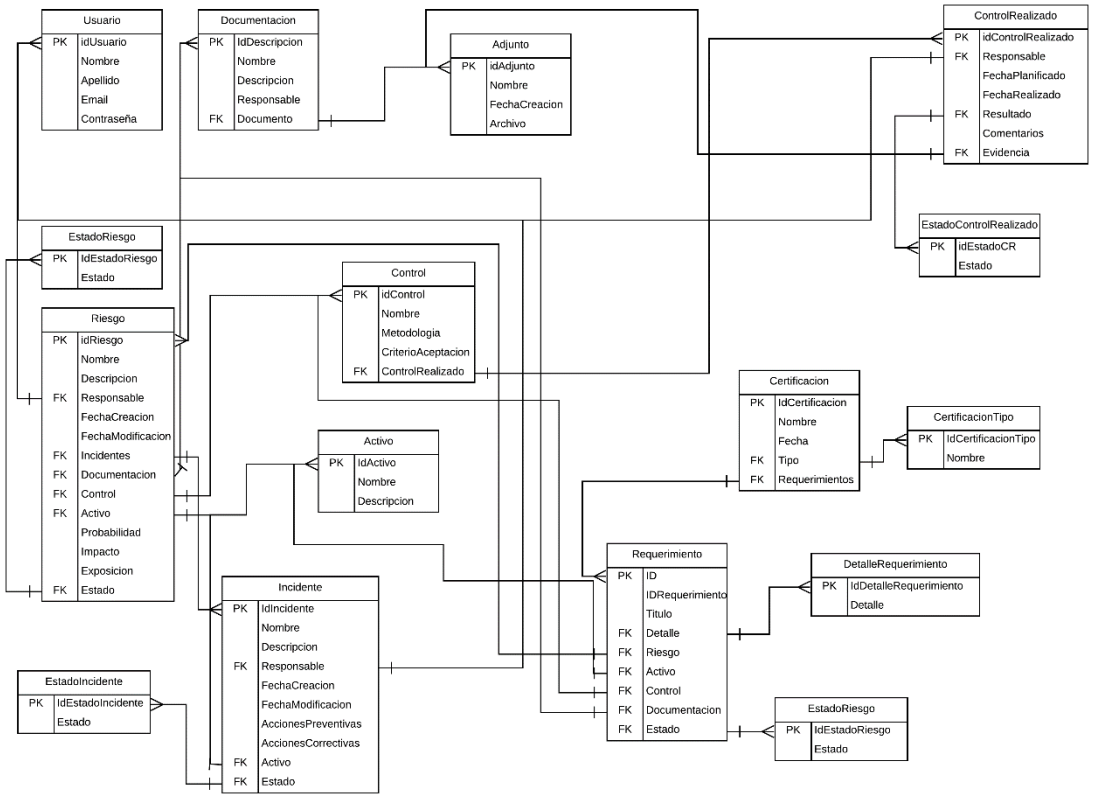


Diagrama 5 - Fuente: Elaboración Propia

Diagrama de Clases

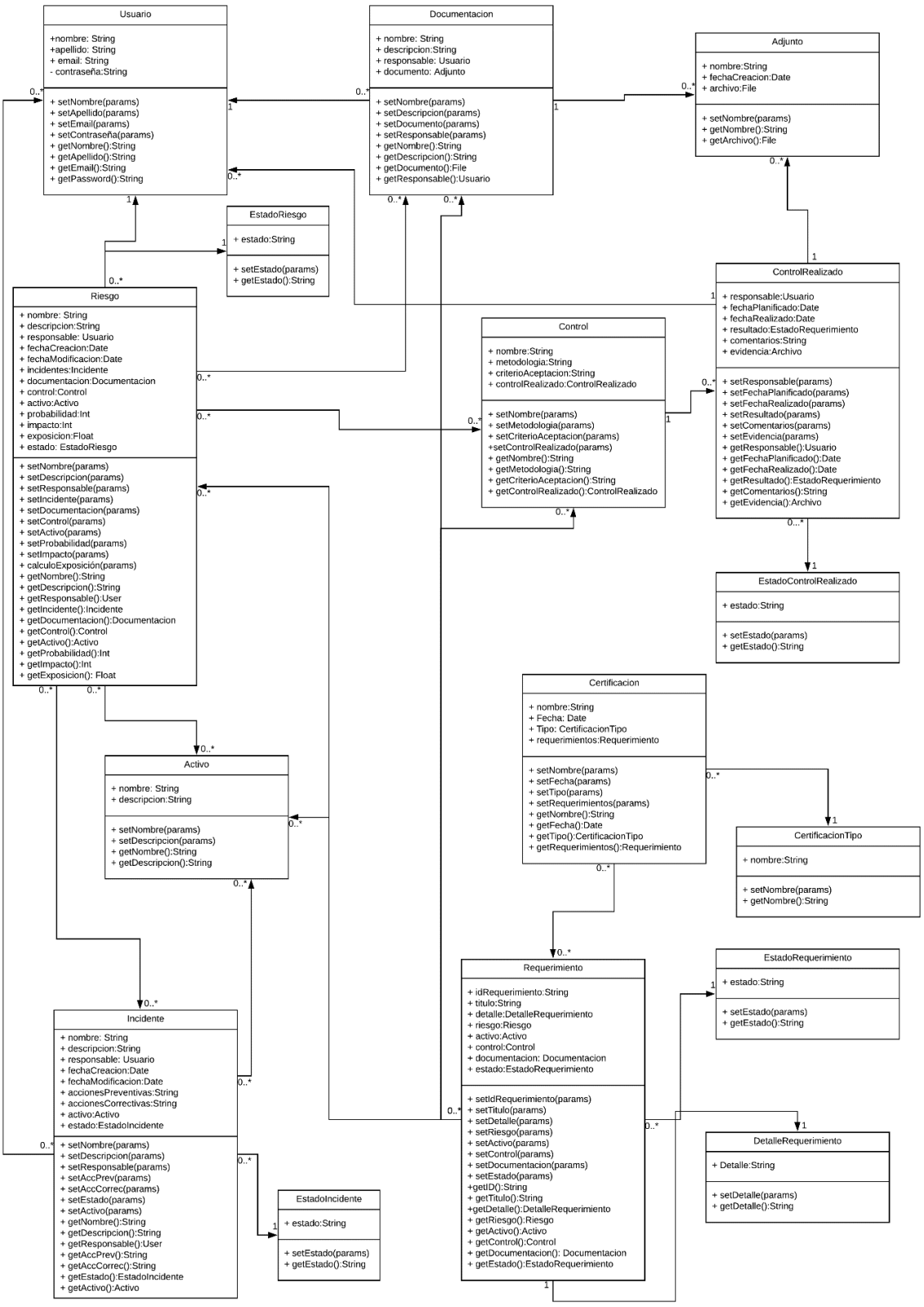


Diagrama 6 - Fuente: Elaboración Propia

Prototipos de interfaces de pantallas

Se presentan los prototipos de las interfaces de pantalla de los procedimientos que pueden realizarse en la aplicación.

En la ilustración 1 podemos ver el menú principal:

Ilustración 1 - Fuente: Desarrollo Propio

Luego se presentan las pantallas de creación de los distintos elementos.

