UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS

DESARROLLO DE SOFTWARE DE ANÁLISIS DE RIESGOS Y GESTIÓN DE SEGURIDAD BASADO EN ISO 27001, CAÑAR - ECUADOR.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

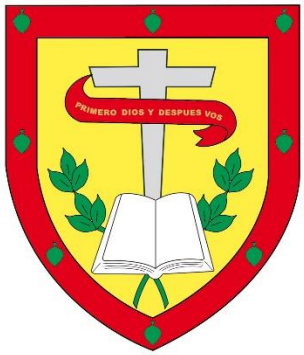
AUTOR: JUAN FERNANDO MUÑOZ MUÑOZ

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS, MSC.

CAÑAR - ECUADOR

2021

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)

CARRERA DE INGENIERÍA DE SISTEMAS

DESARROLLO DE SOFTWARE DE ANÁLISIS DE RIESGOS Y GESTIÓN DE SEGURIDAD BASADO EN ISO 27001, CAÑAR - ECUADOR

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

AUTOR: JUAN FERNANDO MUÑOZ MUÑOZ

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS, MSC.

CAÑAR - ECUADOR

2021

DIOS, PATRIA, CULTURA Y DESARROLLO

DEDICATORIA

A Dios nuestro señor por bendecirme en cada instante de mi vida y con su guía alcanzar una más de mis metas.

A mi madre Muñoz Buñay Juana María quien fue la que me ayudo a lograr esta meta por su esfuerzo dedicación y apoyo en toda mi vida.

A mi hija Muñoz Morocho Grace Nahomi quien ha sido siempre mi mayor inspiración y el pilar fundamental para lograr esta meta.

AGRADECIMIENTO

A Dios por permitir que todas las cosas sean posibles y por las bendiciones recibidas.

A la Universidad Católica de Cuenca Extensión Cañar y en especial a la Facultad de Ingeniería de Sistemas por acogerme y permitir cumplir mis metas.

A todos los catedráticos de la carrera de ingeniería de Sistemas que me guiaron para llegar a la meta deseada que es de ser un profesional y a mis padres que me brindaron todo el apoyo necesario en mi vida de estudiante.

DECLARACION

Yo, Fernando Muñoz Muñoz, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Católica de Cuenca extensión Cañar puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y la Normativa actual de la institución.

Juan Fernando Muñoz Muñoz

C.I: 0302712310

RESPONSABILIDAD

"La responsabilidad del contenido de esta tesis de grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Universidad Católica de Cuenca extensión Cañar".

Juan Fernando Muñoz Muñoz

C.I: 0302712310

CETIFICADO DE APROBACION DE TRABAJO DE TITULACION

Yo Cristhian Humberto Flores Urgilés portador(a) de la cédula de ciudadanía Nº 030163837-5. En calidad de tutor certifico que el estudiante, Sr. Juan Fernando Muñoz Muñoz, ha concluido su trabajo de titulación que lleva por nombre "DESARROLLO DE SOFTWARE DE ANÁLISIS DE RIESGOS Y GESTIÓN DE SEGURIDAD BASADO EN ISO 27001.".

El trabajo realizado a obtenido la nota de cuarenta y nueve puntos sobre cincuenta (49/50)

Aprovecho la ocasión para reiterarle éxitos en el desempeño de sus funciones.

Cañar, 15 de octubre de 2021

F: ……..

Cristhian Humberto Flores Urgilés

C.I. 0301638375

APROBACION DE TRIBUNAL DE GRADO

El tribunal designado por el honorable consejo directivo de la Universidad Católica de Cuenca Extensión Cañar, Facultad de Ingeniería de Sistemas instalado para receptar la sustentación del trabajo final de investigación con el tema: "DESARROLLO DE SOFTWARE DE ANÁLISIS DE RIESGOS Y GESTIÓN DE SEGURIDAD BASADO EN ISO 27001", transcurrido el tiempo reglamentario procede a consignar la calificación de (_____/100).

Cañar, _____de_____ del 2021

PRESIDENTE	**DIRECTOR**
DELEGAGO	**SECRETARIO**

Contenido

ÍNDICE DE TABLAS

INDICE DE ILUSTRACIONES

Resumen

El presente proyecto consiste en el desarrollo de software para el análisis de riesgo de la seguridad de la información, que permita definir los controles necesarios para cumplir todos los requerimientos de protección de los activos de una organización para el desarrollo de este trabajo investigativo se ha definido una metodología de desarrollo de software acorde a la necesidad del proyecto una vez definida la metodología se ha diseñado y desarrollado el software que permite aplicar la metodología MAGERIT para análisis de riesgo de una forma eficaz y eficiente, mostrando los controles de la norma ISO/IEC 27001, el sistema permite realizar un análisis de riesgo informático mediante una valoración de los activos, impacto, probabilidad, identificando el índice de amenazas y el nivel de riesgo en el que se encuentran los activos finalmente se realizó pruebas del software en el que se ingresó activos y se le otorgó la calificación respectiva, se identificaron amenazas correspondientes a dicho activo, se calificó el impacto y la probabilidad, obteniendo así el nivel de riesgo, si el nivel es alto se presenta los controles necesarios para cada amenaza con el fin de mitigar el riesgo.

Palabras claves: magerit, gestión de riesgos, controles, iso/iec 27001.

Abstract

The present paper involves the development of software for the security risk analyses, which allows defining the necessary controls to compile with all protective requirements of an organization`s essets. In order to develop this research project, a software-development methodology was defined, in accordance with the project`s necessities. Once the methodology was defined. A software that allows the use of the MAGERIT methodology was designed and developed, to effectively and efficiently analyze the risks, showing the norm ISO/IEC27001 controls, such system allows to conduct an informatics-risk analysis thru the essessment of assets, impact, probability, identifying the threat index and the risk level of the assets. Finally, the software was tested by entering the essets, and providing it with the respective mark, some threats to such assets were identified,the impact and probability were marked to obtain the risk level, if the level is high, the necessary controls are presented for each threat to mitigate the risk.

Keywords: MAGERIT, risk management, controls, ISO/IEC27001

Introducción

Hoy en día el capital más significativo para las organizaciones es su información, siendo bienes importantes para el buen funcionamiento de las entidades, por lo que requieren ser protegidos ante cualquier evento que pongan en peligro la disponibilidad, la integridad, la confidencialidad de la información. Los riesgos de los sistemas informáticos al ser materializados pueden provocar grandes pérdidas a las empresas si estas no son controladas tiempo. En la actualidad existen metodologías de gestión de riesgos tecnológicos para proteger la información de una forma adecuada, ayudando a conocer las fortalezas y debilidades.

Muchas empresas hoy en día sufren de robos y daños a los activos, debido a que no conocen las amenazas a las que están expuestos y que tan peligrosas pueden ser estas, por esta razón la presente investigación tiene como finalidad desarrollar un software de gestión de riesgo y seguridad de la información, mediante la metodología MAGERIT y el sistema de gestión de seguridad de la información (SGSI) ISO/IEC 27001 para la identificación de los controles a ser aplicados para mitigar las amenazas de los sistemas de información y la infraestructura tecnológica de cualquier organización.

A continuación, se hará una breve descripción de los capítulos

El primer capítulo contiene el marco referencial donde se plantea y formula el problema, con una breve investigación que tiene que ver con los antecedentes, la justificación de la investigación, objetivo general y específico, limitaciones y delimitaciones.

En el segundo capítulo de esta investigación se definen conceptos teóricos de los temas establecidos como: Metodologías de análisis y gestión de riesgo, SGSI, lenguajes de desarrollo, Gestores de Base de Datos, etc.

En el tercer capítulo se presenta el diseño metodológico, en el cual se indica las herramientas a ser utilizados para el desarrollo del software de gestión de riesgos, así como la metodología para su desarrollo.

En el cuarto capítulo se realiza la descripción de la propuesta de este trabajo, donde se describe todas las funciones que cumple el software desarrollado.

CAPITULO I

Marco Referencial

1.1. Planteamiento del Problema

La información es uno de los recursos importantes en las organizaciones, pues de ella depende no solo la base del negocio, sino el logro de los objetivos a mediano o largo plazo, debido a que la información permite la toma de decisiones. Esta es una de las razones por las cuales, actualmente todas las empresas deberían realizar una apropiada gestión de riesgos, permitiéndoles de esa forma conocer las vulnerabilidades que poseen, las amenazas a las que se encuentran expuestas.

En la actualidad existen herramientas que permiten la automatización de los riesgos, pero debido a su costo las empresas obvian su utilización, por ello la presente investigación determina el desarrollo de una solución de software de gestión de riesgos eficaz, gratuita y libre de uso que permita automatizar el proceso de gestión de riesgo, un análisis de las amenazas y el cálculo de las mimas, determinando el nivel de riesgo a la que puedan estar expuestas las organizaciones y de la mimas manera que permita realizar un tratamiento adecuado y la selección de los controles apropiados para evitar dichos riesgos.

1.2. Formulación del Problema

¿Cuáles serán las mejores herramientas de software especializadas para el desarrollo del proyecto y diseño de base de dato?

¿Qué metodología será utilizada para el desarrollo de Software de análisis y gestión de riesgo?

¿De qué manera ayudara la herramienta Software a las organizaciones??

1.3. Antecedentes de la investigación

Existen distintos autores que han desarrollado investigaciones sobre el tema, cuyos resultados han generado una guía de las mejores prácticas a tomarse a consideración. A continuación, se describe algunas de ellas:

Un proyecto similar desarrollado en la Universidad Laica Eloy Alfaro de Manabí facultad de ciencias Informáticas, proyecto previo a la obtención del título de ingeniero en sistema, realizado por Acosta, N. (2018) que lleva por título "SOFTWARE DE ANALISIS DE RIESGO INFORMATICO APLICANDO MAGERIT Y NORMA ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMATICAS" esta investigación tiene como finalidad la realización de un análisis de riesgo con la metodología MAGERIT, y el desarrollo de un software que permita aplicar las metodologías de forma eficiente.

En base a este documento se podrá identificar las vulnerabilidades, los riesgos que pueden afectar a los sistemas, determinar los procesos críticos las cuales necesiten de la implementación de controles para su funcionamiento seguro dentro de la organización. De la misma manera servirá como referencia para entender los conceptos de metodologías de análisis de riesgo, herramientas de análisis de riesgo, etc de manera más clara.

Un trabajo similar desarrollado en la Universidad Católica de Colombia en la facultada de Ingeniería, proyecto previo a la obtención del título de Ingeniero de Sistemas, realizado por Pascagaza, J. (2018) que lleva por título "DESARROLLO DE UN SISTEMA DE INFORMACIÓN PARA LA GESTIÓN DE LOS PROYECTOS DE RESPONSABILIDAD SOCIAL DEL PROGRAMA DE INGENIERÍA DE SISTEMAS

DE LA UNIVERSIDAD CATÓLICA DE COLOMBIA" el objetivo de esta investigación es el desarrollo de una herramienta Software para la gestión de proyectos.

Investigación que será utilizada como referencia para analizar las herramientas para el desarrollo de software, el ciclo y las metodologías de desarrollo de software.

Otra investigación similar desarrollado en la Escuela Politécnica Nacional, facultada de ingeniería de sistemas, realizado por Bravo, M. (2018) titulada "DESARROLLO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA BIBLIOTECAS BASADO EN UNA METODOLOGIA DE ANALISIS DE RIESGO COMPATIBLE CON LA NORMA ISO 27001:2013" en la cual se realiza un estudio de las metodologías para análisis y gestión de riesgos, una identificación de amenazas y riesgos en base a la metodología seleccionada, finalmente desarrolla un sistema de gestión.

Gracias a esta investigación se podrá determinar las metodologías de análisis y gestión de riesgo, y por lo mismo realizar una comparación para determinar el más adecuado para un correcto análisis con la ISO 27001.

Una investigación desarrollada en la Institución Universitaria Politécnica Gran Colombiano, facultad de ingeniería y ciencia básicas, realizado por Arlenys, C. titulada "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO/IEC 27001:2013" en el cual se evalúa los pilares básicos de la seguridad de la información, Integridad, confidencialidad y disponibilidad bajo la norma ISO 27001:2013.

Esta investigación será de gran ayuda para la elaboración del análisis del riesgo en el desarrollo del proyecto, nos facilita las pautas necesarias para seguir un orden adecuado en el análisis y avalar por la confidencialidad, disponibilidad e integridad de la información.

1.4 Justificación de la investigación

Muchas organizaciones buscan el mejoramiento continuo de su negocio, razón por la cual los sistemas de información se convierten en la parte fundamental, debido a la facilidad en la automatización de los procesos, para la correcta toma de decisiones, cabe mencionar que la seguridad de los sistemas de información es uno de los temas de mayor interés en el ámbito tecnológico, toda organización cuenta con información las cuales son consideradas como parte de los activos más importantes las mimas que pueden encontrarse expuestos a vulnerabilidades, por ende, es necesario protegerlo de amenazas tanto externas como internas mediante un sistema de gestión de riesgo.

La norma ISO 27001 (SGSI), facilita un estándar de calidad de seguridad de la información, el objetivo de esta norma o estándar es ayudar a las organizaciones a minimizar los riesgos y conservar los pilares de la seguridad de la información.

En la actualidad existen muchas herramientas tecnológicas para la gestión de riesgo que pueden ser utilizados por las organizaciones para determinar si se encuentran expuestos a riesgos, pero debido a la falta de recurso y al complejo uso de dichas herramientas las entidades optan por no utilizarlos.

El presente proyecto busca desarrollar un Software de fácil manejo y con los recursos necesarios para un correcto análisis y gestión de riesgo, basado en una metodología para gestión de riesgo y la norma ISO 27001, el uso de esta herramienta permitirá conocer las debilidades que existan en el manejo de la información, de manera que se pueda tomar acciones dentro de la entidad para su seguridad.

1.5 Objetivos

1.5.1 Objetivo general

Desarrollar un software de análisis de riesgos y gestión de seguridad para automatizar el proceso de gestión de riesgo basado en la norma ISO 27001.

1.5.2 Objetivos Específicos

- Realizar un estudio teórico sobre los sistemas de gestión de riesgo, ISO 27000, herramientas y metodologías para desarrollo de software.
- Seleccionar la metodología y herramienta para el desarrollo de software que se acople de mejor manera a la norma ISO 20701.
- Desarrollar el software de análisis de riesgos y gestión de seguridad basado en la norma ISO/IEC 27001 y en la metodología seleccionada de análisis y gestión de riesgo.

1.6 Limitaciones

- Tentativamente el proyecto se desarrollará en un lapso de 5 a 6 meses.
- El tiempo que se estima para la realización de este proyecto sea corto y resulte inalcanzable cumplir con los objetivos que se definieron l principio.

1.7 Delimitaciones

- El sistema a desarrollar será solo un prototipo y para que esta sea usable tendrá que pasar por un proceso de validación.

CAPITULO II

MARCO TEÓRICO

2.1 Seguridad informática

Según el artículo de Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001, dice “La seguridad informática está relacionada con las metodologías, procesos y procedimientos para mantener salvaguardada la información y los datos confidenciales de una organización, al interior de los sistemas informáticos”. (Solarte Solarte, Enriquez Rosero, & Benavides Ruano, 2015)

Según (Vieites, 2015) define la seguridad informática como “cualquier medida que impide la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema”.

Los aspectos a considerase a la hora de hablar de seguridad informática son:

- Cumplimiento de las regulaciones legales adaptables a cualquier tipo de organización, dependiendo el marco legal de cada país.
- Control de acceso tales como: contenidos digitales con derecho de autor, fichero de datos personales.
- Identificación de usuario a diferentes sistemas informáticos, etc.

2.2 La seguridad de la información

El autor (GASCO, 2013) define a la seguridad de la información como un "conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información".

Evalúa los riesgos, amenazas, determina un plan de acción para minimizar estos problemas, bajo normas, políticas, procesos y procedimientos que ayuden a garantizar la confidencialidad, integridad y disponibilidad del manejo de la información.

2.2.1 Confidencialidad

"La confidencialidad es un atributo de la seguridad de la información en cual se encarga a que la información no se divulgue a personas o sistemas que no tengan la autorización correspondiente, es decir que el acceso a la información lo puede realizar la persona que esté debidamente autorizada" (Aguilera Lopez, 2010).

2.2.2 Integridad

"La integridad es otro de los atributos de la seguridad de la información, su objetivo es mantener la información de manera exacta es decir tal cual fue creada al principio, sin modificación o alteración por otras personas que no están autorizada" (Aguilera Lopez, 2010)

2.2.3 Disponibilidad

"Todo dato o información se encuentra disponible para ser accedido en cualquier momento por los usuarios que estén autorizados, para ello se deben aplicar medidas de protección para asegurar la información, ejemplo crear copias de seguridad y mecanismos para restaurar los datos que por algún error sufrieron cambios o perjuicios, ya sea por fallos de hardware o actualizaciones del sistema" (Aguilera Lopez, 2010).

En conclusión, la disponibilidad hace referencia a que toda información manejada de manera pública y privada se encuentren disponibles en cualquier momento, información que será accedido siempre y cuando esté autorizado o por una persona designada a su autorización.

2.2 Análisis y gestión de riesgo de seguridad informática.

2.2.1 Análisis de riesgo

El análisis de riesgos es un proceso de mejora continua, que tiene por objeto estimar las probabilidades de que se exhiban acontecimientos que puedan ser peligrosos, determinando la gravedad de dicho impacto negativo, es decir estudia las posibilidades de identificar una vulnerabilidad, una amenaza y evaluar los riesgos que se puedan presentar ante un sistema informático, de manera que se pueda determinar las posibles causas que la provocan y definir un control de seguridad en base a los hallazgos, que permita disminuir la probabilidad de que se plasme una amenaza o reducir la vulnerabilidad del sistema o el posible impacto en la organización (Leon, 2007).

2.2.2 Gestión de Riesgos

La gestión de riesgos es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que peritan controlarlos. Este proceso ayuda a las organizaciones a entender de mejor manera cual es la situación actual en la que se encuentra la seguridad de la misma, el cual permitirá la toma de decisiones para determinar las medidas necesarias a implementarse para minimizar o evitar los riesgos (Parra Moreno, 2012).

2.2.3 Metodología para análisis y gestión de riesgo

2.2.3.1 Metodología Magerit

Esta metodología de análisis y gestión de riesgos de los sistemas de información fue elaborada por el consejo de administración Electrónica en España, este método es utilizado para la investigación de riesgos que puedan soportar los sistemas de información y para proponer medidas de seguridad adecuadas para el control de dichos riesgos (Ministerio de hacienda y administraciones Publicas, 2012).

