Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Software

Desarrollo de una aplicación web y móvil para la gestión de riesgos de seguridad de la información aplicado a una empresa de consultoría de sistemas

TESIS

Para optar el Título Profesional de Ingeniero de Software

AUTOR

Rosel Miguel CASTILLO ROMERO

ASESOR

Dra. Luzmila Elisa PRÓ CONCEPCIÓN

Lima, Perú

2022

Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Castillo, R. (2022). *Desarrollo de una aplicación web y móvil para la gestión de riesgos de seguridad de la información aplicado a una empresa de consultoría de sistemas*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Software]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Rosel Miguel Castillo Romero
Tipo de documento de identidad	DNI
Número de documento de identidad	47230198
URL de ORCID	https://orcid.org/0000-0002-2303-7821
Datos de asesor	
Nombres y apellidos	Luzmila Elisa Pró Concepción
Tipo de documento de identidad	DNI
Número de documento de identidad	08862360
URL de ORCID	https://orcid.org/0000-0003-0622-1173
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Lenis Rossi Wong Portillo
Tipo de documento	DNI
Número de documento de identidad	10438282
Miembro del jurado 1	
Nombres y apellidos	Hugo Rafael Cordero Sánchez
Tipo de documento	DNI
Número de documento de identidad	40512428
Miembro del jurado 2	
Nombres y apellidos	Luzmila Elisa Pró Concepción
Tipo de documento	DNI
Número de documento de identidad	08862360
Datos de investigación	
Línea de investigación	C.0.3.22. Ingeniería de Software
Grupo de investigación	No aplica

Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	Universidad Nacional Mayor de San Marcos País: Perú Departamento: Lima Provincia: Lima Distrito: Cercado de Lima Latitud: -12.053149, Longitud: -77.085572
Año o rango de años en que se realizó la investigación	Noviembre 2019 – Mayo 2022
URL de disciplinas OCDE	Otras ingenierías y tecnologías https://purl.org/pe-repo/ocde/ford#2.11.02

Universidad Nacional Mayor de San Marcos

Universidad del Perú, DECANA DE AMÉRICA

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Software

Acta de Sustentación Virtual de Tesis

Siendo las veinte (20) horas del día cinco (05) del mes de mayo de 2022, se reunieron en la sala virtual meet.google.com/tiw-vttk-ijf, presidido por la Dra. Lenis Rossi Wong Portillo, Ing. Hugo Rafael Cordero Sánchez (Miembro) y la Dra. Luzmila Elisa Pró Concepción (Miembro Asesor), para la sustentación virtual de la Tesis intitulado ***"DESARROLLO DE UNA APLICACIÓN WEB Y MÓVIL PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN APLICADO A UNA EMPRESA DE CONSULTORÍA DE SISTEMAS"****, por el Bachiller* ***Rosel Miguel Castillo Romero,*** *para optar el Título Profesional de Ingeniero de Software.*

Acto seguido de la exposición de la Tesis, la Presidenta invitó al bachiller a dar respuesta a las preguntas establecidas por los Miembros de Jurado.

El bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros de Jurado, el bachiller obtuvo la nota de 17 (diecisiete).

A continuación, la Presidenta del Jurado, Dra. Lenis Rossi Wong Portillo, declara al bachiller ***Ingeniero de Software****.*

Siendo las 20:59 horas, se levantó la sesión.

Dra. Lenis Rossi Wong Portillo
Presidenta

Ing. Hugo Rafael Cordero Sánchez
Miembro

Dra. Luzmila Elisa Pró Concepción
Miembro Asesor

.

Dedicatoria:
La presente investigación esta dedicada a mis padres, Frida y Carlos, a quienes estaré agradecido por todo el apoyo incondicional y la motivación continua. A la memoria de mis abuelos.

Agradecimientos

Agradezco a Dios sobre todas las cosas por la fortaleza de continuar sobre todas las adversidades.

Agradezco a la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos por la oportunidad de haber estudiado dentro de sus prestigiosas aulas. También a mis profesores que fueron parte de mi formación académica en todos los años de estudio.