Ilustración 2 - Fuente: Desarrollo Personal

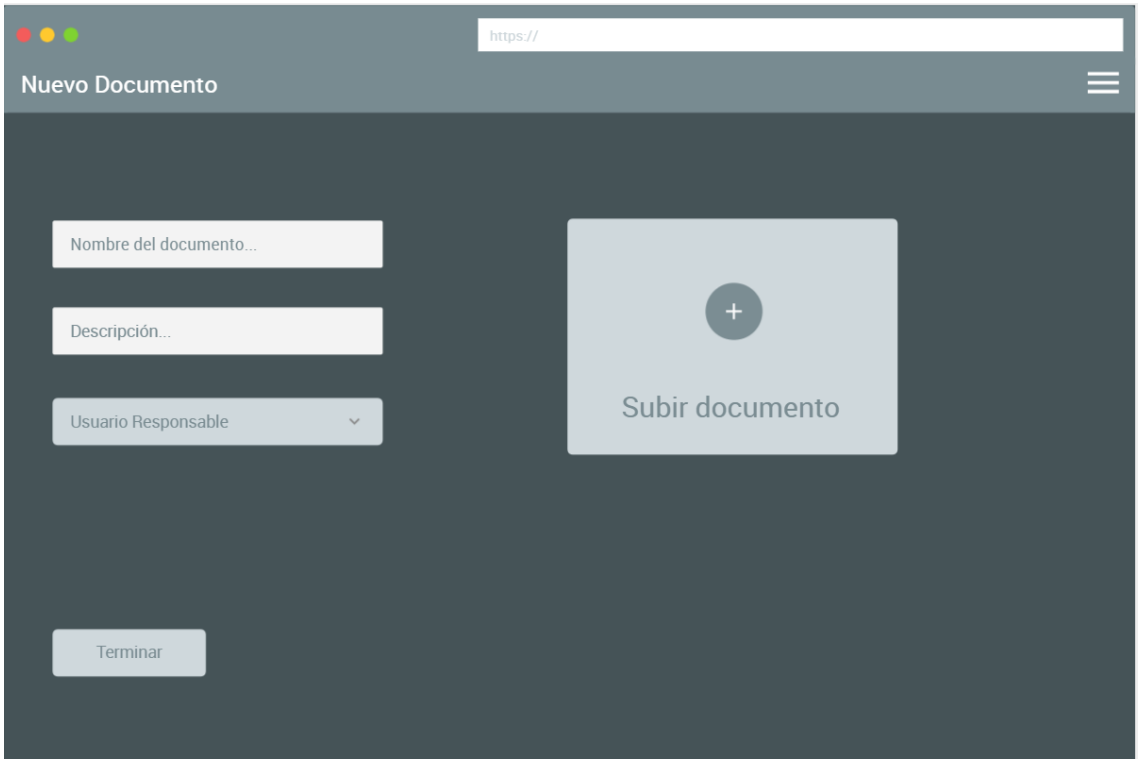


Ilustración 3 - Fuente: Desarrollo Personal

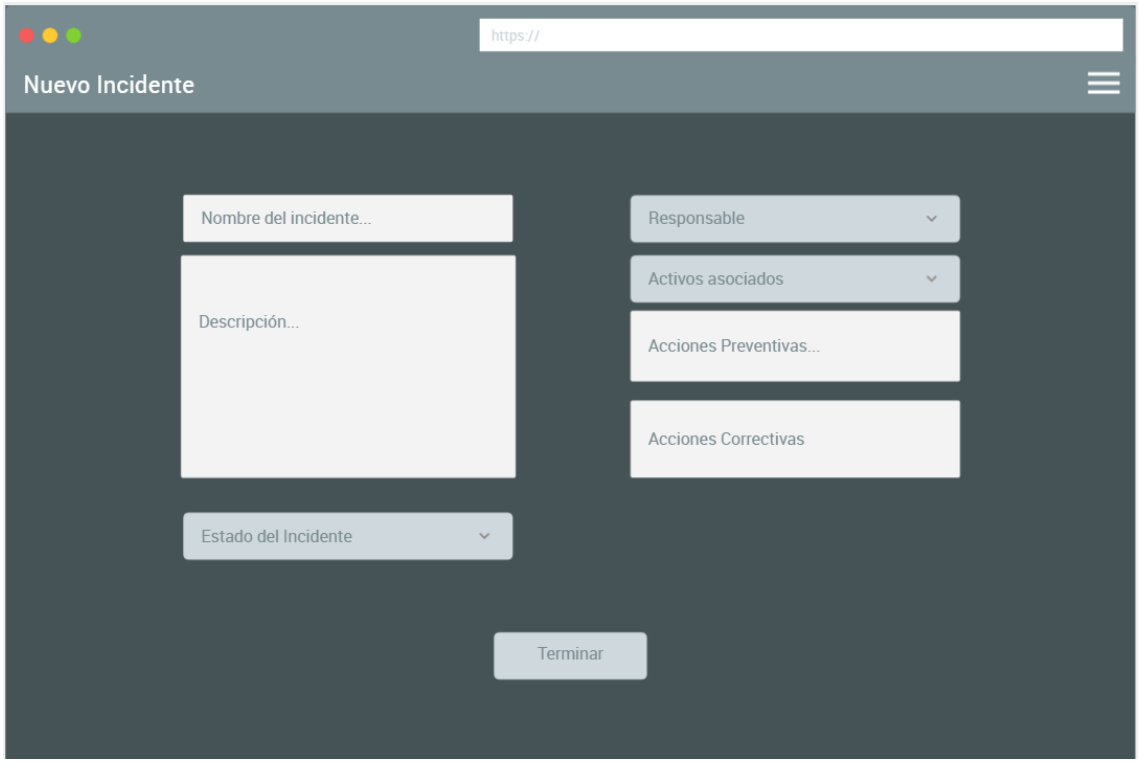


Ilustración 4 - Fuente: Desarrollo Personal