El uso de esta metodología en las organizaciones es de gran importancia debido a que día a día la tecnología avanza y con ella aumentan los riesgos, por lo mismo, es necesario restar los riesgos que se muestran en el uso de los sistemas, de esta manera garantizando la confidencialidad, integridad y disponibilidad de los mismos. Esta metodología plantea 4 etapas:

- **Planeación del análisis y la gestión de riesgos**: En esta etapa se consideran opiniones que puedan ser necesarias para dar inicio al análisis de riesgos y el proyecto de gestión, el cual ayuda a determinar si es conveniente llevarlo a cabo.
- **Análisis de Riesgos:** En esta etapa se identifica y evalúa cada uno de los elementos que intervengan en el riesgo, con el fin de lograr una evaluación del riesgo en las diferentes áreas del domino.
- **Gestión de Riesgos:** En esta etapa se identifica las salvaguardias necesarias que ayuden a reducir el riesgo que han sido detectados.
- **Selección de salvaguardas:** En esta etapa se selecciona las salvaguardas necesarias a implementarse, agrupa los documentos de trabajo para el

análisis de riesgo y el proceso de gestión, presenta las documentaciones finales del proyecto y exhibe los resultados en diferentes niveles.

- **Objetivos**

  La metodología Magerit persigue los siguientes objetivos

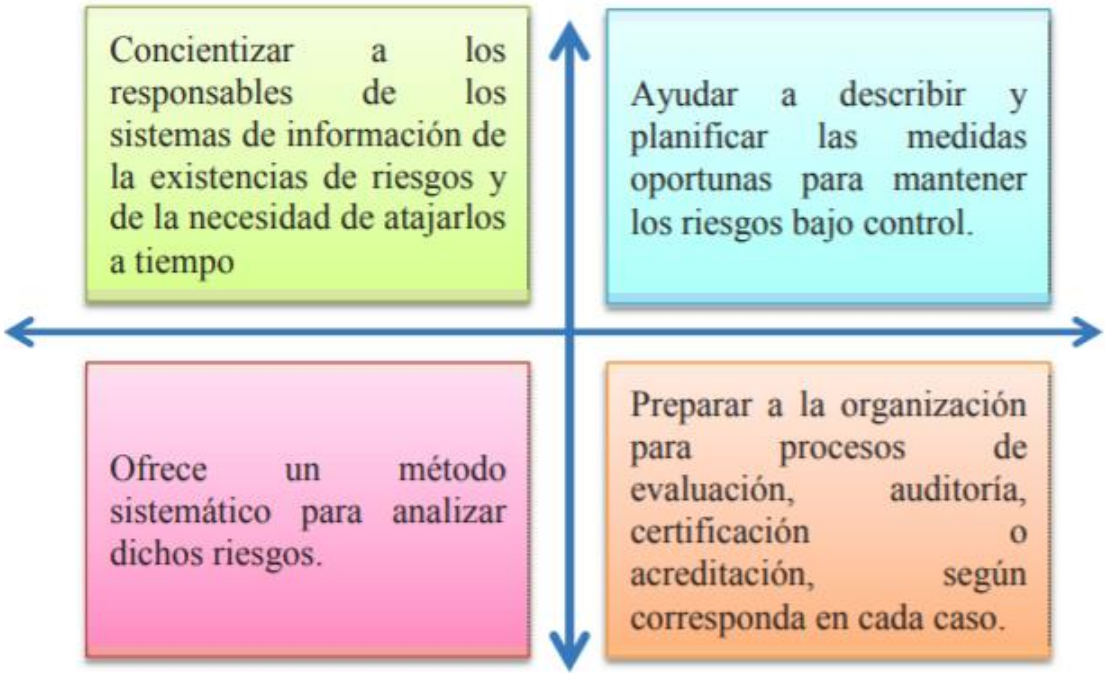


Ilustración 1: Objetivos de Magerit; Fuente: (Jesus & Guadalupe, 2018)

Magerit maneja sub-modelos, tales como elementos de seguridad (actividades, amenazas, impacto, riego y salvaguardas), proceso de seguridad (planificación, análisis de riesgo, gestión de riesgo, gestión de salvaguardas) (Jesus & Guadalupe, 2018).

- **Pasos de la metodología MAGETIR**

  La metodología magerit ejecuta los siguientes pasos:

  - Determinar los activos relevantes para la organización, su valor.
  - Determinar a que amenaza están expuestas aquellos activos.

- Determinar que salvaguardas hay dispuestas y cuan eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como impacto con la tasa de ocurrencia o probabilidad de la amenaza.

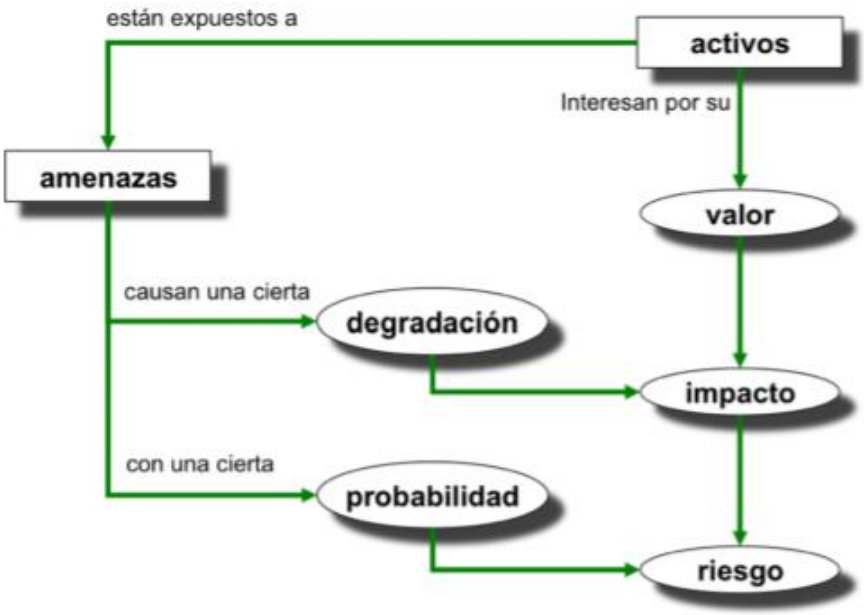


Ilustración 2: Elementos del análisis de riesgo potenciales; Fuente: (Ministerio de hacienda y administraciones Publicas, 2012)

2.2.3.2 Metodología CRAMM

La metodología CRAMM fue desarrollada por la Agencia Central de Cómputo y telecomunicaciones, es utilizada para el análisis y gestión de riesgos con el objetivo de proteger la confidencialidad, la integridad y disponibilidad de la información de un sistema y de sus activos. Esta metodología ofrece información acerca del funcionamiento del sistema y una identificación profunda y clara de los activos que son más arriesgados; se divide en 3 etapas:

- **Identificación de activos y valoración:** Esta etapa permite identificar los activos tanto físicos, el software y los datos que conforman el sistema de información, estos activos son establecidos en diferentes términos, es decir los activos físicos en términos de costo de reanudación, mientras que los activos de datos y software, en términos del impacto causado en caso de que la información no se encontrara disponible.
- **Evaluación de amenazas y vulnerabilidades:** Esta fase tiene como objetivo determinar la probabilidad de que los inconvenientes se originen, siendo CRAMM una metodología que cubre toda variedad de amenazas que puedan perturbar a los sistemas de información.
- **Selección de contramedidas y recomendaciones:** esta fase realiza una comparación entre la evaluación de los riesgos y el nivel de seguridad que se desea obtener, de manera que se pueda determinar la gravedad de los riesgos y así poder justificar la instalación de una contramedida.

2.2.3.3 Metodología Octave Allegro

Esta metodología estudia los riesgos mediante 3 elementos tales como la confidencialidad, integridad y disponibilidad, valora los riesgos de seguridad de la información y requiere menos tiempo de implementación. OCTAVE es una metodología que busca hacer entender a la organización que la seguridad informática no es un solo asunto técnico, sino que también, es un asunto no técnico.

Esta metodología trabaja con 3 fases para su desarrollo:

- **Construir perfiles de amenazas basados en activos:** Esta primera fase determina las amenazas que consiguen inquietar a los activos de una

organización y las medidas de seguridad que se encuentran establecidas para salvaguardara dichos activos.

- **Identificar vulnerabilidades de la infraestructura:** Esta segunda fase determina las vulnerabilidades a nivel de infraestructura de TI, que puedan llevar a una acción no autorizada.
- **Desarrollar las estrategias y los planes de seguridad:** Esta tercera fase se define un plan y estrategias de seguridad en base a los riesgos encontrados, las mismas que pueden afectar en la organización.

2.2.3.4 Metodología MEHARI

Es metodología es un conjunto de funcionalidades para la gestión de la seguridad, mediante un análisis de riesgo clara y precisas, el objetivo de esta metodología es proporcionar métodos que puedan ser útiles para determinar las medidas de seguridad más óptima y adaptable para la organización.

2.2.3.5 Metodología NIST SP 800:30

Esta metodología se caracteriza por establecer prioridades a los controles y a los perfiles claves para disminuir los riesgos, es la más apropiada para ser la guía del análisis de riesgo de la inseguridad personal de los usuarios en las redes de datos y de los sistemas de TI.

Esta metodología esta compuestas por 9 fases tales como:

- **Caracterización de sistema:** Esta fase permite determinar el alcance que tendrá una evaluación de riesgos en la organización.
- **Identificación de amenazas:** se identifican las amenazas para determinar la probabilidad de que estas puedan perjudicar o causar daños a los sistemas

de TI, esta fase permite conocer cada una de las debilidades del sistema las cuales pueden ser aprovechadas por una amenaza.

- **Análisis de controles:** en esta fase se analizan los controles necesarios que ayuden a mitigar los riesgos que se puedan presentar en la organización**.**
- **Determinación de probabilidad:** Esta fase busca determinar la probabilidad existente de que una vulnerabilidad pueda ser aprovechada por una amenaza.
- **Análisis de impacto:** En esta fase se analiza los impactos a los que la organización pueda enfrentarse, es decir si una amenaza identificada por la organización se materializa se determinaría el impacto de la misma y así se podría minimizar los riesgos.
- **Determinación de riesgos:** se realiza una estimación de los riesgos del sistema de información, para determinar el nivel de los mismos, y buscar soluciones en base a los controles establecidos, para poder reducirlos o eliminarlos.
- **Recomendaciones de control:** Se establecen controles que ayuden a prevenir o eliminar los riesgos identificados en los sistemas TI.

2.2.3.6 Matriz comparativa de las metodologías de gestión de riesgo

Tabla 1: Matriz de las metodologías de gestión de riesgo, Magerit, Octave, Mehari, Cramm.

Metodología /Estándar	Tipos de análisis	Caracterización y valoración de activos	Caracterización y valoración de amenazas	Caracterización y valoración de vulnerabilidades	Estimación de riesgos	Tratamiento de riesgos
MAGERIT	Análisis cuantitativos y cualitativos	Detalla la forma de caracterizar activos y hace su valoración, provee de ejemplos y sugiere técnicas	Detalla la forma de caracterizar amenazas y hace su valoración, provee de ejemplos y sugiere técnicas	No se considera explícitamente	Detalla la forma de estimar el impacto del riesgo, estimar el riesgo e interpretar los resultados, provee de ejemplos y sugiere técnicas.	Provee un proceso detallado para la gestión de riesgos.
OCTAVE	Análisis cuantitativos y cualitativos	Detalla la forma de caracterizar activos, provee guías y ejemplos	Detalla la forma de caracterizar amenazas, provee guías y ejemplos	Detalla la forma de caracterizar vulnerabilidades, provee guías y ejemplos	Se identifican los riesgos y se evalúa el impacto en términos de una escala predefinida (alto, medio, bajo)	Se basa en el desarrollo de: - Estrategias de protección - Planes de mitigación y lista de acciones
CRAMM	Análisis cuantitativos o cualitativos	Describe procedimientos para la	Describe procedimientos para	Describe procedimientos para la	Describe el procedimiento para la estimación del riesgo.	No se considera explícitamente.

		identificación y valoración de activos	la evaluación de amenazas.	evaluación de vulnerabilidades		
AS/ NZS ISO 31000	Análisis Cualitativo, Cuantitativo	No se define explícitamente un método de identificación y valoración de activos.	No se define explícitamente un método de identificación y valoración de amenazas.	No se define explícitamente un método de identificación y valoración de vulnerabilidades	Se sugieren métodos cualitativos y cuantitativos que pueden ser aplicados. No detalla alguna técnica en particular.	Estrategias: - Evitar el riesgo - Reducir la probabilidad de ocurrencia. - Reducir las consecuencias. - Transferir los riesgos. - Retener los riesgos
MEHARI	Análisis cuantitativos y cualitativos	Describe procedimientos para la identificación de activos	Describe procedimientos para la identificación de amenazas.	Describe procedimientos para la identificación de vulnerabilidades	Describe procedimientos para la estimación del riesgo.	- Retención del riesgo - Reducción del riesgo - Evitar el riesgo - Transferencia del riesgo

2.3 SGSI: Sistema de Gestión de Seguridad de la Información

El SGSI es el concepto central sobre el que se construye ISO 27001. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías (Iso27000, 2012).

Un sistema de gestión de seguridad de la información, es una herramienta que cualquier empresa organización puede utilizar. La norma ISO 27001 le permite establecer políticas, procedimientos y controles con el fin de minimizar los riesgos que se presentan en una organización.

2.3.1 Nivel de madurez

- **Incipiente:** Quiere decir que, no existe un plan de seguridad, un proceso de gestión, ni un marco normativo que esté debidamente formalizado. Se aplican controles de seguridad, pero no se encuentran normalizado.
- **Bajo:** No existe un plan de seguridad, ni un proceso de gestión, si existe un marco normativo debidamente documentado y formalizado, pero no se encuentra alineado a un estándar internacional relacionado a la seguridad de la información.
- **Medio:** Si existe un plan de seguridad, pero no está alineado a las estrategias de la entidad, existe un proceso de gestión y un marco normativo.
- **Alto:** Existe un plan de seguridad alineado a la estrategia de la entidad, un proceso de gestión y un marco normativo documentado, formalizado y alineado a algún

marco o estándar de referencia internacional en materia de seguridad de la información (Costa Rica, 2017).

2.4 Familia ISO 27000

La Organización Internacional de Estándares (ISO, 2013) "desarrolla la serie de normas 27000 que contienen las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) e incluyen":

- Sistema de gestión de la seguridad de la información
- Valoración de riesgos
- Controles

2.4.1 Norma ISO/IEC 27001:2013

La ISO 27001 es una de las principales normas de la serie 27000, fue desarrollado con el fin de proporcionar un modelo que permita implementar y llevar un control de un SGSI. La norma establece que en el SGSI se debe proteger la confidencialidad, integridad, y disponibilidad de la información, a tal punto que las partes interesadas confíen en que los riesgos son gestionados debidamente, a su vez establece que las partes interesadas no son solamente los accionistas o propietarios sino también incluye a las personas interesadas directa o indirectamente en la organización, así como las autoridades legales y regulatorias.

2.4.1.1 Beneficios de la norma ISO/IEC 27001

"Permite disminuir posibles riesgos de vulnerabilidades en los sistemas informáticos y en la información en general manejada por personal de la empresa, además mejora los procesos y servicios prestados, teniendo una mejor organización de los procesos, aumentando la competitividad de la empresa debido a que se demuestra el interés por

salvaguardar la integridad, confidencialidad y disponibilidad de la información de los clientes" (Bermudez Molina & Bailon Sanchez, dspace.ups.edu.ec, 2015).

2.4.1.2 Dominios de la seguridad de la ISO/IEC 27001

- Política de seguridad
- Organización de la seguridad
- Gestión de activos
- Seguridad de los recursos humanos
- Seguridad Física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad de los negocios
- cumplimiento (Iso27000, 2012).

2.4.2 Norma ISO/IEC 27002:2013

La norma ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)" (Iso27000, 2012).

2.4.2.1 Estructura de la norma ISO 27002

La ISO 27002, en su versión 2013 está compuesta de 14 dominios, 35 objetivos de control y 114 controles siendo cada una de ellas de gran importancia.

A continuación, se muestra una lista de todos los controles que sujeta esta norma:

Tabla 2: Estructura de la Norma ISO 27002:2013; Autor: Propio

Estructura de la norma		
Dominio		**Control**
5	Políticas de seguridad de la información	Dirección de la gestión de la seguridad de la información
6	Organización de la seguridad de la información	Organización interna. Dispositivos móviles y teletrabajo.
7	Seguridad de los recursos humanos	Previo a la contratación. Durante el empleo Terminación y cambio de empleo
8	Gestión de activos	Responsabilidades por los activos Clasificación de la información Manejo de los medios de almacenamiento
9	Control de acceso	Requerimientos de negocio del control de accesos Gestión de acceso de usuarios Responsabilidades de los usuarios Control de acceso de sistemas y aplicaciones.
10	Criptografía	Controles criptográficos
11	Seguridad física y ambiental	Áreas seguras

		Seguridad del equipamiento
12	Seguridad de las operaciones	Procedimientos y responsabilidades operacionales. Protección contra el malware Respaldo Registro de monitoreo Control del software operativo Gestión de las vulnerabilidades técnicas Consideraciones de la auditoria de sistemas de información.
13	Seguridad de las comunicaciones	Gestión de la seguridad de redes Transferencia de información
14	Adquisición, desarrollo y mantenimiento de sistemas	Requerimientos de seguridad de los sistemas de información Seguridad en los procesos de desarrollo y soporte Pruebas de datos.
15	Relaciones con proveedores	Seguridad de la información en las relaciones con proveedores Gestión de entrega de servicios de proveedores
16	Gestión de incidentes de seguridad de la información	Gestión de incidentes y mejoras de la seguridad de la información
17	Aspectos de la seguridad de la información en la gestión de continuidad de negocios	Continuidad de seguridad de la información Redundancias

18	Cumplimiento	Compromiso con los requerimientos legales y contractuales. Revisiones de la seguridad de la información

2.5 Metodologías de desarrollo de Software

2.5.1 Scrum

Scrum a más de ser una metodología de desarrollo de software, es un método de gestión de proyectos, el cual puede adaptarse a diferentes tipos de proyectos. Aplicada al desarrollo de software, scrum está basada en el modelo de la metodología agiles, incrementales, interacciones y revisiones continuas. “Esta metodología tiene como objetivo engrandecer al máximo la productividad del equipo de desarrollo. Reduce al máximo las actividades no orientadas a producir software funcional y promueve resultados en periodos cortos de tiempo” (Chancusi, Ordoñez, & Ortega).

Scrum se caracteriza por ser un modelo que define un conjunto de prácticas y roles que pueden tomarse como punto de inicio para definir los procesos a ser trabajados durante el proyecto.

- **Actividades a realizar con Scrum**

  Sprint Planning: La planificación de las tareas se las realiza en iteración, el cual consta de 2 reuniones cada una de ellas con una duración de 4 horas máximo, donde se tratan puntos específicos como el levantamiento de requerimientos para el desarrollo de software.

  Sprint: Los proyectos en scrum son ejecutados por bloques temporales cortos y fijos. La ejecución de cada sprint deberá proporcionar un resultado completo y satisfactorio.

Product Backlog: La lista de requerimientos representa la visión y expectativa del cliente con respecto al software que desea obtener. El cliente es el responsable de crear y gestionar la lista de requisitos.

Srum Taskboard: "La lista de objetivos a completar en el sprint se puede gestionar mediante un tablón de tareas (ScrumTaskboard). Al lado de cada objetivo se ponen las tareas necesarias para completarlo, en forma de post-its, y se van moviendo hacia la derecha para cambiarlas de estado (pendientes de iniciar, en progreso, hechas)" (ORTIZ & SUAREZ, 2017).

Modelo de desarrollo aplicando SCRUM

- **Beneficios**
  - Scrum define las tareas necesarias para poder completar cada requisito.
  - Realiza una estimación de tiempo necesario para desarrollar cada tarea.
  - Es el equipo o desarrollador que asume la responsabilidad de completar en la iteración los requisitos que selecciona.
  - Scrum distingue entre dos elementos principales: Actores y acción. Los actores son los que ejecutan la acción, y las acciones son cada una de las fases del ciclo de desarrollo del Scrum.

2.5.2 XP

La metodología XP es el más detectado de los procesos agiles de desarrollo de software. “La programación extrema se diferencia de las metodologías tradicionales principalmente en que pone más énfasis en la adaptabilidad que en la previsibilidad. El ciclo de vida ideal de XP consisten en 6 fases: exploración, planificación de la entrega, iteraciones, producción, mantenimiento y muerte del proyecto” (Ulloa, 2014).

- Ventajas y desventajas de la metodología XP
    - **Ventajas:**

      Programación organizada.

      Menor taza de errores.

      Satisfacción del programador.
    - **Desventajas:**

      Es recomendable emplearlo solo en proyectos a corto plazo.

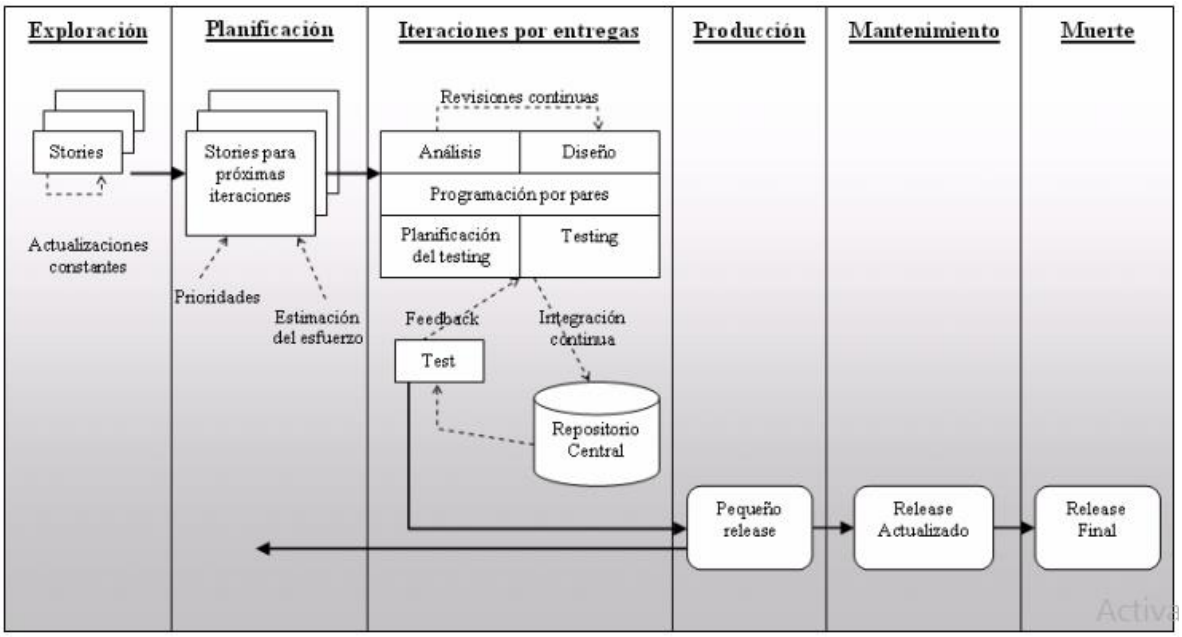
      Altas comisiones en caso de fallar.
    - **Beneficios:**

      El cliente tiene el control sobre las prioridades.

      Se hacen pruebas continuas durante el proyecto.

La XP es mejor utilizada en la implementación de nuevas tecnologías donde los requerimientos cambian rápidamente.

Tabla 3: Ciclo de vida XP; Fuente: (Calabria & Píriz, 2003)



2.6 Lenguajes de Programación

Un lenguaje de programación es aquel elemento dentro de la informática que nos permite crear, diseñar y desarrollar programas mediante una serie de instrucciones y reglas que ponen a disposición del programador para que este pueda comunicarse con los dispositivos hardware y software.

2.6.1 PHP

Los PHP son lenguajes de programación usados generalmente en la creación de contenidos para sitios web, usado originalmente para el desarrollo de aplicaciones que actúen a lado del servidor, capaces de generar contenido dinámico en la World Wide web.

El lenguaje de programación PHP nace en el año 1994, como un paquete de programas CGI creado por Rasmus Lerdorf. Es un software libre gratuito y de código abierto, licenciado bajo la PHP License, una licencia incompatible con la GNU debido a las restricciones en los términos de uso de PHP (Arias, 2013).

❖ **Características de PHP**

- Velocidad y robustez
- Estructurado y orientado a objetos
- Portabilidad, independencia de plataforma, ejecuta en cualquier lugar.
- Tapeado dinámico
- Sintaxis similar a C++ y Perl
- Open-source.

Ilustración 3: Lenguaje de programación PHP.

2.6.2 Java

"El lenguaje de programación Java nace en el año de 1996 por la empresa Sun Microsystems, del JDK 1.0, disponible de manera gratuita para las personas que están inmersas en el desarrollo de aplicaciones Java" (COBO, GÓMEZ, & PÉREZ, 2005).

Java es un lenguaje de programación clásico, se pueden crear dos tipos de programas tales como:

- **Applets:** Programas que se integran en las páginas web y que, residiendo en el servidor, son ejecutados por el cliente. La ejecución necesita de la interpretación del código compilado por el software cliente.
- **Aplicaciones:** Programas autónomas que se pueden ejecutar en cualquier equipo. Se generan códigos con compilación y para su ejecución necesitan de un intérprete o código compilado ejecutable directamente como cualquier otro lenguaje de programación (COBO, GÓMEZ, & PÉREZ, 2005).

❖ **Características de Java**

Java es un lenguaje con altas prestaciones, mucho mayor que las de lenguajes interpretados.

- Es un lenguaje orientado a objetos
- Admite programación concurrente
- Dispone de clases de objetos para la gestión de interfaces graficas de usuario
- Tiene prestaciones multimedia
- Resulta un lenguaje familiar, al tener una sintaxis similar al C++, el uso de punteros, la gestión de la memoria y el control de acceso a los elementos de arrays.
- Es un lenguaje simple, robusto y seguro
- A través de internet se puede acceder a todo lo necesario para desarrollar applets Java

Ilustración 4: Lenguaje de programación Java.

2.6.3 ASP.NET

"El lenguaje de programación ASP nace en el año de 2002, ASP.NET es un lenguaje de programación que permite crear aplicaciones tanto de escritorio como para entorno web, donde se puede programar en cualquiera de los lenguajes de .NET" (Villach, 2010).

❖ **Características**

- ASP.NET se integra totalmente con .NET, y sus páginas se pueden programar en cualquiera de los lenguajes de .Net, haciendo uso de la programación orientada a eventos
- ASP.NET es compilado. Esto ofrece múltiples ventajas, como un rendimiento mucho mejor, y una depuración mucho más potente
- La configuración y despliegue es mucho más sencillo, ya que la configuración tiene lugar en único archivo texto, y para hacer el despliegue basta con copiar los archivos en el directorio correspondiente (Villach, 2010).

Ilustración 5: Lenguaje de programación ASP. NET.

2.7 Gestores de Base de Datos Relacionales

"Una base de datos denominado como un conjunto de datos almacenados sistemáticamente para su posterior uso. Existen programas denominados sistema de gestión de base de datos (SGBD), las cuales permiten almacenar y acceder a los datos de forma rápida y estructurada" (Caiza, 2012).

2.7.1 Microsoft SQL Server

SQL Server es un SGBD producido por Microsoft basado en el modelo relacional, constituye la alternativa de Microsoft a otros potentes SGBDs.

- **Características**
  - Soporte de transacciones.
  - Escalabilidad, estabilidad y seguridad.
  - Soporta procedimiento almacenados
  - Incluye también un potente entorno grafico de administración.

- Permite trabajar de modo cliente-servidor, donde la información y datos se alojan en el servidor y los terminales o clientes de la red solo acceden a la información (Martín, 2010).

❖ **Desventajas**

- Es un SGBD propietario
- MS-SQL server tiene 6 tipos de licencias según el tipo de usuario (Trovamala & Bahena).
- MSSQL usa Address Windowing para el direccionamiento de 64-bit. Esto le impide usar la administración dinámica de memoria y solo le permite alojar un máximo de 64 GB de memoria compartida (Gomez).

Ilustración 6: Gestor de base de datos SQLServer.

2.7.2 Oracle

Es un sistema de gestor de base de datos relacional, desarrollado por Oracle Corporación. Este sistema de gestor de base de datos es considerado como uno de los más completos.

❖ **Ventajas**

- Soporte multiplataforma
- Herramienta cliente/servidor
- Cuenta con soporte de transacciones, estabilidad, escalabilidad (Martín, 2010).

El SGBD relacional Oracle está compuesto por tres partes principales, que son:

- El kernel de Oracle
- Las instancias del sistema de Base de Datos
- Los archivos relacionados al sistema de Base de Datos (Martín, 2010).

Ilustración 7: Gestor de base de datos Oracle.

2.7.3 PostgreSQL

"PostgreSQL es un servidor de base de datos el mismo que es un objeto racional y libre porque incluye características orientado a objetos tales como: herencia, tipo de datos, restricciones, funciones, reglas e integridad transaccional. Es un gestor de base de datos

dirigido a la comunidad de desarrolladores conocidas como PGDG (PostgresSQL Global Development Group)" (Ibarra & Flores, 2008).

- **Ventajas de PostgreSQL**
  - Posee código abierto.
  - Es ideal para una variedad de modelos de negocios a una gran escala.
  - Es flexible y estable.
  - Es multiplataforma.
  - Tiene una gran capacidad de almacenamiento.
  - Es un sistema muy estable.
  - Posee un alto rendimiento (Ibarra & Flores, 2008).

- **Desventajas de PostgreSQL**
  - La sintaxis de comandos no es intuitiva
  - Este gestor de base de datos requiere una cantidad más grande de recursos en Hardware (Ibarra & Flores, 2008).

Ilustración 8: Gestor de base de datos PostgreSQL.

2.7.4 MySQL

MySql fuera creador en 1995 por la empresa MySQL AB, con el afán de crear una solución eficiente y sencilla como económicas para los usuarios y profesionales frente a complicado y costosas soluciones que existen.

MySql es un motor de base de datos de código abierto, uno de los más populares para el desarrollo con software libre, su fácil integración con lenguajes de programación hace que sea una herramienta fácil de usar.

❖ **Ventajas de MySql**

- Lo mejor de MySQL es la velocidad a la hora de realizar operaciones, lo que le convierte en un gestor de mejor rendimiento.
- Su bajo consumo hace que se pueda ejecutar en una maquina con escasos recursos sin problema alguno.
- Las utilidades de administración son mejores a los demás gestores de base de datos, debido a su factibilidad de configuración e instalación.
- El conjunto de aplicaciones Apache-PHP-MySQL son unos de los más usados en internet en servicio de foro y de buscadores de aplicaciones (Alvarado & Garcia, 2006).

❖ **Desventajas de MySQL**

- Carece de soporte para transacciones y su consulta
- El hecho de que no maneje la integridad referencial, hace de este gestor una solución sobre para muchos campos de aplicación.
- No es viable para su uso con grandes bases de datos, a las que se accede continuamente (Alvarado & Garcia, 2006).

Ilustración 9: Gestor de base de datos MySQL.

CAPITULO III

Marco Metodológico

3.1 Enfoque de la Investigación

El presente trabajo de investigación tiene la necesidad de desarrollar un software de análisis de riesgos y gestión de seguridad basada en ISO 27001, utilizando un enfoque mixto ya que maneja variables cualitativas como cuantitativas.

3.2 Nivel de Investigación

El nivel de investigación para el presente proyecto será descriptivo, debido a que se realizará una recolección de información de la metodología tanto para el desarrollo de software como para el análisis y gestión de riesgo, de la misma manera para la selección de la herramienta.

3.3 Población y muestra

No aplica

3.4 Técnicas e instrumentos de recolección

Toda información necesaria para el desarrollo del presente trabajo investigativo será obtenida a través de libros digitales, artículos científicos, revistas, etc.

3.5 Tratamiento de la información

La información recolectada será confidencial y debidamente tratada, ya que serán la base fundamental para el desarrollo del sistema.

3.6 Interpretación de resultados

En el presente capitulo se realizará la elección de la herramienta, la metodología para el desarrollo del sistema, de la misma manera se seleccionará la metodología de gestión de riesgo que se acople con la norma ISO 27001 que será abordado en el sistema.

3.7 Matriz comparativa de las metodologías para el desarrollo del software

Tabla 4: Matriz comparativa de las metodologías para desarrollo de software; Autor: Propio.

Criterio	Metodologías Para desarrollo de software		
	XP	**SRUM**	**PMBOK**
Integración	-Integración tan ponto y a menudo como sea posible. -Propiedad colectiva del código. -Medición de la velocidad del proyecto.	-Verifica aprobación del proyecto y su financiación en las fases de planificación. -Validad herramientas e infraestructuras en la fase de planificación. -Gestión de cambios con el producto.	-Desarrolla acta constitución del proyecto -Desarrolla en plan del proyecto. -Dirige la ejecución del proyecto. Monitoriza y controla el trabajo del proyecto.
Fases	- Planificación - Diseño - Codificación - Prueba - Lanzamiento	- Inicio - Planificación y estimación - Implementación - Revisión y retrospectiva - Lanzamiento	- Arranque - Planeación - Ejecución y control - Cierre
Alcance	-Historias de usuario -Planificación de lanzamiento, pequeñas versiones.	-Analizar y construir el modelo esquemático del proyecto. - Elaboración de la lista de backlog del proyecto.	- Plan de alcance - Recopila requisitos - Define y controla el alcance

		-Definición de funcionalidades que se incluirá en cada versión. -Seleccionar versión más adecuada para desarrollo inmediato.	
Coste		Estimación de costes de la versión en la fase de planificación.	- Plan de costes - Estimación de costes - Determina el presupuesto - Controla los costes
Calidad	- Énfasis en el testing - Uso de estándares de calidad y pruebas	- Revisión y ajustes las normas con el que el proyecto se acordó - Reunión revisión del diseño - Reunión Planificación y revisión del sprint	- Plan de calidad - Realiza aseguramiento de calidad. - Realizar controles de calidad
Recursos humanos	-Rotación del personal en varios puestos - Programación en pareja - Buenas condiciones de trabajo.	- Nombramiento del equipo de proyecto para cada versión - Participaciones del equipo en reuniones de sprint - Participación del equipo en scrums diario.	- Plan de RRHH - Adquirir el equipo - Dirigir el equipo
Riesgos	-Crear prototipo para reducir riesgos.	- Evolución de riesgos al inicio del proyecto -Revisar los riesgos en las reuniones de revisión.	-Plan e identificación de riesgo - análisis cuantitativo - Plan de respuesta - Monitorizar y controlar
Comunicaciones	- Usar lenguajes no técnicos para explicar el proyecto	- Comunicación de las normas del proyecto al equipo - Reunión para la revisión de diseño.	- Plan de comunicaciones - Dirigir las comunicaciones - Controlar las comunicaciones

	- Cliente siempre disponible - Reuniones diarias	- Reunión para la planificación del sprint

3.7.1 Selección de la metodología para desarrollo de software

En base a una investigación realizada por Zambrano, W. (2017) en el cual analiza cada uno de los criterios mencionados en la Tabla 4, mediante la aplicación de un formato de entrevista en referencia al marco internacional y nacional realizada por la empresa *Versiones Agile Made Easier*, obtiene que la metodología scrum obtiene un 50%, xp 18.4% en cuanto a los criterios de evaluación analizados, mencionando que dichos criterios son las principales mejoras que se evidenciaron al implementar metodologías agiles.

De la mismas manera un estudio comparativo de las metodologías para desarrollo de software Tabla 4, realizado por Rodríguez Manuel en su proyecto "Estudio comparativo entre metodologías agiles y las metodologías tradicionales para la gestión de proyectos de software", menciona que no existe una metodología perfecta que garantice el éxito de cualquier tipo de proyecto, pero resalta que las metodologías agiles son las más utilizadas en la actualidad, las mismas deben ajustarse al tipo de proyecto que se desarrolle, y por ello recomienda el uso de dichas metodologías para la ejecución de proyectos de software.

En base a estas investigaciones se opta por la selección de las metodologías agiles, en este caso para el desarrollo del presente proyecto se utilizará la metodología Scrum, el cual consta de 4 conceptos importantes, Product Backlog, Sprints, Daily Meeting, Sprint Review, los cuales serán abordados para el desarrollo del software.

3.8 Matriz comparativa de lenguajes de programación

Tabla 5: Matriz comparativa de los diferente lenguajes de programación; Autor: Propio.

Criterios	Lenguajes de programación orientado a objetos			
	PHP	**Java**	**C++**	**C#**
Características	• Utilizado para generar páginas web dinámicas • Se ejecuta en el servidor • Los usuarios no pueden ver el código PHP únicamente recibe en sus navegadores código HTML • Lenguaje de alto nivel	• Este lenguaje de programación es orientado a objetos • Multiplataforma	• Orientado a objetos • Rápido	• Está orientado a objetos • Esta estandarizado por Microsoft como parte de su plataforma net.
Ventajas	• Es un lenguaje muy popular tiene una comunidad muy grande • Es multiplataforma y rápido • Libre y gratuito • Maneja base de datos	• Orientado Objetos • Es sencillo y practico, provee toda la funcionalidad de un lenguaje potente. • Sus sistemas de verificación le proveen	• Al aplicar un programa en C++ se genera código objeto, nativo de cada máquina. • Permite controlar la memoria y provee al programador la capacidad de programas a bajo nivel.	• No importa el orden en que hayan sido definidas las clases ni las funciones. • Conceptos formalizados de los métodos get y set.