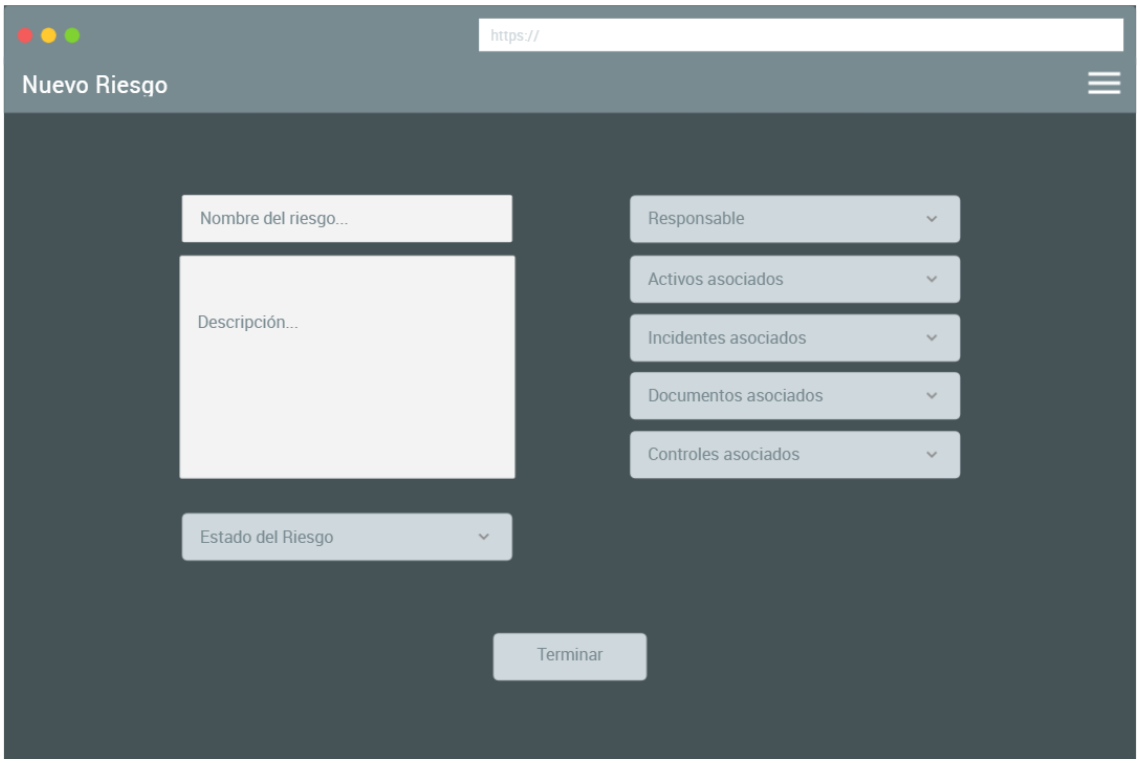


Ilustración 5 - Fuente: Desarrollo Personal

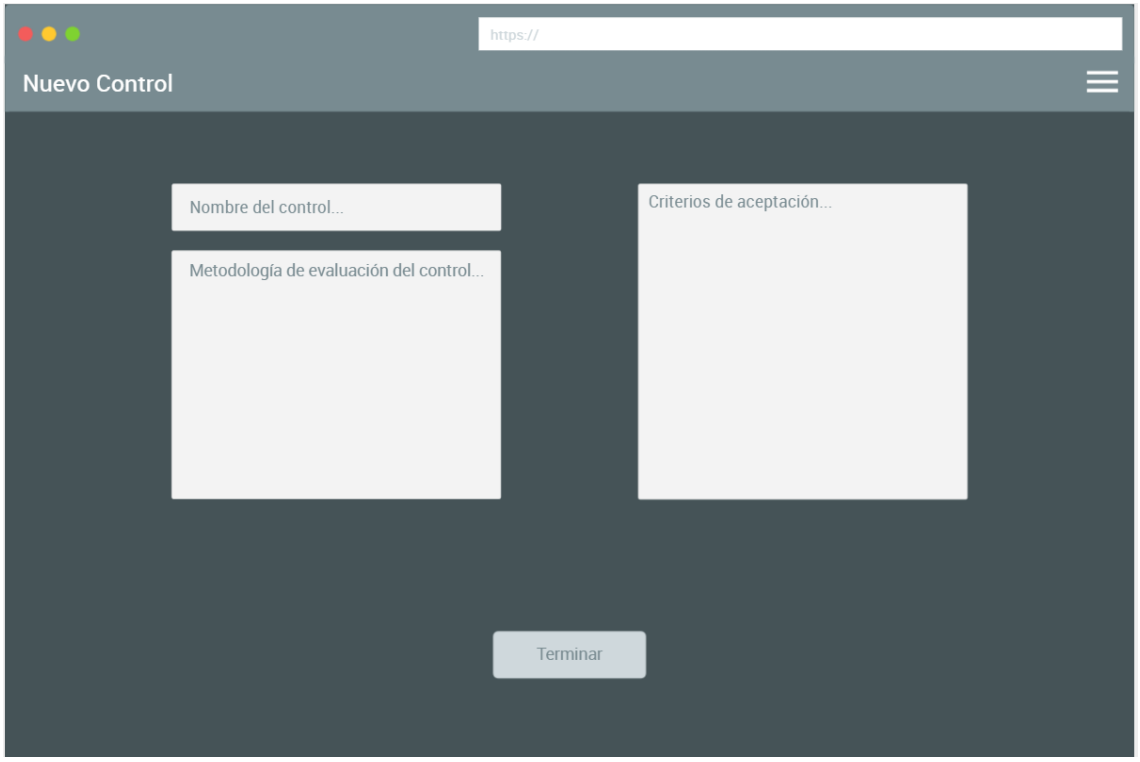


Ilustración 6 - Fuente: Desarrollo Personal

Las siguientes ilustraciones muestran la interfaz sobre los controles