	• Puede ser combinado junto a HTML • Consta de varios frameworks que facilitan el desarrollo en este lenguaje.	robustez, ya que realizan verificaciones de problemas tanto en tiempo de ejecución como en tiempo de corrida, por medio del cual detectan errores en el ciclo de desarrollo. • La ejecución del código Java es segura y fiable • Es completamente Multiplataforma • Es un entorno de programación multi-hilo • Soporta el desarrollo rápido de aplicaciones.		• .NET ofrece mucha documentación de ayuda incluida en el IDE y de soporte • Todos los códigos que se ejecutan en el ambiente .Net son compilados, lo cual proporciona un gran rendimiento a diferencia de versiones interpretadas.
Desventajas	• Necesita un servidor para funcionar • La POO es deficiente para aplicaciones grandes	• Debido a la capacidad de portabilidad que java presenta, el código de Java es convertido a un código intermedio,	• No es en un lenguaje multiplataforma. • No presenta una arquitectura estándar de	• El mantenimiento de proyectos en múltiples lenguajes es costoso

	Todo el trabajo se ejecuta en el servidor y mucha información puede ser ineficiente	llamado Byte, antes de convertirlo a código máquina. Este paso provoca que los programas escritos en Java sean más lentos que los demás programas realizados en otros leguajes.	desarrollo orientado a internet • No presenta un toolkit rico como otros lenguajes • Aunque existen varias librerías en la red para C++, no son estándar del lenguaje y algunas son de paga.	• .NET no es multiplataforma , solo está disponible para la familia de Windows • Es un código cerrado, no hay licencia libre, adquirir una representa un alto costo para las empresas.
Sistema Operativo	Unix-like, Windows	Unix, Linux, Solaris, Windows, Mac, etc.	Es posible lograr que las aplicaciones se ejecuten en varios sistemas operativos, pero se requiere de ciertos esfuerzos.	Windows
Opinión	El código PHP se procesa en un servidor web por un intérprete PHP implementado como un módulo o como un ejecutable de interfaz de entrada(CGI)	Las aplicaciones escritas en Java proveen independencia de la plataforma, robustez y fiabilidad.	La STL ofrece una serie de funciones que representan operaciones comunes, y cuyo objetivo es la parametrización de las operaciones, de modo que su lectura y mantenimiento sean más fáciles de realizar.	Es utilizado para desarrollar aplicaciones para el entorno .Net de Microsoft, ofrece un alternativa de desarrollo basado en JAVA.

3.8.1 Selección del lenguaje de programación para desarrollo de software

Con el desarrollo de la matriz comparativa Tabla 3, y el estudio realizado por Estrada Luis (2011), en donde se especifica las características, ventajas y desventajas de cada lenguaje de programación mencionadas se opta por realizar el software de gestión de riesgo con el lenguaje JAVA, debido que a más de ser el lenguaje más utilizado a nivel mundial, ofrece una gran variedad de ventajas y genera interfaces más cómodas e intuitivas a diferencia de los demás lenguajes de programación. El software será desarrollado en NetBeans ya que permite desarrollar productos de forma ágil, eficiente y eficaz aprovechando los puntos fuertes de la plataforma Java.

3.9 Cuadro Comparativa de los gestores de Base de Datos

Tabla 6: Matriz Comparativa de los Gestores de Base de Datos; Autor: Propio.

Criterio	**Gestores de Base de Datos Relacionales**		
	SQL Server	**MySQL**	**PostgreSQL**
Velocidad	Es un gestor completo y ejecuta de manera rápida miles d registros de las cuales se generan gráficos.	MySQL es mucho más rápido que la mayor parte de su competencia, ya que tiene la opción de seleccionar el mecanismo de almacenamiento que ofrece diferentes velocidades de operación, soporte físico, capacidad, distribución geográfica, transacciones.	La velocidad de respuesta del gestor es relativamente pequeña, puede parecer un poco deficiente. Es capaz de ajustarse al número de CPUs y a la cantidad de memoria que posee el sistema de forma optima

Modelo Conceptual	Modelo Relacional	Modelo Relacional	Orientado a objetos
Tipos de datos soportados	SQL Server soporta datos Como: Short, Long, Long text, Long binary.	Tipos numéricos, tipos de fechas, tipos de cadena	Tipos numéricos, tipos de caracteres, tipo de datos binarios, tipos de fecha, tipos booleanos.
Fiabilidad	SQL Server es más flexible y potente, su capacidad de programación permite albergar todo tipo de reglas de negocio	MySQL es ms fácil de utilizar y administrar. Las herramientas de MySQL son potentes y flexibles, sin sacrificar su capacidad de uso.	Sus características técnicas la hacen una de las base de datos más potentes.
Arquitectura de implementación	Cliente / servido	Cliente /servidor	Cliente / servidor
Manejo de transacción	La transacción más simple en SQL Server es una única sentencia UPDATE, es una transacción autocompletada.	MySQL cuenta con la agrupación de transacciones, reuniendo de varias conexiones parta incrementar el número de transacciones por segundo.	Limitación: Actualmente, las transacciones abortan completamente si se encuentra un fallo durante su ejecución.
Tamaño en registro		MySQL soporta hasta 50 millones de registros	Los registros son ilimitados(Depende del sistema de almacenamiento)

Interfaz	SQL Server proporciona unas interfaces como: interfaces graficas SQL server Management Studio, Visual Estudio, etc.	Existen varias interfaces de programación de aplicaciones que permiten, a aplicaciones escritas en diversos lenguajes de programación. C, C++, C#, Pascal.	La instalación de PostgreSQL incluye solo C y la interfaces embebidas de C.
Plataformas Soportadas	Windows	GNU/Linux, Windows. Usa GNU automake, Autoconf, y libtool para portabilidad.	Cualquier plataforma moderna tipo Unix debe ser capaz de ejecutar PostgreSQL

3.9.1 Selección del Gestor de Base de datos para el desarrollo del software

Los criterios mencionados en la tabla 5 fueron tomados de deferentes investigaciones, una de ellas "Comparación de desempeño de los sistemas de gestores de base de datos MySQL y PostgreSQL" realizado por López, P (2016) en el cual utiliza algunos criterios mencionados para comparar los gestores de base de datos.

En base a ello y demás investigaciones de los SGBD se desarrolló el cuadro comparativo, cabe mencionar que MySQL ha sido un gestor de datos utilizado a nivel mundial, debido a que soporta una gran cantidad de datos, y la velocidad al realizar operaciones le convierte en un gestor con un buen rendimiento, a vista de que cumple con cada uno de los criterios de manera óptima, se concluye que MySQL será apto para el desarrollo del software de gestión de riesgo.

3.10 CUADRO COMPARATIVO DE LAS METODOLOGÍAS DE ANÁLISIS DE RIESGOS

Tabla 7: Cuadro comparativo de las metodologías de análisis y gestión de riesgo; Autor: Propio.

Metodología	Ámbito de aplicación	Etapas/ fases que se llevan a cabo
MAGERIT	Uso preferente en la administración pública española, pero puede adaptarse a cualquier tipo de organización. Y está adaptada a los sistemas informáticos.	1. Análisis de riesgos 2. Caracterización de los activos • Caracterización de las amenazas • Caracterización de las salvaguardas • Estimación del estado del riesgo 3. Gestionar los riesgos
OCTAVE	Cualquier organización pública o privada. También está orientada a los sistemas informáticos.	**Fase 1.- Construir perfiles de amenazas basados en los activos** Proceso 1: Identificar el conocimiento de los altos directivos. **Fase 2.- Identificar vulnerabilidades en la infraestructura** Proceso 5: Identificar componentes claves Proceso 6: Evaluación de componentes seleccionados **Fase 3.- Desarrollar estrategias y planes de seguridad** Proceso 7: Realizar un análisis de riesgos Proceso 8: Desarrollar estrategias de protección
CRAMM	Uso preferente en la administración pública británica, pero puede ser adaptada a cualquier entidad pública o privada.	1. Definir marco de gestión de riesgo 2. Identificar riesgos 3. Identificar propietarios de los riesgos 4. Evaluar riesgos 5. Definir niveles aceptables de riegos 6. Identificar respuestas adecuadas al riesgo 7. Implantar respuestas 8. Obtener garantías de la efectividad

		9. Monitorizar y revisar.
AS/ NZS **ISO 31000**	Cualquier organización pública o privada. Estándar de carácter genérico orientado a una amplia gama de actividades, operaciones, procesos, funciones, proyectos, productos, servicios, activos.	1. Establecer el contexto 2. Identificar riesgos 3. Analizar riesgos 4. Evaluar riesgos 5. Tratar riesgos 6. Monitorear y revisar 7. Comunicar y consultar
MEHARI	Gobiernos, organismos, Empresas medianas y grandes, compañías comerciales, sin fines de lucro (Educación, salud, servicios públicos, organizaciones no gubernamentales) Orientada a los sistemas de información.	**Fase 1.- Valoración del riesgo** - Identificación del riesgo - Estimación de riesgos - Evaluación de riesgos **Fase 2.- Tratamiento del riesgo** - Retener el riesgo - Reducir el riesgo - Transferir el riesgo - Evitar el riesgo **Fase 3.- Gestión del riesgo** - Desarrollo de planes de acción - Implementación de planes de acción - Monitoreo

3.9.2 Selección de la metodología de análisis y gestión de riesgo

Las metodologías como **Magerit** y **Octave** brindan mayor amplitud para cada una de las etapas de análisis de riesgos, también brindan herramientas adicionales para apoyar el trabajo como guías, ejemplos, métodos de caracterización y valoración de catálogos de elementos y herramientas software.

Octave es una metodología que parte de la perspectiva de los integrantes que están más involucrados en los procesos y que brinden un enfoque desde la perspectiva organizacional y tecnológico.

Por su parte **Magerit** es una de las metodologías adecuadas a la hora de realizar un análisis y gestión de riesgos ya que proporciona pasos precisos para el proceso de análisis de riesgos, así como indica métodos particulares para la caracterización y valoración de activos, amenazas y salvaguardas, así también para la estimación del riesgo ya sean estos potenciales y residuales.

Existes investigaciones en las cuales hacen uso de diferentes criterios para la comparación de las metodologías, entre ellas las mencionadas en la Tabla 7, que fueron seleccionadas para el desarrollo de la presenta investigación debido a que se requiere conocer de manera clara el ámbito de aplicación de las metodologías y las fases que conlleva cada una de ellas, que permitan una correcta identificación, clasificación y priorización de los eventos que puedan tener impacto negativo para el logro de los objetivos.

En base a una matriz comparativa realizada de todas las metodologías de análisis y gestión de riesgo, en las cuales se evaluaron los siguientes criterios como, ámbito de aplicación, las etapas y las faces que lleva cada metodología para una correcta gestión de riesgo, se determinó que para el desarrollo del software de gestión de riesgo y seguridad será con la aplicación de la metodología MAGERIT, junto a la ISO 27001.

CAPITULO IV

PROPUESTA

4.1 Título de la Propuesta

"Desarrollo de software de análisis de riesgos y gestión de seguridad basado en ISO 27001".

4.2 Objetivos de la Propuesta

4.2.1 Objetivo General

Desarrollar un software de análisis de riesgos y gestión de seguridad para automatizar el proceso de gestión de riesgo basado en la norma ISO 27001.

4.2.2 Objetivo Específico

- Levantar los requerimientos necesarios para el desarrollo de software.
- Desarrollar la base de datos guiado en los requerimientos establecidos.
- Desarrollar el sistema de gestión de riesgo y gestión de seguridad.

4.3 Diseño del software de análisis de riesgo y gestión de seguridad

El software de análisis de riesgo y gestión de seguridad trabaja con:

La metodología MAGERIT para análisis y gestión de riesgo y la norma ISO 27001 para la gestión de seguridad.

4.4 Ejecución Del Proyecto

La ejecución del proyecto se llevó a cabo mediante el cumplimento de las fases de la metodología ágil Scrum, Aprovechando su enfoque dinámico a la hora de realizar un proyecto, obteniendo resultados satisfactorios.

4.4.1 Fase 1: Inicialización

El trabajo de investigación denominado “Desarrollo de software de análisis de riesgo y gestión de seguridad”, pretende ayudar a las organizaciones a conocer los riesgos que pueden presentar al materializarse una amenaza en los diferentes activos de información, está basada en una metodología ágil denominada Scrum.

Los requerimientos para el desarrollo de software fueron analizados en base a una matriz de riesgo realizada con la metodología Magerit y la norma ISO 27001, identificando los tipos de activos, la dimensión de calificación y amenazas con las que trabaja Magerit, de la misma manera se otorga un valor al impacto y probabilidad puntos importantes en la metodología Magerit para estimar el nivel del riesgo.

- **Matriz de riesgo tomando la metodología Megerit y la norma ISO 27001**

Tipo de activo	Codigo	Activo	Dimenciones de Valoracion						Catalogo de Amenazas	Calculo del Riesgo				Tratamiento de los Riesgos		
							Bajo 1 Medio 2 Alto 3 Muy Alto 4 Critico 5			Insignificante 1 Menor 2 Moderado 3 Mayor 4 Catastrófico 5	Improbable 1 Probable 2 Casi Seguro 3	FE = I*P	R= VA*FE Bajo 1--37 Medio 38--74 Alto 75--111 Critico 112--375		Bajo 1 Medio 2 Optimo 3	
			Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	TOTAL /25	Amenazas	Impacto	Probabilidad	Factor de Exposición	RIESGO	Control	Eficiencia de Control	Riesgo Residual
[SW] Software - Aplicaciones informáticas	SW-Ac1	Sistema Integrado de Servicios Municipales	5	5	5	5	4	24	[I.5] Avería de origen físico o lógico	5	2	10	240	**11 SEGURIDAD FÍSICA Y AMBIENTAL**. 11.1 Áreas seguras. 11.1.1 Perímetro de seguridad física. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.2 Seguridad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos.	3	80
									[E.1] Errores de los usuarios	4	1	4	96		3	32
									[E.2] Errores del administrador	4	2	8	192		2	96
									[E.8] Difusión de software dañino	5	2	10	240		2	
									[E.9] Errores de [re-]encaminamiento	4	1	4	96		3	
									[E.14] Escapes de información	5	2	10	240		3	
									[E.20] Vulnerabilidades de los programas (software)	4	2	8	192		3	
	SW-Ac2	Sistema AME (Asociación de Municipalidades Ecuatorianas) Para la gestión contable	5	4	5	4	4	22	[E.10] Errores de secuencia						3	
									[E.15] Alteración accidental de la información	1	1	1	22			
									[E.18] Destrucción de información	3	1	3	66			
									[E.21] Errores de mantenimiento / actualización de programas (software)							
									[E.24] Caída del sistema por agotamiento de recursos							
									[A.6] Abuso de privilegios de acceso							

Ilustración 10: Matriz de riesgo (Requerimiento para el desarrollo de software); Autor: Propio

4.4.2 Planificación y Estimación

Una de las fases de la metodología ágil para el desarrollo de software es la planificación, por lo que esta etapa será analizada una vez durante el desarrollo de cada sprint. Para ello se inició con la identificación del Product Backlog o requerimientos del producto.

Product backlog o pila

El desarrolle del software de gestión de riesgo fue en base al product backlog, el cual consiste en determinar o recoger los requerimientos necesarios para el desarrollo del sistema, el cual ira mejorando a medida que lo hace el producto.

Tabla 8: Historial de Requerimiento; Autor: Propio

Historial de Requerimientos

ID	Requerimientos funcionales	Descripción
M1	Creación de la base de Datos	Se creara el esquema de base de datos para la carga de información, teniendo en cuenta las relaciones existentes entre las demás tablas, de la misma forma validar la carga de información, en este caso el tipo de activo, tipo de amenaza, tipo de control y la recuperación de la misma.
M2	Acceso al Sistema (Login)	Para el Login se usara un usuario y una contraseña registrada en la base de datos del sistema, para poder tener acceso
M3	Mantenimiento Usuario(Crear, Modificar, Eliminar)	La persona responsable del sistema podrá crear un nuevo usuario con la información requerida,

		de igual forma se podrá modificar, eliminar en caso se requiera y actualizarlo.
M4	Mantenimiento de Activos(Crear, Modificar, Eliminar)	Una vez ingresado el usuario, podrá ingresar los activos, de acuerdo a su tipo, de la misma manera podrá modificar, eliminar y actualizar..
M5	Mantenimiento de Amenazas(Crear, Modificar, Eliminar)	La persona responsable podrá registrar las amenazas que afecten a los activos ingresados, y la misma será cargada con su tipo de amenaza correspondiente.
M6	Creación del menú Administrador	El menú del Administrador deberá estar enlazado a todos los módulos establecidos, permitiendo el acceso a las mismas.
M7	Reporte - Calculo del Riesgo	Se generara un solo reportes donde se visualice los activos, valor de los mismos, la Amenaza, el impacto, probabilidad, el nivel de riesgo, los controles, y el riesgo residual.

4.4.1.1. Definición de los Sprints.

En este apartado se define cada Sprint según sea la importancia de los requerimientos de usuario, el tiempo de trabajo y la dedicación para el desarrollo del mismo.

Tomando en cuenta el nivel de importancia de cada requerimiento se procede a agrupar las mismas y determinar la cantidad de Sprints para el proyecto, obtenido lo siguiente:

Tabla 9: Tabla de estimación del Sprint Nº 1; Autor: Propio.

Modulo	Requerimiento	Prioridad	Tiempo de estimación
MBD	Creación de la Base de Datos	Alta	15 días
MLG	Acceso al Sistema (Login)	Alta	10 días
	Total de días del Sprint		**25 días**

Tabla 10: Tabla de estimación del Sprint Nº 2; Autor: Propia.

Modulo	Requerimiento	Prioridad	Tiempo de estimación
MU	Mantenimiento Usuario(Crear, Modificar, Eliminar)	Alta	15 días
MA	Mantenimiento Activos(Crear, Modificar, Eliminar)	Alta	15 días
MM	Mantenimiento de Amenazas(Crear, Modificar, Eliminar)	Alta	15 días
	Total de días del Sprint		**45 días**

Tabla 11: Tabla de estimación del sprint Nº 3; Autor: Propio.

Modulo	Requerimiento	Prioridad	Tiempo de estimación
MM	Mantenimiento de Control(Crear, Modificar, Eliminar)	Alta	15 días
MMA	Creación del menú Administrador	Alta	15 días
MCR	Calculo del Riesgo	Alta	15 días
MR	Reporte	Alta	15 días
Total de días del Sprint			**60 días**

4.4.1.2. TaskBoard inicial y Burn Down Chart Inicial

En esta siguiente etapa se presenta el Taskboard de desarrollo inicial del proyecto con todos los requerimientos y la condición inicial de cada uno de Sprints. En la siguiente tabla N° 11 el taskboard de los requerimientos se encuentra en un estado de pendiente las mismas que serán finalizadas según el avance del proyecto, para ello se estudiara cada módulo para su posterior desarrollo.

Tabla 12: Taskboard de desarrollo inicial del proyecto sus respectivos requerimientos; Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos	■		
	Acceso al Sistema (Login)	■		
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)	■		
	Mantenimiento Activos(Crear, Modificar, Eliminar)	■		
Sprints Nº 3	Mantenimiento de Amenazas(Crear, Modificar, Eliminar)	■		
	Creación del menú Administrador	■		
	Reporte - Calculo del Riesgo	■		

4.4.3 Implementación

4.4.3.1 Desarrollo del sistema

Sprint Nº 1

Creación de la Base de Datos

El desarrollo de este primer Sprint se lleva a cabo por semanas cumpliendo el tiempo establecido en la fase 2.

Primera Semana:

- En la siguiente tabla se muestra el Taskboard de la primera semana, donde el requerimiento “Creación de base de Datos” se encuentra en curso.

Tabla 13: TaskBoard Primera Semana; Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos		■	
	Acceso al Sistema (Login)	■		
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)	■		
	Mantenimiento Activos(Crear, Modificar, Eliminar)	■		
Sprints Nº 3	Mantenimiento de Amenazas(Crear, Modificar, Eliminar)	■		
	Creación del menú Administrador	■		
	Reporte - Calculo del Riesgo	■		

Segunda Semana:

En esta semana se finaliza con el diseño de la base de datos, el cual contiene todos los campos y parámetros necesarios para el desarrollo del software de análisis de riesgo y gestión de seguridad.

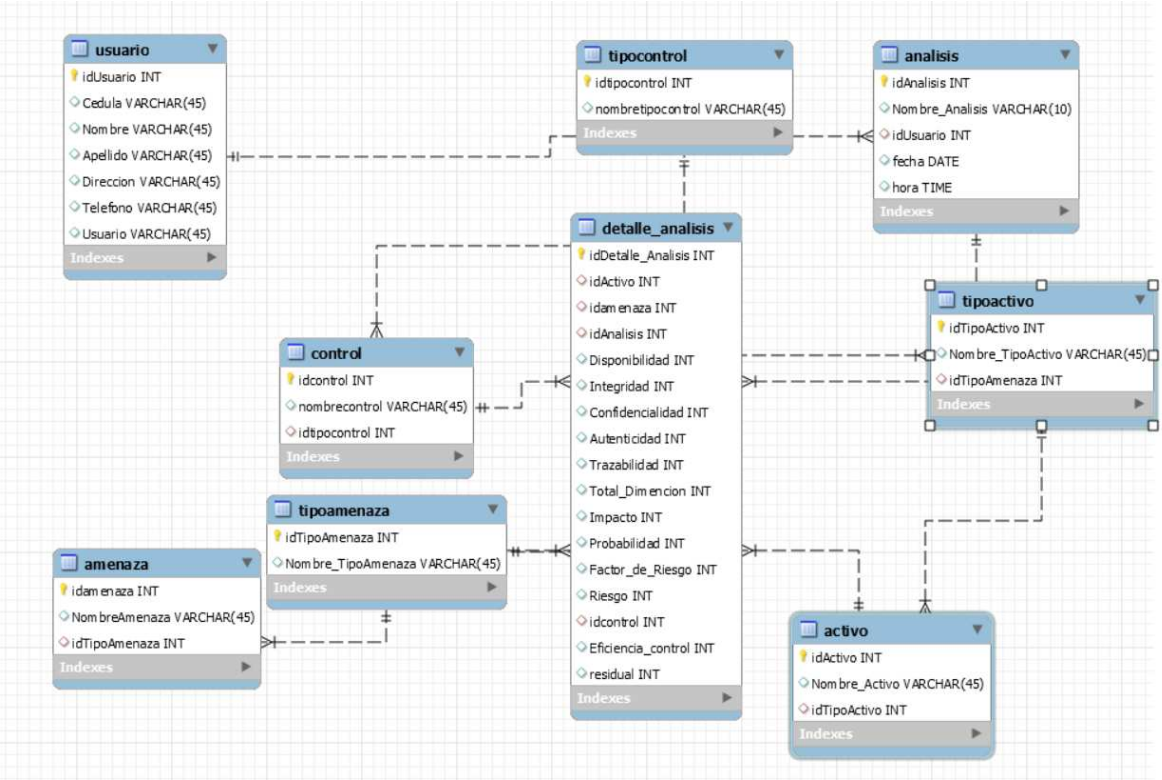


Ilustración 11: Diseño de base de datos para el análisis de riesgo y gestión de seguridad; Autor: Propio.

Se muestra el Taskboard de la segunda semana, donde el requerimiento de usuario "Creación de Base Datos" perteneciente al sprint 1 se encuentra finalizada y el Login se encuentra en curso.

Tabla 14: Taskboard de la segunda semana (Creación de la Base de Datos); Autor: Propio.

Sprints	**Requerimiento de Usuario**	**Pendiente**	**En curso**	**Hecho**
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)		■	
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)	■		

	Mantenimiento Activos(Crear, Modificar, Eliminar)	■
	Mantenimiento de Amenazas(Crear, Modificar, Eliminar)	■
Sprints Nº 3	Creación del menú Administrador	■
	Reporte - Calculo del Riesgo	■

Acceso al Sistema (Login)

Semana 3:

Esta semana se inicia con el diseño de la interfaz del LOGIN, en el cual se analizará los colores y logos, de la misma manera los datos y campos a ingresar para su acceso.

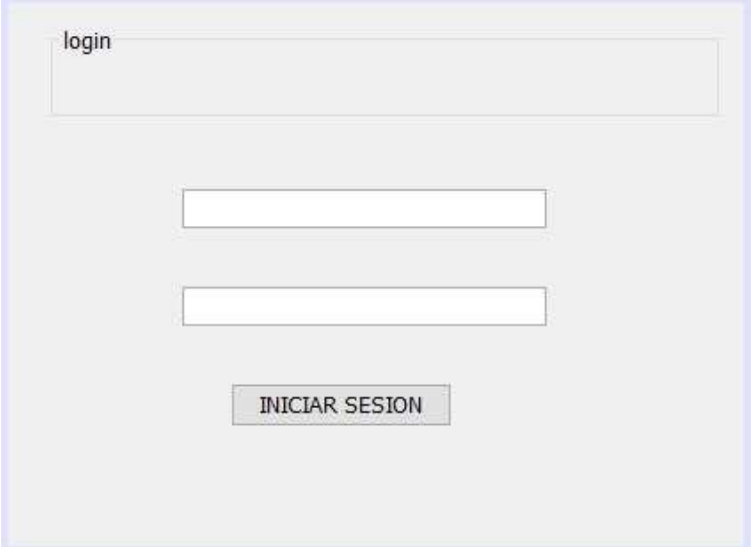


Ilustración 12: Interfaz - Acceso al sistema Login; Autor: Propio.

Una vez finalizada con la interfaz, se procede con la ejecución del código para poder validar si el usuario y contraseña son correctos. Al reconocer el usuario y contraseña, el software permitirá el acceso sistema.

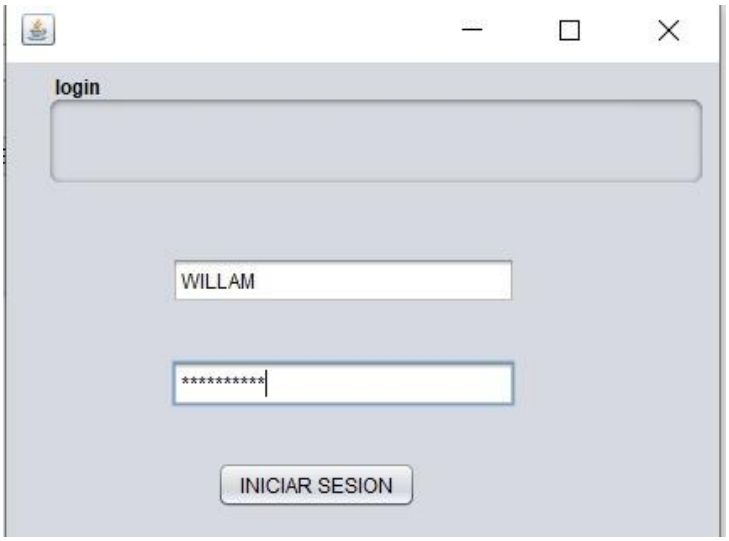


Ilustración 13: Validación de usuario y contraseña para el ingreso al sistema; Autor: Propio.

Como resultado se muestra el Taskboard de la semana 3, donde el requerimiento de usuario "Acceso al sistema (Login)" del Sprint1 se encuentra finalizada.

Tabla 15: Resultados obtenido de la semana 3; Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)			■
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)	■		
	Mantenimiento Activos(Crear, Modificar, Eliminar)	■		
Sprints Nº 3	Mantenimiento de Amenazas(Crear, Modificar, Eliminar)	■		
	Creación del menú Administrador	■		
	Reporte - Calculo del Riesgo	■		

Sprint Nº 2

Mantenimiento Usuario (Crear, Modificar, Eliminar)

Cuarta Semana:

Se muestra el Taskboard de la cuarta semana, en donde el requerimiento "Mantenimiento de usuario" que corresponde al sprint 2 se encuentra en curso.

Tabla 16: Taskboard curta semana (Mantenimiento de Usuarios); Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)			■
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)		■	
	Mantenimiento Activos(Crear, Modificar, Eliminar)	■		
	Mantenimiento de Amenazas (Crear, Modificar, Eliminar)	■		
Sprints Nº 3	Mantenimiento de Control (Crear, Modificar, Eliminar)	■		
	Creación del menú Administrador	■		
	Calculo del Riesgo	■		
	Reporte	■		

Quinta Semana:

Mantenimiento de Usuarios

En la siguiente pantalla se muestra los datos necesarios para el registro de los usuarios quienes vayan a realizar un análisis de riesgo, los datos solicitados son los siguientes: Cedula, Nombres, Dirección, teléfono, dichos usuarios pueden ser Actualizados o eliminados.

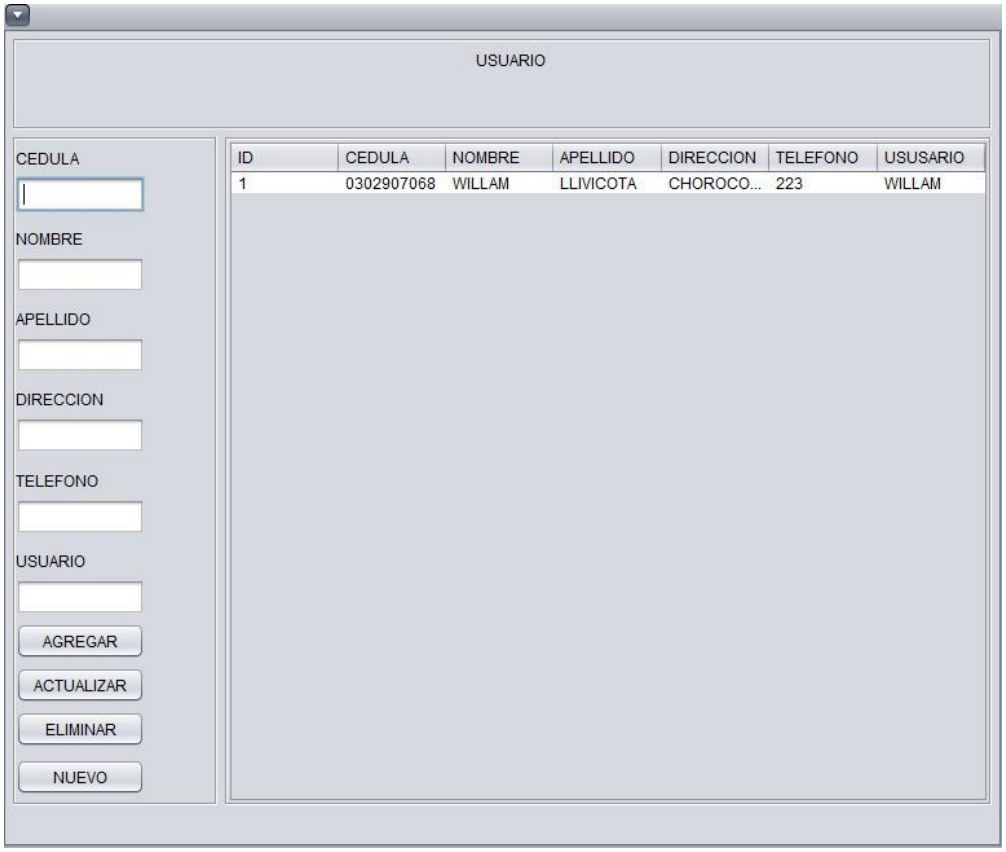


Ilustración 14: Interfaz de ingreso de usuarios; Autor: Propio.

Los datos ingresados de los usuarios son almacenados en la base de datos, se verifica la funcionalidad de cada botón, se llena los campos solicitados y al presionar agregar se nos carga en la tabla, con doble clic en el usuario se carga en todos los campos antes mencionados, se modifica uno de ellos y al presionar actualizar se guarda con los cambios realizados.

Se muestra el Taskboard de la quinta semana, donde el requerimiento “Mantenimiento de usuario” del Sprint 2 se encuentra finalizada.

Tabla 17: Taskboard del cumplimiento de requerimiento "Mantenimiento de Usuario"; Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)			■
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)			■
	Mantenimiento Activos(Crear, Modificar, Eliminar)		■	
	Mantenimiento de Amenazas(Crear, Modificar, Eliminar)	■		
Sprints Nº 3	Mantenimiento de Control (Crear, Modificar, Eliminar)	■		
	Creación del menú Administrador	■		
	Calculo del Riesgo	■		
	Reporte	■		

Mantenimiento Activos (Crear, Modificar, Eliminar)

Sexta y séptima Semana:

El software mostrara los campos inicializados en blanco y la relación con el tipo amenazas ya creadas en la Base Datos, los datos podrán ser actualizados o eliminados. El sistema validara que los datos ingresados sean correctos, en la misma ventana se visualizara una lista con todos los activos ingresados y su respectiva amenaza.

Ilustración 15: Interfaz de mantenimiento de activos, Agregar, Actualizar, Eliminar, Nuevo; Autor: Propio.

Se muestra el Taskboard de la Sexta y séptima semana, donde el requerimiento "Mantenimiento de Activo" se encuentra finalizada correspondiente al Sprint Nº 2.

Tabla 18: Taskboard de cumplimiento de requerimiento "Mantenimiento de Activo"; Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)			■
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)			■
	Mantenimiento Activos(Crear, Modificar, Eliminar)			■

	Mantenimiento de Amenazas (Crear, Modificar, Eliminar)	■
	Mantenimiento de Control (Crear, Modificar, Eliminar)	■
Sprints Nº 3	Creación del menú Administrador	■
	Reporte - Calculo del Riesgo	■

Mantenimiento de Amenazas (Crear, Modificar, Eliminar)

Octava y novena Semana:

El software mostrara los campos en blanco y la relación con el tipo de amenazas ya creadas en la Base Datos, los datos podrán ser actualizados o eliminados, permite la creación de nuevas amenazas. El sistema validara que los datos ingresados sean correctos, en la misma ventana se visualizara una lista con todas las amenazas ingresadas y su respectivo tipo amenaza.

Ilustración 16: Interfaz de mantenimiento de Amenazas,, Agregar, Actualizar, Eliminar, Nuevo; Autor: Propio.

A continuación, se muestra el Taskboard de la octava y novena semana, en el cual demuestra el cumplimiento del requerimiento “Mantenimiento de Amenazas” determinando la finalización del módulo y del Sprint 2. Se coloca en curso el módulo de “control2 del Sprint 3.

Tabla 19: Taskboard de cumplimiento del requerimiento "Mantenimiento de Amenazas"; Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)			■
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)			■
	Mantenimiento Activos(Crear, Modificar, Eliminar)			■
	Mantenimiento de Amenazas (Crear, Modificar, Eliminar)			■
Sprints Nº 3	Mantenimiento de Control (Crear, Modificar, Eliminar)		■	
	Creación del menú Administrador	■		
	Calculo del Riesgo	■		
	Reporte	■		

Sprint Nº 3

Mantenimiento de control (Crear, Modificar, Eliminar)

Semana 10, 11:

En la ilustración Nº 6 se muestra la ventana de registro de los controles de la norma ISO 27001, en el cual se indica cuáles son los campos necesarios para el registro de los mimos,

permite la selección de tipo de control que ya son almacenados en la base de datos, la información almacenada podrá ser actualizado o eliminado en caso ser necesario. Una vez registrado los controles estas son cargados en una lista en la parte izquierda de la ventana.