cargados en la plataforma, incluyendo el listado con sus planificaciones y la realización de uno.

Ilustración 7- Fuente: Desarrollo Personal

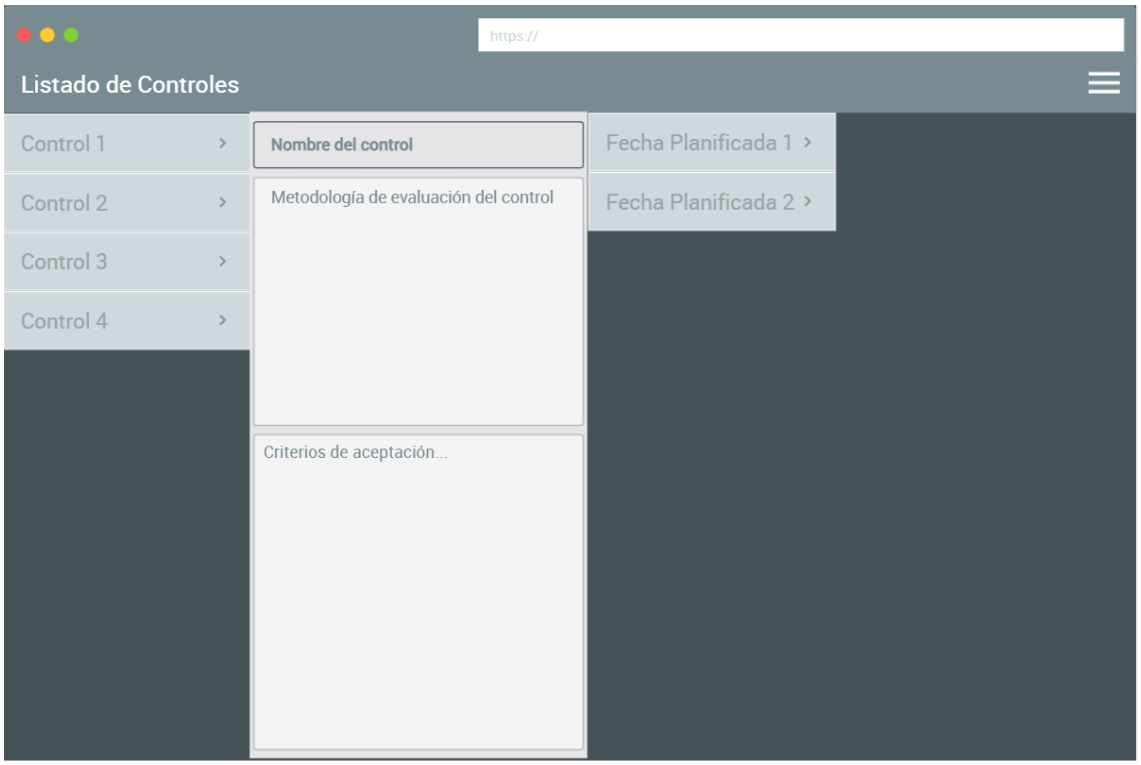
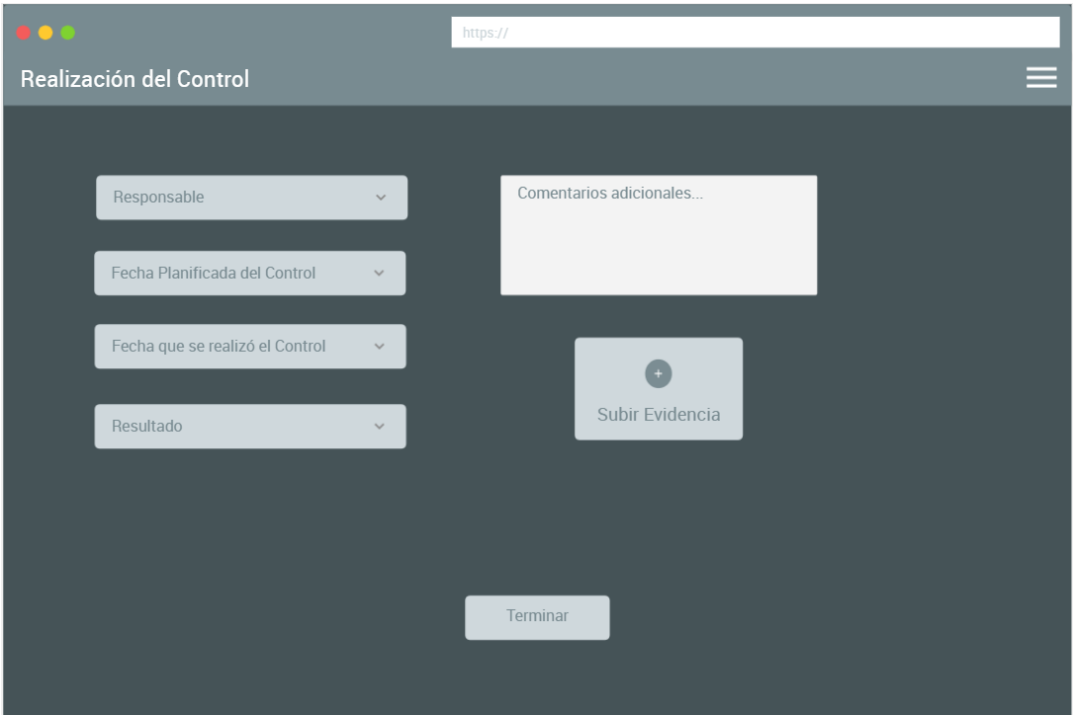