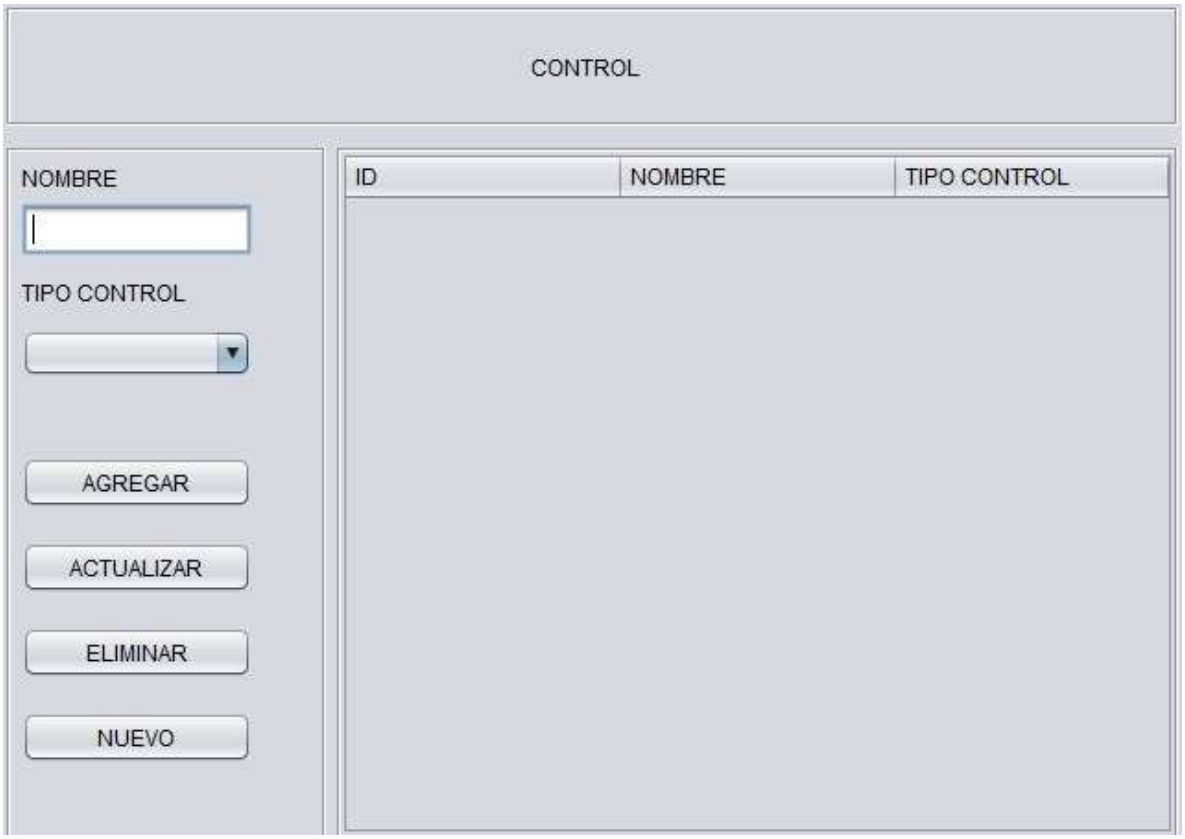


Ilustración 17: Ventana de ingreso de control; Autor: Propio.

A continuación, se muestra el Taskboard del Sprint Nº 3 de la semana 10, 11, en el cual demuestra el cumplimiento del requerimiento "Mantenimiento de Control" finalizando con cada una de los puntos establecidos.

Tabla 20: Taskboard de cumplimiento del requerimiento "Mantenimiento de control"; Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)			■

Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)			■
	Mantenimiento Activos(Crear, Modificar, Eliminar)			■
	Mantenimiento de Amenazas (Crear, Modificar, Eliminar)			■
Sprints Nº 3	Mantenimiento de Control (Crear, Modificar, Eliminar)			■
	Creación del menú Administrador		■	
	Calculo del Riesgo	■		
	Reporte	■		

Creación del menú Administrador

Semana 12, 13:

En la ilustración Nº 18 se muestra la ventana del menú en el cual se encuentran los módulos antes mencionados, esta ventana permitirá accedes a las diferentes sub-ventanas para realizar la tarea respectiva.

Ilustración 18: Menú administrador; Autor: Propio.

En la siguiente tabla Nº 21 se muestra el Taskboard de la semana 12, 13, en el cual se da cumplimiento al requerimiento “Creación del menú Administrador” determinando la finalización del presente modulo

Tabla 21: Taskboard de la semana 12, 13 (Creación del menú administrador); Autor; Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)			■
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)			■
	Mantenimiento Activos(Crear, Modificar, Eliminar)			■
	Mantenimiento de Amenazas (Crear, Modificar, Eliminar)			■
Sprints Nº 3	Mantenimiento de Control (Crear, Modificar, Eliminar)			■
	Creación del menú Administrador			■
	Calculo del Riesgo		■	
	Reporte	■		

Calculo de riesgo

Semana 14, 15:

En la siguiente ilustración Nº 7, se visualiza la ventana del cálculo de riesgo, esta interfaz cuenta con el cálculo de los activos, el cual visualiza los activos, tipo activos y el cálculo del mismo, con su respectiva dimensión de valoración obteniendo un total según el rango establecido.

Al seleccionar el activo, las amenazas son cargadas automáticamente, en base a ello se le otorga un valor al impacto y a la probabilidad con el cual se obtiene el FE, al multiplicar dicho resultado por el total del activo se obtienen el nivel de riesgo y los controles para mitigarlos.

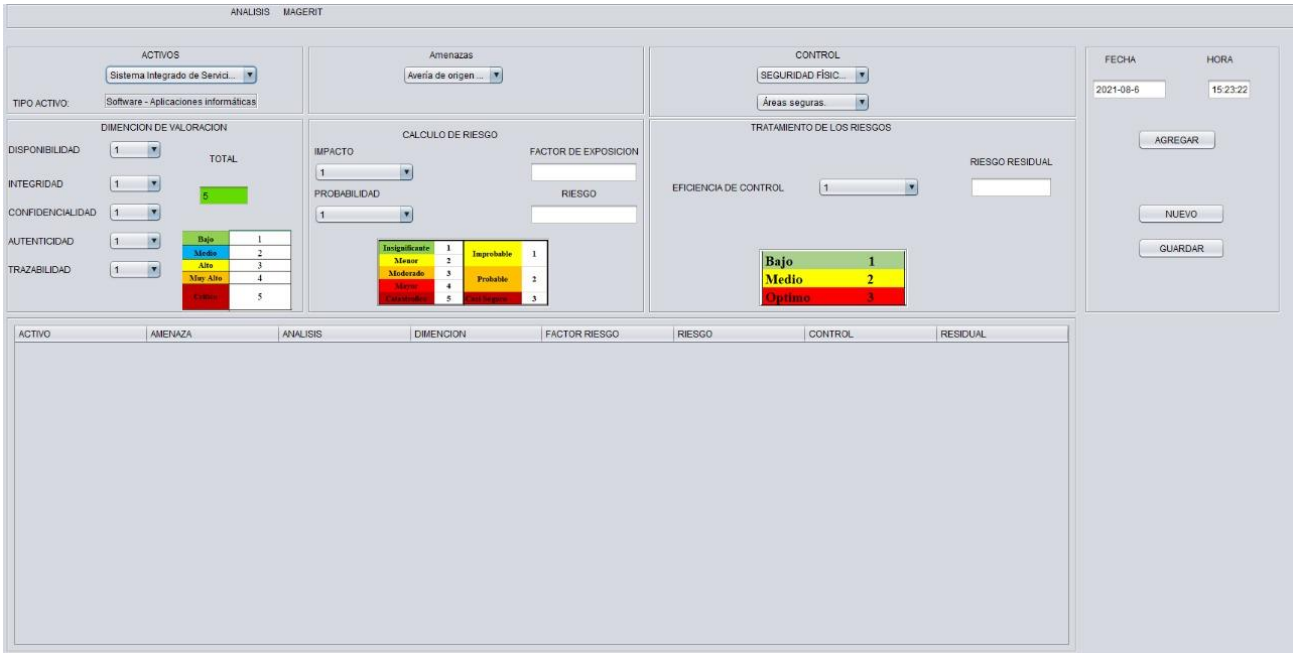


Ilustración 19: Software de cálculo de Riesgo; Autor: Propio.

En la siguiente tabla Nº 22 se muestra el Taskboard de la semana 14, 15, en el cual se da cumplimiento al requerimiento “Calculo de Riesgo” obteniendo como resultado un cálculo de riesgo satisfactorio, así dando finalización del presente modulo y colocando en curso al siguiente que corresponde a los “reportes”.

Tabla 22: Taskboard semana 14, 15 (Calculo del riesgo); Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)			■
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)			■
	Mantenimiento Activos(Crear, Modificar, Eliminar)			■
	Mantenimiento de Amenazas (Crear, Modificar, Eliminar)			■
Sprints Nº 3	Mantenimiento de Control (Crear, Modificar, Eliminar)			■
	Creación del menú Administrador			■
	Calculo del Riesgo			■
	Reporte		■	

Reporte

Semana 16, 17:

En esta semana se realiza el ultimo modulo correspondiente al requerimiento de "Reportes" en el cual se muestra los resultados obtenidos en el análisis de riesgo, cargando los datos de los siguientes campos, Activo, Amenaza, Dimensión, Factor de Riesgo, Riesgo, Control, eficiencia, Riesgo Residual.

REPORTE ANALISIS MAGERIT

ACTIVO	TOTAL DIMENSION	AMENAZA	FACTOR RIESGO	RIESGO	CONTROL	EFICIENCIA DEL CONTROL	RIESGO RESIDUAL
Sistema Integrado de Servicios Municipales	5	Avería de origen físico o lógico	1	1	Áreas seguras.	null	1
Sistema Integrado de Servicios Municipales	7	Avería de origen físico o lógico	3	21	Áreas seguras.	null	7
Sistema Integrado de Servicios Municipales	24	Avería de origen físico o lógico	10	240	Áreas seguras.	3	80

Ilustración 20: Reporte del cálculo de riesgo (Análisis de riesgo y gestión de seguridad); Autor: Propio.

En la siguiente tabla se muestra el Taskboard de la semana 16, 17 correspondientes al Sprint Nº 3, con el requerimiento "Reportes" y con ello se concluye el Sprint 4 y todos los módulos establecidos.

Cumplimiento de todos los requerimientos de usuario y obtención del software de análisis de riesgo y gestión de seguridad para su respectiva revisión.

Tabla 23: Taskboard de requerimientos cumplimento de módulos y obtención del software; Autor: Propio.

Sprints	Requerimiento de Usuario	Pendiente	En curso	Hecho
Sprints Nº 1	Creación de la Base de Datos			■
	Acceso al Sistema (Login)			■
Sprints Nº 2	Mantenimiento Usuario(Crear, Modificar, Eliminar)			■
	Mantenimiento Activos(Crear, Modificar, Eliminar)			■

	Mantenimiento de Amenazas (Crear, Modificar, Eliminar)	■
Sprints Nº 3	Mantenimiento de Control (Crear, Modificar, Eliminar)	■
	Creación del menú Administrador	■
	Calculo del Riesgo	■
	Reporte	■

4.4.4 Revisión

Nombre del Proyecto	Desarrollo de software de análisis de riesgos y gestión de seguridad basado en ISO 27001
Fecha	17/08/2021
Numero de Sprint	3

	¿Que salió bien en el Sprint?	**¿Que no salió bien en los Sprint?**	**Recomendaciones**
Sprint Nº 1	La recuperación de datos para el login y la base de datos se ejecutaron sin mayor complicación.	El tiempo de ejecución del segundo requerimiento tomo un poco más de tiempo, pero al final del sprint se logró finalizar.	Se recomienda mantener actualizado el Taskboard para mantenerse informado para no generar retraso en el desarrollo.
Sprint Nº 2	El realizar cada módulo de manera	Al tener mantenimiento	Se recomienda realizar la programación por

	independiente y con un oren especifico no se presentaron problemas a la hora de generar y enlazar los cogidos para la carga de datos.	independiente se tuvo que cargar datos en una ventana para poder recuperar en otra.	modulo ya que facilita su desarrollo y ayuda a mantener concentrado en el mismo enfoque.
Sprint Nº 3	Al tener ya todos los módulos creados y bien indexados la finalización del proyecto fue más sencilla.	Los tiempos de desarrollo para cada historia de usuarios fueron muy cambiantes.	Se recomienda hacer un análisis de todas las actividades que se puedan presentar dentro del desarrollo del proyecto, y así evitar prolongación de plazos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se realizó investigaciones de los temas más relevantes en cuanto al SGSI y metodologías de análisis de riesgo, en el cual se concluye que la normativa ISO/IEC 2001: 2013 desempeña un papel importante a la hora de desarrollar un software de gestión de seguridad ya que ayuda en la identificación de controles que garantizan la seguridad de la información.

Por otra parte, las metodologías de análisis y gestión de riesgo ayudan a comprender la importancia de la información que toda organización maneja ya que vienen siendo activos importantes para el funcionamiento de los mismos.

Se estudiaron metodologías de análisis de riesgo informáticos, mediante una matriz comparativa, señalando como el más adecuado a MAGERIT, el cual permite un análisis de riesgo de la seguridad de los activos de información.

De igual manera se realizó un cuadro comparativo de las metodologías para desarrollo de software en el que se tuvo como resultado a Scrum, siendo el método ágil y eficaz en la ejecución del proyecto.

Por otra parte, se realizó un análisis de los lenguajes de programación optando por Java para la ejecución del proyecto, gracias al empleo de las buenas prácticas que propone Scrum, permitió llevar acabo el desarrollo del software de una manera ordenada, adecuada y correcta.

Se llevó acabo el desarrollo de prototipo de software de análisis de riesgo y gestión de seguridad de la información basada en la metodología MAGERIT y la implementación de los controles de la norma ISO/IEC 27001 y la guía de buenas prácticas ISO 27002.

Recomendaciones

- Se recomienda, la creación del equipo de trabajo de desarrollo de software para realizar las mejoras del sistema de análisis de riesgo, manteniendo la metodología Scrum en miras de ejecutar futuros proyectos de mejora continua.
- Se recomienda mantener comunicación con el cliente y programador durante el proceso de desarrollo del software, con la finalidad de lograr una retroalimentación concreta que permita desplegar resultados satisfactorios, que cumpla con la expectativa deseada.
- Se recomienda realizar pruebas del sistema de forma continua de manera que ayude a reducir los posibles problemas que puedan presentarse a lo largo de una implementación de una iteración para lograr un producto funcional y de calidad.

Anexos

Anexo 1: Formato del Anteproyecto.

A. TÍTULO
Desarrollo de software de análisis de riesgos y gestión de seguridad basado en ISO 27001

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Analítica de Datos	
		Ingeniería de Software	X
		Algoritmos computacionales	
		Inteligencia de negocios	
		Gobierno de TI	
		Auditoria y Seguridad Informática	
		Simulación	

C. PLANTEAMIENTO DEL PROBLEMA
La información es uno de los recursos importantes en las organizaciones, pues de ella depende no solo la base del negocio, sino el logro de los objetivos a mediano o largo plazo, debido a que la información permite la toma de decisiones. Esta es una de las razones por las cuales, actualmente todas las empresas deberían realizar una apropiada gestión de riesgos, permitiéndoles de esa forma conocer las vulnerabilidades que poseen, las amenazas a las que se encuentran expuestas, evaluando dichas necesidades se determina el desarrollo de una solución de software de gestión de riesgos eficaz, gratuita y libre de uso que permita automatizar el proceso de gestión de riesgo, un a análisis de las amenazas y el cálculo de las mimas, determinando el nivel de riesgo a la que puedan estar expuestas las organizaciones y de la mimas manera que permita realizar un tratamiento adecuado y la selección de los controles apropiados para evitar dichos riesgos.

D. OBJETIVO GENERAL
Desarrollar un software de análisis de riesgos y gestión de seguridad para automatizar el proceso de gestión de riesgo basado en la norma ISO 27001.

E. OBJETIVOS ESPECÍFICOS
1. Realizar un estudio teórico sobre los sistemas de gestión de riesgo, ISO 27000, herramientas y metodologías para desarrollo de software.
2. Seleccionar de la metodología y herramienta para el desarrollo de software que se acople de mejor manera a la norma ISO 20701.
3. Desarrollar el software de análisis y gestión de riesgo.

F. JUSTIFICACIÓN
Muchas organizaciones buscan el mejoramiento continuo de su negocio, razón por la cual los sistemas de información se convierten en la parte fundamental, debido a la facilidad en la automatización de los procesos, para la correcta toma de decisiones, cabe mencionar que toda organización cuenta con información las cuales son consideradas como parte de los activos más importantes las mimas que al no contar con un sistema de gestión de riesgo pueden encontrarse expuestos a amenazas. La norma ISO 27001 (SGSI), facilita un estándar de calidad de seguridad de la información, el objetivo de esta norma o estándar es ayudar a las organizaciones a minimizar los riesgos y conservar los pilares de la seguridad de la información. En la actualidad existen muchas herramientas tecnológicas para la gestión de riesgo que pueden ser utilizados por las organizaciones para determinar si se encuentran expuestos a

riesgos, pero debido a la falta de recurso y al complejo uso de dichas herramientas las entidades optan por no utilizarlos.

El presente proyecto busca desarrollar un Software de fácil manejo y con los recursos necesarios para un correcto análisis y gestión de riesgo, basado en una metodología para gestión de riesgo y la norma ISO 27001.

G. ALCANCE

El alcance del presente proyecto será el desarrollo y prueba del Software de gestión de riesgo.

H. CONCEPTOS RELACIONADOS

Tecnologías y lenguaje

- ASP.NET
- PHP
- JavaScript
- Python

Sistema de información (SI)

Es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos. (López, 2010)

Políticas de seguridad

Recoge las directrices u objetos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la dirección. El objetivo principal de la redacción de una política de seguridad es la de

conciencia a todo el personal de una organización, y en particular al involucrado directamente con el sistema de la información, en la necesidad de conocer que principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados (López, 2010)

Norma ISO/IEC 27001

ISO/IEC 27001, en su apartado 0.3 Compatibilidad con otros sistemas de gestión, asegura que esta norma internacional sigue las pautas marcadas en las normas ISO 9001:2000 e ISO 14001:2014 para asegurar una implementación integrada y consistente con las mencionadas normas de gestión. Esta norma internacional está diseñada para posibilitar a una organización el adaptar su SGSI a los requisitos de los sistemas de gestión (Mesquia, Mas, Amengual, & Cabestrero, 2010)

ISO 27002

El estándar ISO/IEC 27002 fue creado con el objetivo de proporcionar la debida información a los responsables de la implementación de seguridad de la información. Es considerado como una buena práctica para el desarrollar y mantener normas de seguridad en una organización y así mejorar la confidencialidad de la seguridad de la información. En él se define las estrategias de 114 controles de seguridad organizados bajo 14 dominios. (ISOTools Excellence, 2017)

I. TRABAJOS RELACIONADOS

Existen distintos autores que han desarrollado investigaciones sobre el tema, cuyos resultados han generado una guía de las mejores prácticas a tomarse a consideración. A continuación, se describe algunas de ellas:

Un proyecto similar desarrollado en la Universidad Laica Eloy Alfaro de Manabí facultad de ciencias Informáticas, proyecto previo a la obtención del título de ingeniero en sistema, realizado por Acosta, N. (Jesus & Guadalupe, 2018) Que lleva por título "SOFTWARE DE ANALISIS DE RIESGO INFORMATICO APLICANDO MAGERIT Y NORMA ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMATICAS" esta investigación tiene como finalidad la realización de un análisis de riesgo con la metodología MAGERIT, y el desarrollo de un software que permita aplicar las metodologías de forma eficiente.

La presente investigación servirá como referencia para entender los conceptos de metodologías de análisis de riesgo, herramientas de análisis de riesgo, etc de manera más clara.

Un trabajo similar desarrollado en la Universidad Católica de Colombia en la facultada de Ingeniería, proyecto previo a la obtención del título de Ingeniero de Sistemas, realizado por Pascagaza, J. (GITIERREZ, 2018) que lleva por título "DESARROLLO DE UN SISTEMA DE INFORMACIÓN PARA LA GESTIÓN DE LOS PROYECTOS DE RESPONSABILIDAD SOCIAL DEL PROGRAMA DE INGENIERÍA DE SISTEMAS DE LA UNIVERSIDAD CATÓLICA DE COLOMBIA" el objetivo de esta investigación es el desarrollo de una herramienta Software para la gestión de proyectos.

Investigación que será utilizada como referencia para analizar las herramientas para el desarrollo de software, el ciclo y las metodologías de desarrollo de software.

J. METODOLOGÍA
el presente proyecto será descriptivo, debido a que se realizará una recolección de información de la metodología tanto para el desarrollo de software como para el análisis y gestión de riesgo, de la misma manera para la selección de la herramienta.

K. CRONOGRAMA DE ACTIVIDADES																								
N°	ACTIVIDAD	MES I				MES II				MES III				IV				V				MEDIOS DE VERIFICACIÓN
		S1	S2	S3	S4	S 1	S2	S 3	S 4	S1	S 2	S3	S4	S 1	S 2	S 3	S 4	S1	S 2	S 3	S4	
1	**Realizar un estudio teórico sobre los sistemas de gestión de riesgo, ISO 27000, herramientas y metodologías para desarrollo de software.**																					
1.1	Revisar información científica relacionada al tema en la Bases de Datos de la Institución.																					Lista de documentos de investigación almacenadas en Excel.
2	**Seleccionar de la metodología y herramienta para el desarrollo de software que se acople de mejor manera a la norma ISO 20701.**																					
2.1	Matriz Comparativa de las herramientas Software																					Hojas de Excel
2.2	Selección de la herramienta																					Documentación de resultados
2.3	Selección de la metodología																					Documentación de resultados
3	**Desarrollar el software de análisis y gestión de riesgo.**																					
3.1	Levantamiento de Requerimientos																					Documentación
3.2	Diseño de la base de datos																					
3.3	Conexión de la base de datos																					
3.4	Desarrollo del sistema.																					

L. DECLARACIÓN FINAL
Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES	
DIRECTOR:	Ing. Cristhian Flores Urgilés, MSC.
ESTUDIANTE 1	Juan Fernando Muñoz Muñoz

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	
Fecha:	
Firmas:	
Nombre: Ing. Cristhian Flores, MSC. CC: **Director del Proyecto**	Nombre: Fernando Muñoz Muñoz C.C.: **Estudiante / Egresado**

O. APROBACIÓN	
Firmas:	
Nombre: CC: **Primer Par Revisor**	Nombre: C.C.: 0302712310 **Segundo Par Revisor**

P. REFERENCIAS

[1] J. AREITIO BERTOLIN, Seguridad de la información. Redes, informática y sistemas de información, Madrid: Editorial Paraninfo, 2008.

[2] V. Rodrigo Raya, Gestión de Proyectos (GRADO SUPERIOR), Madrid: Grupo Editorial RA-MA, 2014.

[3] P. A. López, Seguridad Informatica, Editex, 2010.

[4] C. V. MIRANDA, Sistemas informáticos y redes locales, Madrid: Ediciones Paraninfo, S.A., 2005.

[5] A. L. Mesquia, A. Mas, E. Amengual y I. Cabestrero, «Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001,» *REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software,* p. 11, 2010.

[6] ISOTools Excellence, «Norma ISO 27002: El dominio política de seguridad,» 3 agosto 2017. [En línea]. Available: https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/. [Último acceso: 01 marzo 2021].

[7] E. M. Torres Nuñez, «repo.uta.edu.ec,» julio 2015. [En línea]. Available: http://repo.uta.edu.ec/bitstream/123456789/13057/1/Tesis_t1030si.pdf.

[8] K. G. Bermudez Molina y E. R. Bailon Sanchez, «Analisis en seguridad informatica y seguridad de la informacion basado en la norma ISO/IEC 27001-Sistemas de gestion de seguridad de la informacion dirigido a una empresa de servicios financieros,» 01 marzo 2015. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf.

[9] M. Campoverde-Molina y L. Valverde, «Accessibility analysis of the web portals of the educational institutions in Cuenca, Ecuador,» *Revista Cátedra,* vol. 2, nº 2, pp. 55-75, 2019.

[10] V. Simbaña-Gallardo y S. Luján-Mora, «Instructions about the manuscript structureof Revista Cátedra,» *Revista Cátedra,* vol. 1, nº 1, pp. 36-52, 2018.

[11] Universidad Católica de Cuenca, «Directrices para autores/as,» 2020. [En línea]. Available:https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/about/submissions.

UNIVERSIDAD CATÓLICA DE CUENCA

Anexo 2:

Universidad Católica de cuenca

Extensión Cañar

Octubre, 2021

Introducción

En el presente manual se explica de manera detallada y entendible cada uno de los módulos que corresponden a los diferentes menús que conforman el sistema de Análisis de riesgo y gestión de seguridad, describiendo cada uno de ellos paso a paso en cada pantalla desplegada según la opción seleccionada.

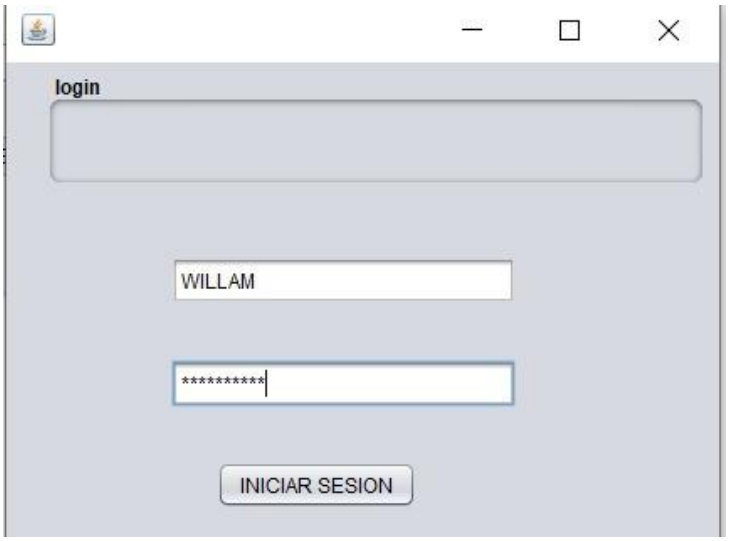
Este sistema busca facilitar el uso de la herramienta y una mejor productividad en el tiempo de ejecución en cuanto a la gestión de riesgo. El usuario solo tendrá que seguir las instrucciones plasmadas en el presente manual para resolver cualquier inconveniente que se le presente durante la ejecución del sistema.

Desarrollo

Se detalla las acciones y procesos a los cuales tendrá acceso el usuario.

Ingreso al sistema de gestión de seguridad

Desde el escritorio damos doble clic en el icono del sistema “Análisis de riesgo”. Al iniciar el sistema se presenta una ventana de identificación de usuario (Login) en el cual se debe ingresar el usuario y contraseña de acceso al sistema.



Haga clic en el botón iniciar sesión para ingresar al sistema.

Ventana de Inicio

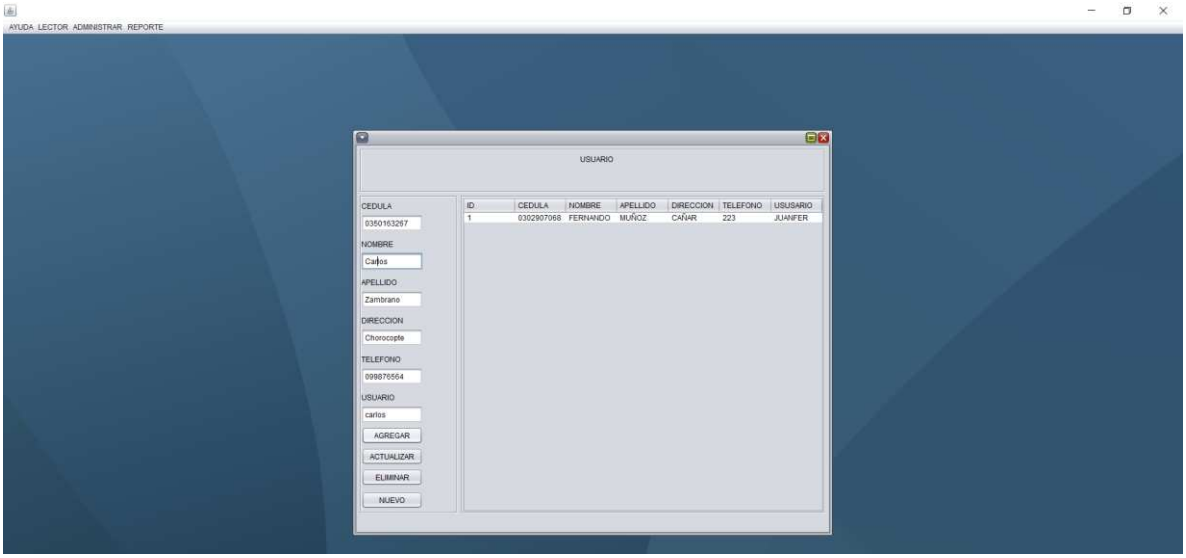
La ventana de inicio tiene como fin brindar al usuario una lista de opciones que le permitirá realizar una correcta gestión de riesgo.

En la parte superior izquierda se muestra el menú principal del sistema, siempre visible mientras esta en uso el software, se puede navegar entre diferentes opciones de acuerdo a lo que se desea hacer.

Ingresar Usuario

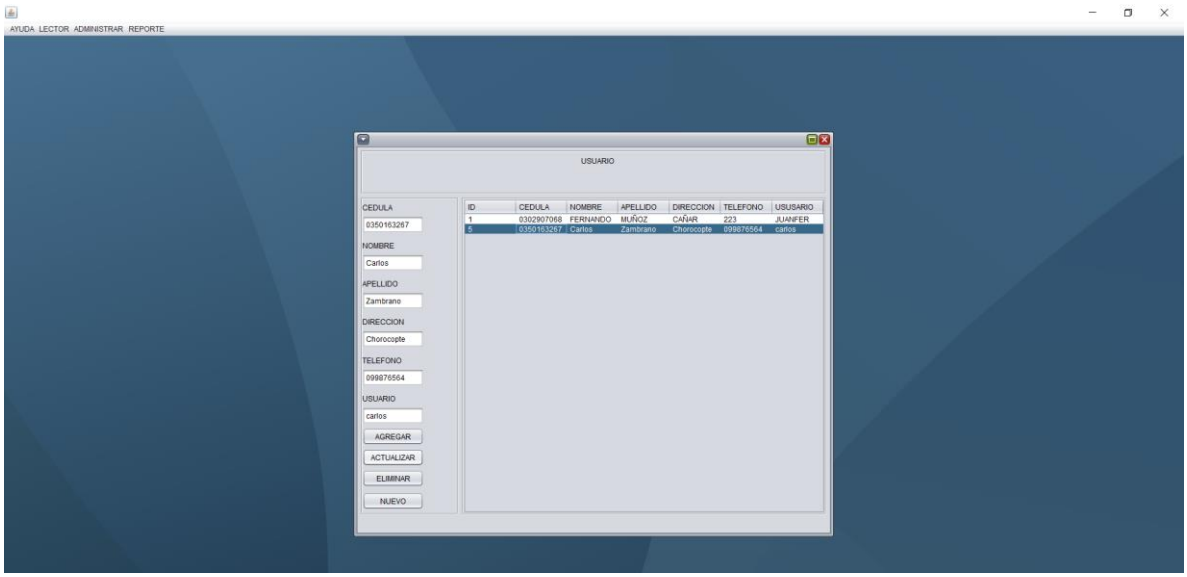
Para ingresar a un usuario hacemos clic en el botón “Usuario”.

Ingresamos los campos solicitados como son; Cedula, nombres, apellidos, dirección y teléfono, presionamos agregar, el usuario agregado se visualizará en la tabla posterior.



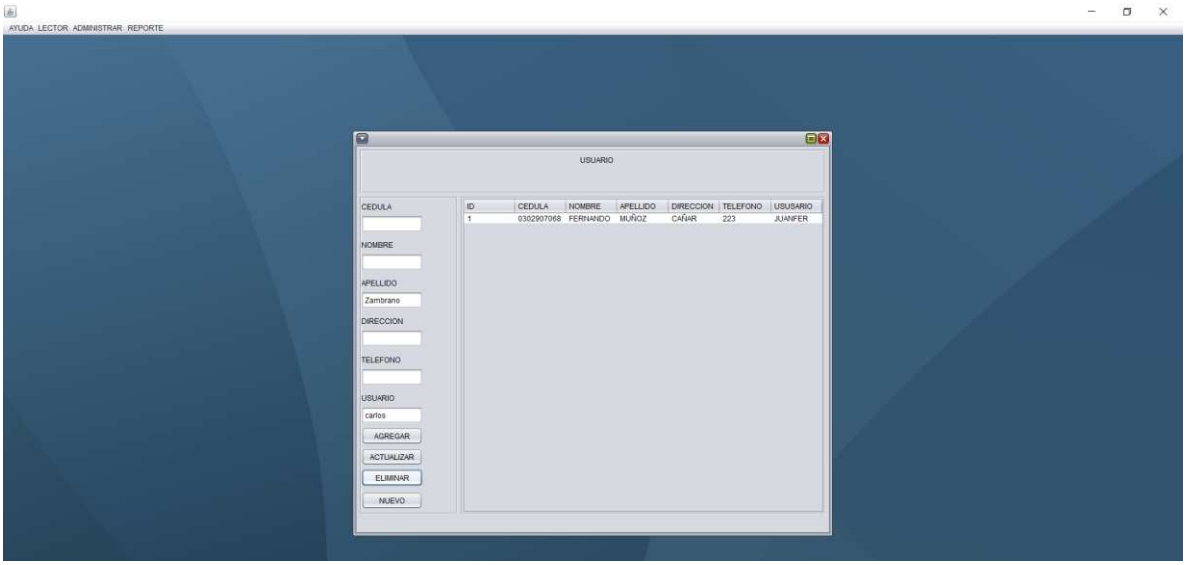
Actualización de usuario

Para la actualización de los usuarios ingresados, presionamos doble clic en el usuario que se desea actualizar datos, inmediatamente se colocaran los datos en los campos correspondientes, realice la modificación requerida y presione actualizar.



Eliminar Usuario

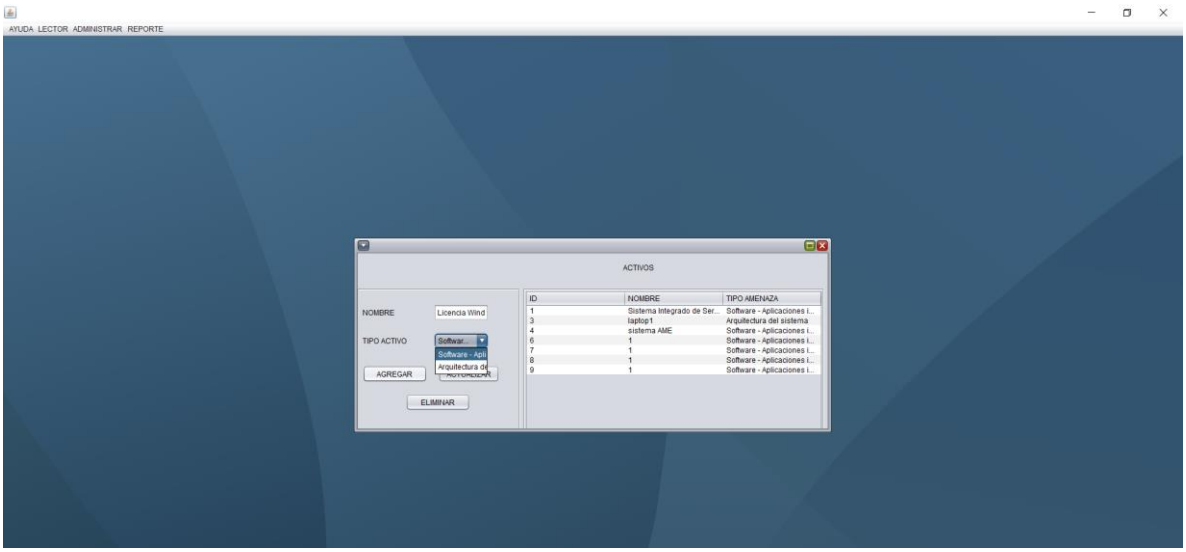
Para la eliminación de la base de datos seleccione el usuario que desea retirar y presione clic en eliminar.