Ilustración 8- Fuente: Desarrollo Personal



Finalmente, se muestra el listado de normas, con sus respectivos requerimientos y los distintos elementos relacionados a dicho requerimiento.

Ilustración 9- Fuente: Desarrollo Personal

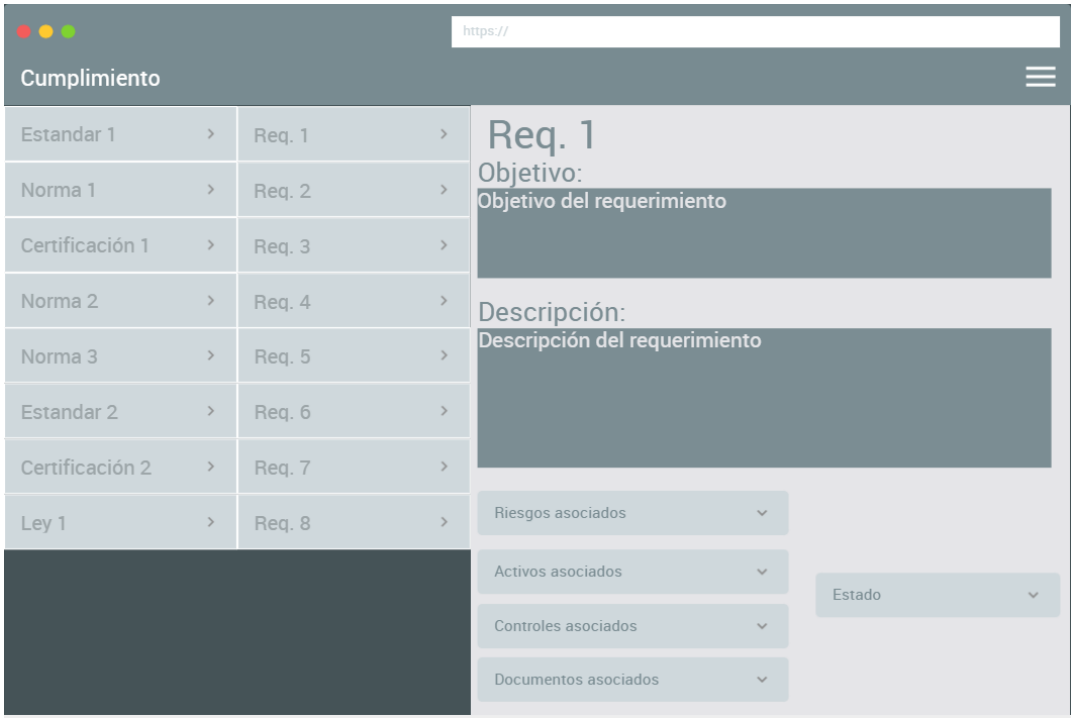
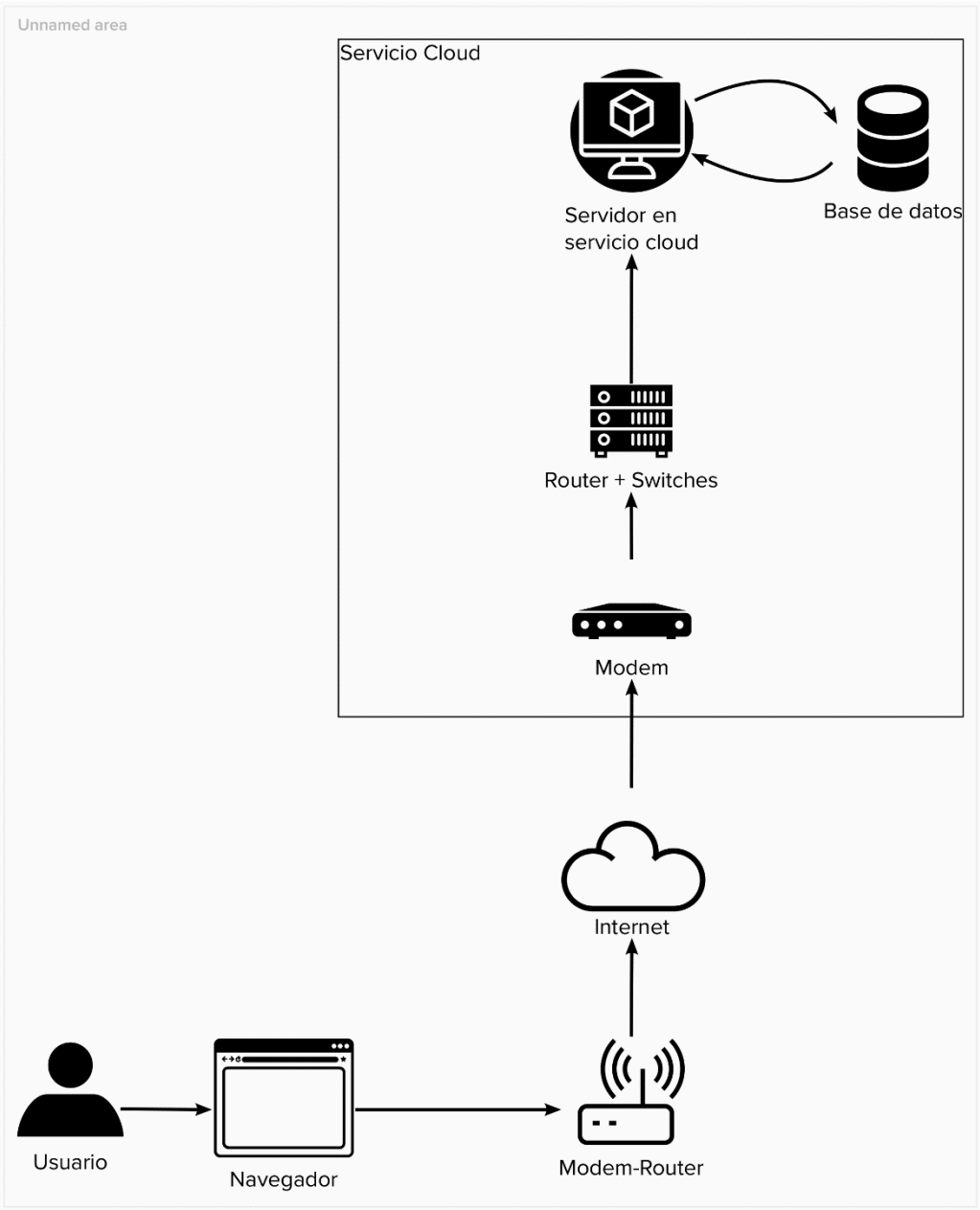