Ingresar Activos

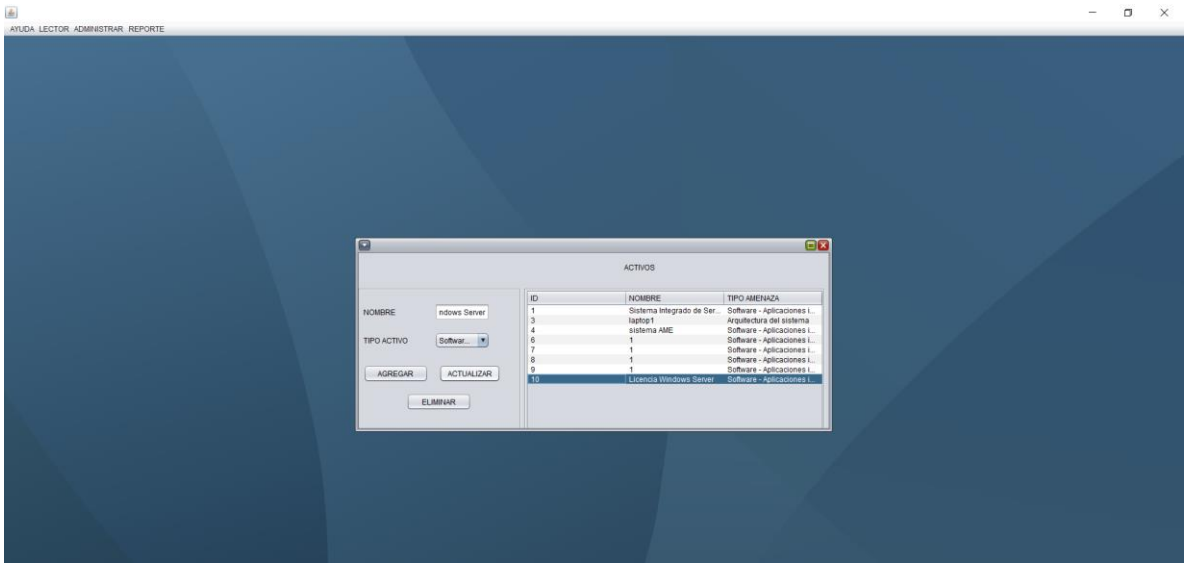
Para el ingreso de activos presionamos clic en el botón “Activos”

Ingresamos los campos solicitados, ID, Nombre del activo, y el tipo de amenaza a la que pertenece dicho activo, presionamos **agregar.**



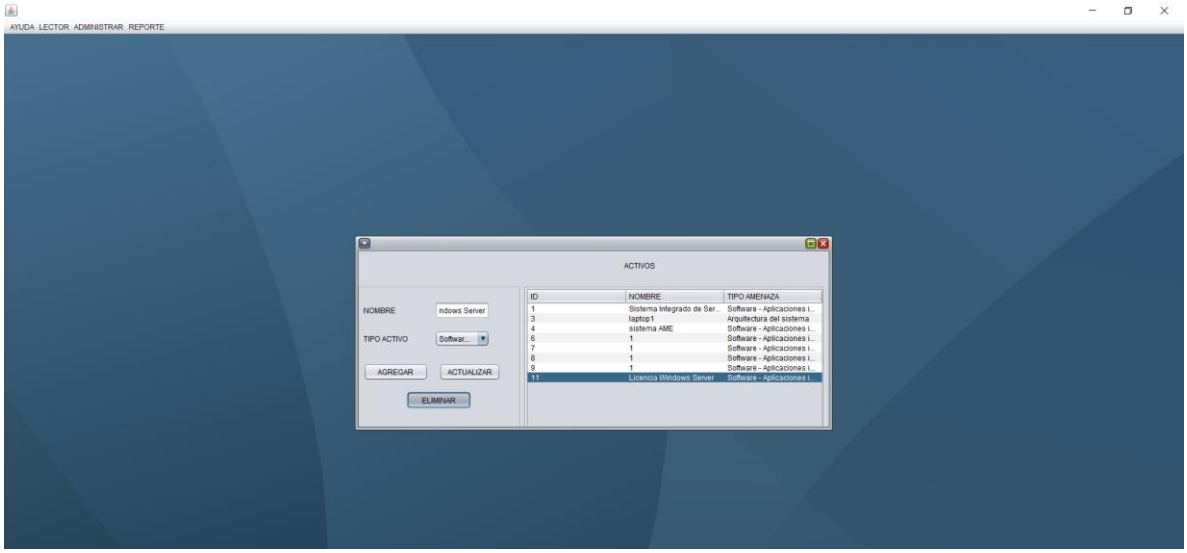
Actualización de Activo

Para la actualización de los Activos ingresados, presionamos doble clic en el activo que se desea actualizar la información, inmediatamente se colocaran los datos en los campos correspondientes, realice la modificación requerida y presione actualizar.



Eliminación de Activo

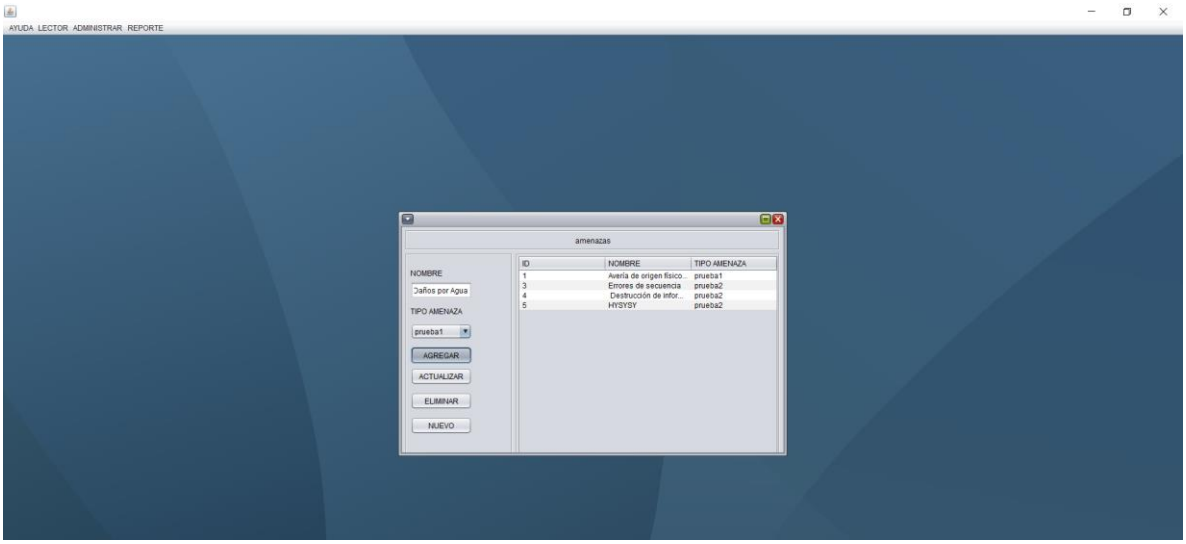
Para la eliminación de la base de datos seleccione el Activo que desea retirar y presione clic en eliminar.



Agregar Amenazas

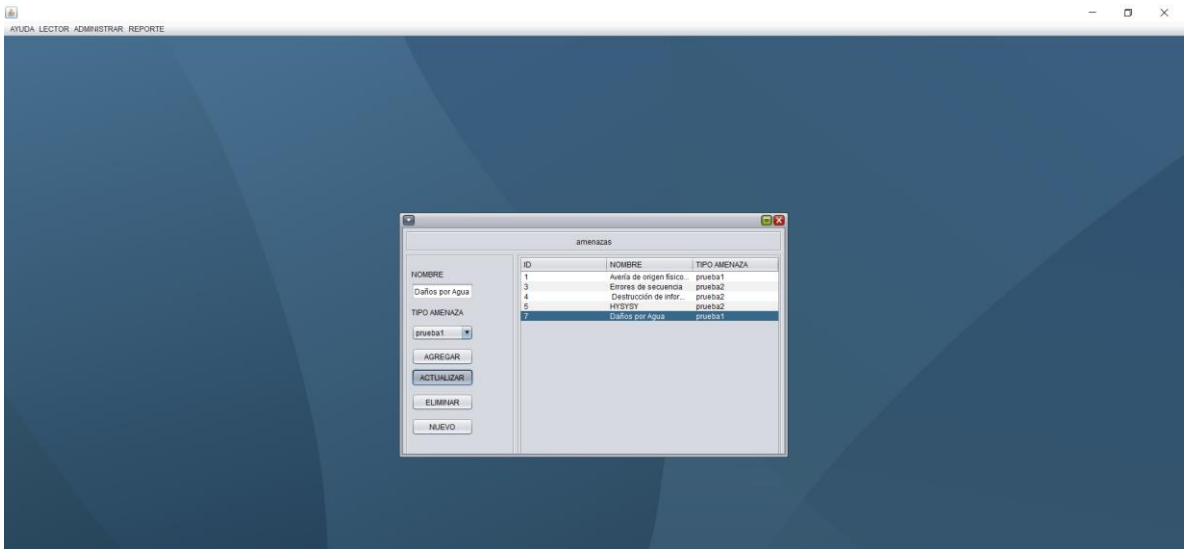
Para el ingreso de amenazas presionamos clic en el botón “Amenaza”

Ingresamos los campos solicitados, Nombre de la amenaza, seleccione el tipo de amenaza y presionamos **agregar.**



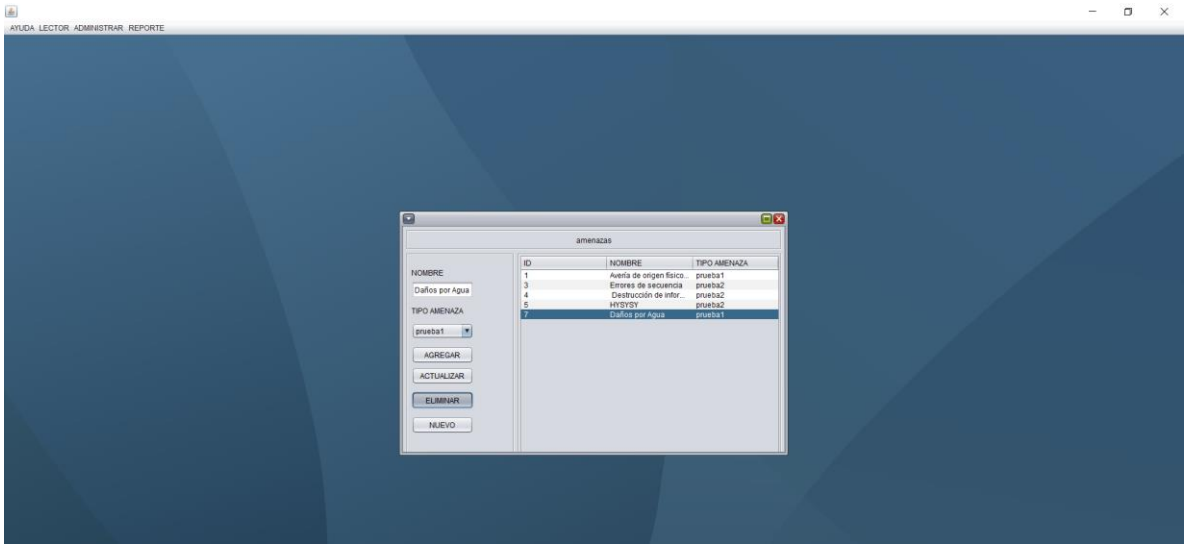
Actualización de Amenaza

Para la actualización de las amenazas ingresadas, presionamos doble clic en la amenaza que se desea actualizar la información, inmediatamente se colocaran los datos en los campos correspondientes, realice la modificación requerida y presione actualizar.



Eliminación de amenaza

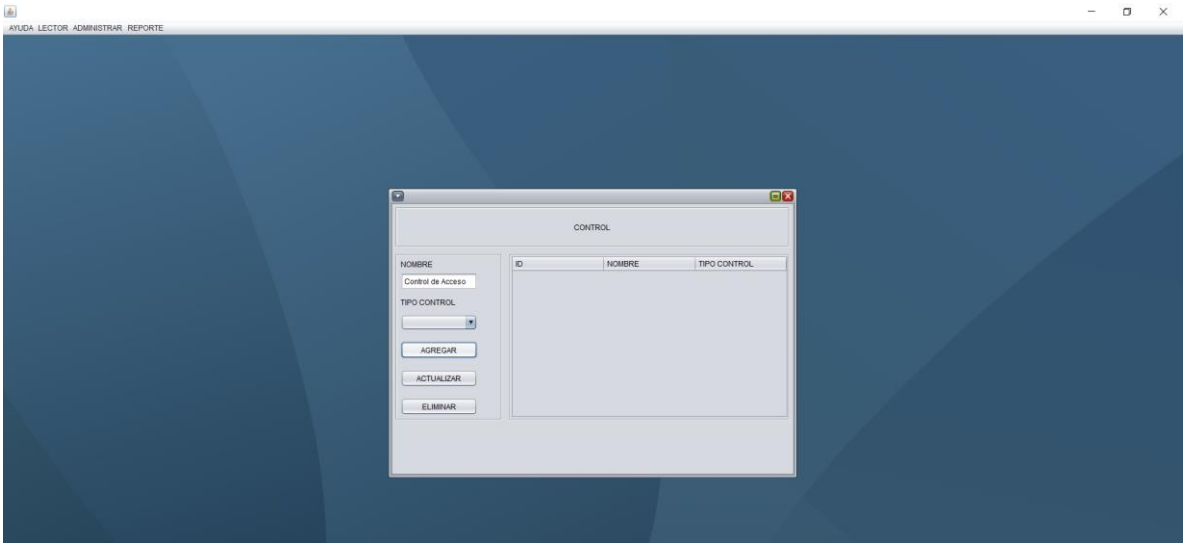
Para la eliminación de la base de datos seleccione la amenaza que desea retirar y presione clic en eliminar.



Ingreso de Control

Para el ingreso de los controles presionamos clic en el botón “Control”

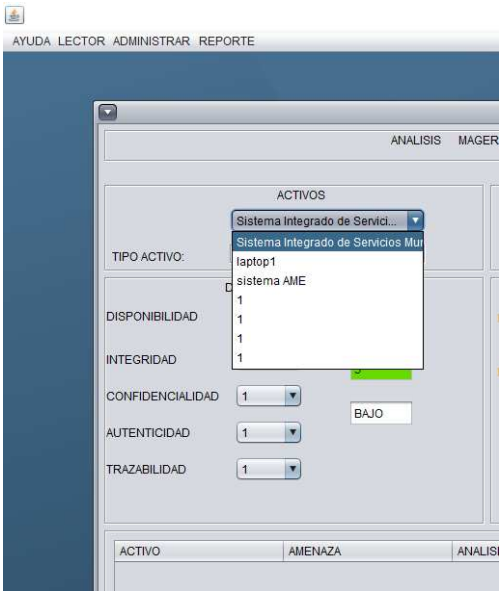
Ingresamos los campos solicitados, Nombre del control, cabe recalcar que los controles a ser ingresados serán basados en la norma ISO 27001, seleccione el tipo de control y presione **agregar.**



Análisis y gestión de riesgo

Para realizar el análisis de riesgo, presione clic en el botón administrar y seleccione análisis.

Una vez dentro de la ventana análisis de riesgo seleccionamos el activo al que se va a realizar la respectiva calificación, una vez seleccionada se cargará de manera automática el tipo de activo.



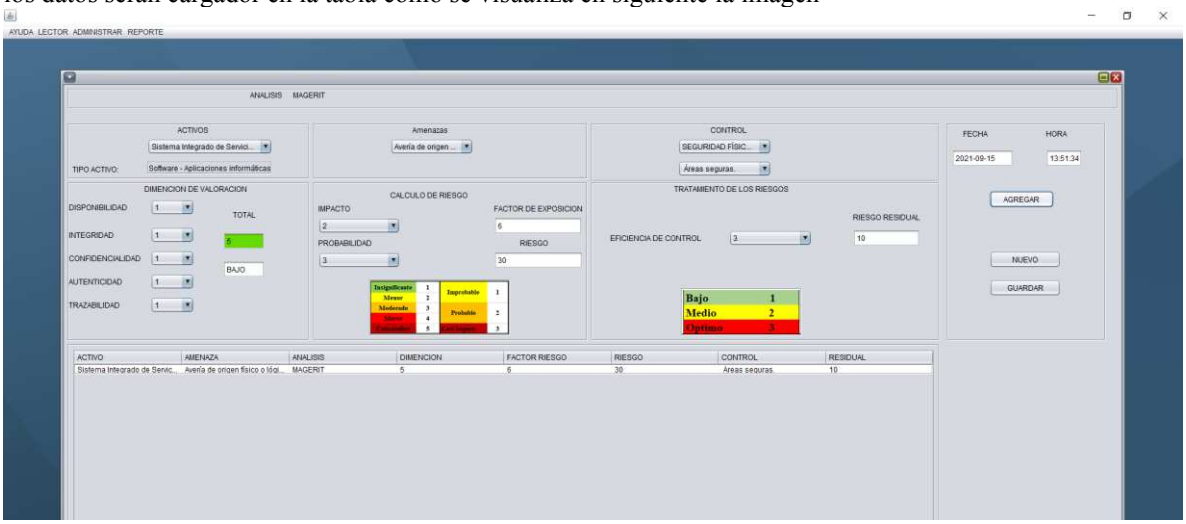
Una vez determinado el activo proceda la calificación para ello nos dirigimos a la parte de dimensión de valoración y seleccionamos el valor a ser otorgado tanto para integridad, confidencialidad, autenticidad, trazabilidad, se obtendrá el total de la calificación del activo.

Obtenida la calificación del activo, procede con la selección de la amenaza , para ello hace clic en la parte inferior donde dice amenaza y seleccionamos de la lista.

Para le calculo del impacto y la probabilidad nos dirigimos a la parte donde dice calculo del riesgo seleccionamos un valor de la lista y automáticamente se carga los campos en blanco de factor de exposición y el nivel de riesgo.

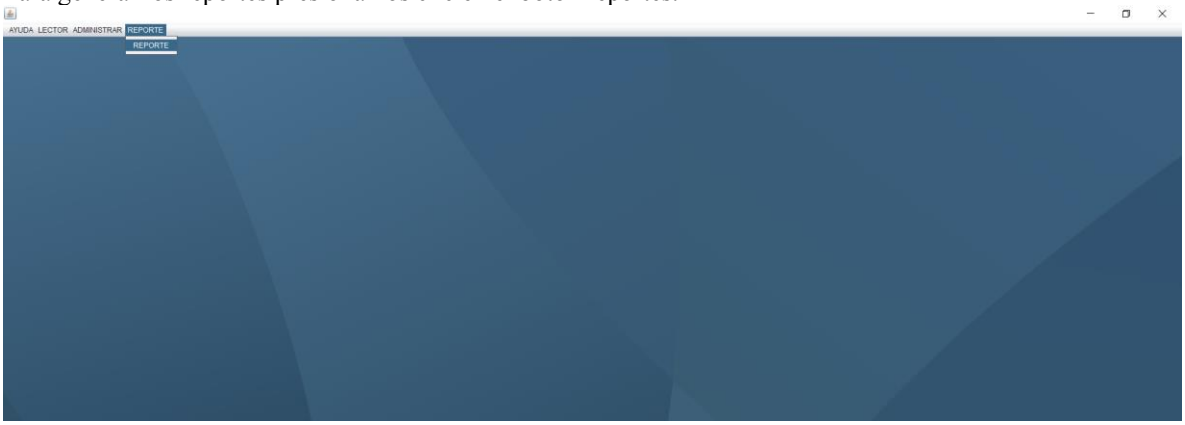
Obtenida el nivel de riesgo, algunos de ellos requiere la implantación de controles para mitigar los mismo, para ello seleccionamos el control, para la eficiencia del control nos dirigimos a la parte de eficiencia y seleccionamos el valor , el cual calculará el riego residual.

Una vez llenada todo los campos, proceda a guardar los cambios, para ello presione clic en el botón agregar, los datos serán cargador en la tabla como se visualiza en siguiente la imagen



Reportes

Para generar los reportes presionamos clic en el botón reportes.

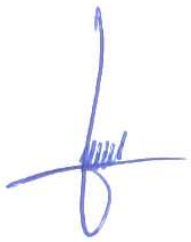


Nos dirigirá a la siguiente ventana, donde se visualizará todos los análisis realizados en el sistema.

UNIVERSIDAD CATÓLICA DE CUENCA

Juan Fernando Muñoz Muñoz portador(a) de la cédula de ciudadanía Nº 0320712310. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación "DESARROLLO DE SOFTWARE DE ANÁLISIS DE RIESGOS Y GESTIÓN DE SEGURIDAD BASADO EN ISO 27001." de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, 15 de octubre de 2021



F: ……..

Juan Fernando Muñoz Muñoz

C.I. 0302712310