Diagrama de arquitectura

En la siguiente ilustración (11), se visualiza la arquitectura de la herramienta. Iniciando desde el usuario, utilizando su navegador de internet, se conecta a la aplicación que está alojada en un servidor en un servicio en la nube, la cual se relaciona con la base de datos para obtener la información almacenada en ella.

Ilustración 10- Fuente: Elaboración Personal



Seguridad

Dada la importancia de mantener la confidencialidad y la disponibilidad de la información que se contenga en la aplicación, se plantea dos tipos de políticas que serán usadas en ella para preservar estos dos pilares de la seguridad. Primero, se plantea la política de acceso a la aplicación, la cual garantiza el ingreso a la misma de forma segura y hace hincapié en los roles de usuarios y la seguridad de la contraseña. Por otro lado, las políticas de respaldo de la información, que nos permite tener copias de seguridad de la aplicación y su base de datos, en caso de que exista algún incidente que lleve a la pérdida de alguna de las dos.

Políticas de acceso a la aplicación

1. Se utiliza un usuario único junto con la contraseña, para el inicio de sesión.
2. La contraseña debe cumplir los siguientes requisitos:
    a. Mínimo de 8 caracteres.
    b. No debe ser similar al usuario, nombre, apellido o e-mail del usuario.
    c. Se compara la contraseña contra un listado de más de 20.000 contraseñas más comunes y no debe pertenecer a ese listado
    d. No debe contener todos caracteres numéricos.
3. La contraseña se encripta utilizando el algoritmo PBKDF2, con un hash SHA-256.
4. La aplicación permite la gestión de roles y permisos de los usuarios de manera que podamos crear roles y asignarle permisos específicos a cada rol.

Políticas de respaldo de la información

Para el realizar el respaldo la información en la base de datos, se utiliza un servicio en la nube, donde se hará una copia de seguridad diario y éste luego será respaldado a su vez utilizando redundancia geográfica. El sistema retiene hasta un máximo de 30 días, realizando copias incrementales.

Para el caso del respaldo del código, se utiliza uno local y una copia que será almacenada en Github, un servicio de versionado en la nube, con el fin de poder recuperarlo en caso de no tener acceso a la instancia local.

Análisis de Costos

A continuación, se presentan los costos principales para el desarrollo del proyecto, teniendo en cuenta: Hardware, Software y capital humano.

Tabla 44 Costos de Hardware - Fuente: elaboración Propia

Hardware	Descripción	Precio Unitario	Cantidad	Precio Final	Referencia de precio
Notebook	Procesador: Intel Core i5 SO: Windows 10 Pro 64 bits Memoria: 16.0GB DDR4 Almacenamiento: 256GB SSD	$162.999,00	4	$651.996	Ref. 1
Disco Duro Externo	SEAGATE BASIC USB 3.0 2TB	$8.390	1	$8.390	Ref. 2
Azure	Azure App Service	$6,265 (Por hora)	480	$3.007,2	Ref. 3
Azure	Azure Database for MySQL	$3,409 (Por hora)	480	$1.636,32	Ref. 4
			Total:		$665.029,62

Obtenidos el 16/6/2021:
REF. 1: https://www.lenovo.com/ar/es/laptops/thinkpad/serie-e/E15-G2/p/20TES0X200
REF. 2: https://www.venex.com.ar/almacenamiento/discos-externos/disco-duro-externo-2tb-seagate-basic-usb-30.html
REF. 3: https://azure.microsoft.com/es-es/pricing/details/app-service/windows/#overview
REF 4: https://azure.microsoft.com/es-es/pricing/details/mysql/server/

Es importante tener en cuenta que las herramientas de desarrollo utilizadas son de software libre o gratuitas, por lo que no existe costo alguno por la utilización de ellas.

Tabla 45 Costos de Software - Fuente: elaboración Propia

Software	Licencia	Precio Unitario	Cantidad	Precio Final
Windows 10	Paga	$0 (Incluido con el costo de la notebook)	4	$0
Python	Libre	$0	4	$0
Django	Libre	$0	4	$0
MySQL	Libre	$0	1	$0
			Total:	$0

Los costos del capital humano fueron obtenidos del sitio del Consejo Profesional de Ciencias de las Informáticas de Buenos Aires (Honorarios, 2021):

Tabla 46 Costos Capital Humano - Fuente: elaboración Propia. Obtenido 16 de junio del 2021

Recurso Humano	Cantidad	Salario por mes	Cantidad de meses	Precio final
Líder de proyectos	1	$168.453	3	$505.359
Desarrollador Python	1	$149.404,50	3	$448.214
Programador de páginas Web	1	$109.012,50	3	$327.038
Tester	1	$124.618,50	3	$373.856
			Total:	$1.654.467

Finalmente, se presenta una tabla con la sumatoria de los costos de cada categoría, mostrando el costo total del proyecto.

Tabla 47 Costo Total - Fuente: elaboración Propia

Concepto	Costo
Hardware	$665.029,52
Software	$0
Capital Humano	$1.654.466
Total:	$2.319.495,02

Análisis de Riesgos

Se realizo un análisis de los posibles riesgos que pueden presentarse al momento de desarrollar este proyecto, en el cual se identifica la causa de estos, la probabilidad de ocurrencia durante el período de desarrollo, que es evaluada del 1 al 3, siendo bajo: 1, medio: 2 y alto: 3; y el impacto que puede tener, el cual es evaluado del 1 al 5, considerando impactos muy bajo, bajo, medio, alto y muy alto, respectivamente. Con estos valores, se establece un valor final que está determinado por la multiplicación de el impacto y la probabilidad, el cual nos da el valor de exposición. Este valor nos permite determinar en qué casos se deben tomar acciones para mitigar ya sea el impacto o la probabilidad de ocurrencia.

Teniendo en cuenta que el proyecto está planificado para tres meses, la información se presenta en la siguiente tabla.

Tabla 48- Riesgos - Fuente: Elaboración Propia

Riesgo	Causa	Probabilidad	Impacto	Exposición
Fallas en la planificación	Debido a errores u omisiones a la hora de planificar el proyecto, se realiza una planificación que no coincide con la real	2	4	8
Falta de conocimiento técnico en el equipo de trabajo	Personal del equipo puede no tener el conocimiento suficiente para desarrollar alguna historia de usuario	1	3	3
Rotación de personal	El personal deja el equipo de trabajo por una mejor oferta laboral	1	4	4
Cambios en el costo del proyecto	Debido a la inestabilidad económica, el costo del proyecto puede aumentar	2	3	6
Error en el diseño del producto	Debido a un mal análisis, se produce un error en el diseño del producto	2	4	8
Cambios de requerimientos	Pueden surgir cambios o requerimientos adicionales que no estaban planificados	3	5	15
Demoras por fallas en la implementación	Existen fallas a la hora de implementar la herramienta en la nube que pueden no haber estado planificadas	1	4	4

Teniendo en cuenta las variables analizadas, se establece una matriz de evaluación de riesgos la cual permite tomar los valores de exposición y determinar un plan de contingencia adecuado para cada tipo de riesgo. Dicha matriz permite caracterizar los riesgos en 3 categorías de acuerdo con el valor de su exposición: Bajo (menor o igual a 3), Medio (valores entre 4 y 6) y Alto (Exposición mayor a 6).

Tabla 49- Matriz de evaluación de riesgos - Fuente: elaboración Propia

Probabilidad \ **Impacto**	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15

De acuerdo con lo dicho anteriormente, se determina qué tipo de acciones deben ser tomadas para mitigar el impacto o la probabilidad de ocurrencia en el proyecto.

- Alto: Deben tomarse acciones inmediatas.
- Medio: Deben tomarse acciones a corto o mediano plazo.
- Bajo: Pueden no tomarse acciones, pero deben ser monitoreadas constantemente.

Se determinan las siguientes acciones de mitigación tomadas para los riesgos medios y altos:

Tabla 50 - Acciones de mitigación - Fuente: Elaboración Propia

Riesgo	Exposición	Mitigación
Cambios de requerimientos	15	Dado que se utiliza la metodología SCRUM, en las instancias que se tiene con el cliente, determinar la criticidad de los cambios y reevaluar la planificación
Fallas en la planificación	8	Evaluar la planificación en base a la productividad que posee el equipo. Evaluar la posibilidad de modificar los tiempos de cada sprint, en caso de ser necesario
Error en el diseño del producto	8	Establecer instancias de aseguramiento de conformidad del cliente y de validación de requerimientos
Cambios en el costo del proyecto	6	Solicitar al cliente la posibilidad de un pago por adelantado de aquellos costos que puedan variar más rápidamente, como las laptops
Demoras por fallas en la implementación	4	Evaluar la posibilidad de contratar una persona adicional que haga la configuración inicial
Rotación de personal	4	Dada la corta duración del proyecto, al momento de la contratación, validar el compromiso de los miembros del equipo para finalizar el proyecto

Conclusiones

El proyecto llevado a cabo es una herramienta que permite a las organizaciones poder establecer, implementar y mantener un sistema de gestión de la seguridad de la información. Gracias a mis años de experiencia laboral en seguridad, pude comprender la importancia que tiene la información y que la misma esté segura, lo que llevó a que decidiera elegir esta temática para el proyecto. Lo anterior mencionado, sumado al hecho de que aquellas empresas que no siempre tienen los recursos para contratar costosos servicios de consultoría o aplicaciones similares, les suele tomar mucho tiempo la implementación de sistemas similares no pudiendo ver los resultados en un plazo cercano y muchas veces abandonando los proyectos. La aplicación logra los objetivos planteados ya que permite que las organizaciones puedan establecer un SGSI de forma concisa y completa. Permitiendo a su vez nuclear todo en una sola herramienta. Además, permite que se conozca claramente el estado de la organización con respecto a estándares, normativas y certificaciones, pudiendo visualizar claramente la brecha existente entre la situación actual de la organización y lo requerido. Esto último, hace que las organizaciones puedan planificar de forma concreta y precisa qué acciones deben tomar para que dicha brecha no exista.

Gracias al desarrollo del proyecto tuve la posibilidad de vincular mis años de experiencia en el rubro con los conocimientos adquiridos durante toda la carrera. Encontré en el mismo un desafío a la hora de desarrollar el producto, ya que no es una actividad que realice a diario. El proceso de desarrollar la aplicación requirió mucho tiempo de investigación, sobre todo la implementación de la tecnología blockchain, que desde un principio sentí que estaba muy por encima de mis conocimientos.

Encuentro muy placentero y satisfactorio el poder haber logrado el proyecto. Lograr vincular dos cosas que me apasionan como son la seguridad de la información y el cumplimiento con la programación y la informática, teniendo que esforzarme para superar mis propios límites con el fin de cumplir los objetivos, obteniendo muchos conocimientos nuevos en el camino que son útiles para mi vida personal y profesional.

Demo

El enlace presentado a continuación, hace referencia a una carpeta en la nube en Google Drive, la cual contiene todo lo necesario para desplegar la aplicación de forma local.

https://drive.google.com/drive/folders/1dzxdP6f9QMFvbGBC2r3JNxy7l5O3umO6?usp=sharing

Referencias

Blockhead, T. (2016). *Guía Definitiva de Prácticas Ágiles esenciales de Scrum.* Babelcube Inc.

Eramba. (s.f.). *Eramba Frequently Asked Questions*. Obtenido de Eramba Frequently Asked Questions: https://www.eramba.org/faq

Fitzgerald, T. (2018). *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers.* CRC Press.

Forcier, J., Bissex, P., & Chun, W. (2008). *Python Web Development with Django.* Addison-Wesley Professional.

Honorarios. (16 de Junio de 2021). Obtenido de Consejo Profesional de Ciencias de la Informatica de Buenos Aires: http://www.cpciba.org.ar/honorarios

International Organization for Standardization. (2018). ISO. *Information technology — Security techniques — Information security techniques — Information security and vocabulary*.

KnowBe4. (s.f.). *KCM GRC Platform Product Features*. Obtenido de KCM GRC Platform Product Features: https://kcmgrc.knowbe4.com/kcm-grc-platform-product-features

Laurence, T. (2017). *Blockchain for dummies.* John Wiley & Sons, Inc.

May, M. M., & Elliot, D. (10 de 4 de 2021). *Consortium for Research on Information Security and Policy*. Obtenido de Consortium for Research on Information Security and Policy: https://fsi.stanford.edu/research/consortium_for_research_on_information_security_and_policy

Nemati, H. R. (2008). *Information Security and Ethics: Concepts, Methodologies, Tools and Applications.* Universidad de Indiana.

Python Software Foundation. (s.f.). *What is Python? Executive Summary*. Obtenido de What is Python? Executive Summary.: https://www.python.org/doc/essays/blurb

Anexos

Anexo 1 – Planilla de Riesgos

Nombre del Riesgo	Activo Afectado	Responsable	Probabilidad	Impacto	Exposición (Impacto x Probabilidad)	Mitigación	Exposición Final	Acción sobre el riesgo

Tabla 51 - Fuente: Elaboración Propia

Anexo 2 – Planilla de Incidentes

Nombre del Incidente	Tipo de Incidente	Responsable	Fecha de ocurrencia	Descripción del incidente	Impacto	Acciones Preventivas	Acciones Correctivas

Tabla 52 - Fuente: Elaboración Propia

Anexo 3 – Planilla de Listado de Controles

Nombre del Control	Activo a Revisar	Responsable	Fecha Programada	Fecha Realizada	Evidencia Registrada	Ubicación de la evidencia	Resultado

Tabla 53 - Fuente: Elaboración Propia

Anexo 4 – Declaración de Aplicabilidad

ID Control	Control	Descripción del Control	Responsable	¿Cumple?	Activo asociado	Controles asociados	Políticas asociadas	Procesos asociados

Tabla 54 - Fuente: Elaboración Propia