A mi asesora Luzmila Pro por su tiempo, dedicación y paciencia en la orientación, guía, revisión y apoyo del presente trabajo de investigación

A mis amigos, compañeros de trabajo quienes aportaron con ideas y sugerencias sobre el trabajo de investigación.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SOFTWARE

Desarrollo de una Aplicación Web y Móvil para la Gestión de Riesgos de Seguridad de la Información aplicado a una Empresa de Consultoría de Sistemas

Autor: Rosel Miguel Castillo Romero.
Asesor: Dra. Luzmila Elisa Pró Concepción
Fecha: Julio 2021

RESUMEN

La presente investigación tiene como objetivo principal desarrollar una aplicación web y móvil para la gestión de riesgos de seguridad de la información de acuerdo a una metodología adecuada en el marco de la norma NTP -ISO 27001 para el sector empresarial de consultoría de sistemas. En la investigación se propone gestionar y salvaguardar los activos de información de una empresa frente a riesgos de perdida, divulgación, indisponibilidad o alteración. Para lo cual, se realizó una investigación sobre las metodologías existentes y estándares de calidad internacionales referentes a la gestión de seguridad de la información, seleccionando la metodología MAGERIT y teniendo en cuenta las normativas ISO, luego se procedió a desarrollar la aplicación web y móvil para la gestión de riesgos de seguridad de la información. Para el desarrollo de las aplicaciones se realizó mediante metodología ágil de desarrollo de software, respetando los procesos de aseguramiento de calidad en el software, los cuales se detallan junto a los aspectos técnicos y funcionales en la presente investigación. Luego del desarrollo de las aplicaciones se realizó el despliegue de la propuesta en una empresa Consultora de Sistemas, se estableció políticas y actividades a evaluar en los riesgos de la información, para ello se tomó como prueba piloto la implementación de las aplicaciones planteadas en la consultora de sistemas. Se evaluó el sistema propuesto INFORISK mediante encuestas a usuarios y obtuvo unas calificaciones aceptables que lo respaldan, cumpliendo así con el objetivo del estudio.

Palabra claves: Seguridad de la información, Metodología de seguridad de la información, ISO 27001, Gestión de riesgos, Metodología MAGERIT, Aplicación web y móvil.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SOFTWARE

Desarrollo de una Aplicación Web y Móvil para la Gestión de Riesgos de Seguridad de la Información aplicado a una Empresa de Consultoría de Sistemas

Autor: Rosel Miguel Castillo Romero.
Asesor: Dra. Luzmila Elisa Pró Concepción
Fecha: Julio 2021

ABSTRACT

The objective of this research is to develop a web and mobile application for information security risk management according to an adequate methodology within the framework of the NTP -ISO 27001 standard aimed at the business sector of systems consulting. The research aims to manage and safeguard the information assets of a company against risks of loss, disclosure, unavailability or alteration. For which, an investigation was carried out on the existing methodologies and international standards regarding information security management, selecting the MAGERIT methodology and taking into account the ISO regulations, then proceeded to develop a web and mobile application for information security risk management. For the development of the applications, it was carried out through agile software development methodology, respecting the quality assurance processes in the software, which are detailed together with the technical and functional aspects in this research. After the development of the applications, the proposal was deployed in a Systems Consulting company, policies and information risk assessment activities were established, for which the implementation of the applications proposed in the systems consultant. The proposed INFORISK system was evaluated through user surveys and obtained acceptable supporting scores, thus fulfilling the proposed primary objective of the research.

Key Words: Information security, Information security methodology, ISO 27001, Risk management, MAGERIT methodology, Web and mobile application.

ÍNDICE

Lista de Tablas

Lista de figuras

CAPITULO I

INTRODUCCIÓN

En este capítulo se detallará el contexto situacional que determinó la elección del tema de la investigación luego de la recopilación de datos, noticias y reportes de ciberseguridad acerca de la relevancia e importancia de la seguridad de la información en la actualidad, así como la problemática encontrada. También se define el alcance y los objetivos que se desarrollaran en la tesis.

1.1 Antecedentes del problema

Actualmente los diversos sistemas de información, incluyendo tanto hardware como software, los datos y la información son los activos más valiosos que puede tener las empresas y organizaciones. Distintos investigadores y ejecutivos concuerdan que el activo más valioso a proteger para las organizaciones es la información. Najar (2015) en su artículo “Information Security: A Valuable Asset of the Organization”, concluye que el activo más valioso e importante de las organizaciones es la información, y debido a esto requiere especial protección e inversión; y todo lo que se haga proteger la información en las organizaciones será muy importante; Sin embargo, se debe reconocer que la información siempre estará amenazada y que personas ajenas a las organizaciones podrían aprovechar vulnerabilidades de los sistemas.

La información de las empresas no solo se considera como un activo más de la organización, sino que es también un activo estratégico. Así lo menciona Zúñiga (2015) en su artículo “La información como activo estratégico en la administración de la PYME” -publicado por la Red de Investigadores en Competitividad - donde el autor demuestra, mediante pruebas descriptivas y estadísticas, que la información que resulta de la administración se toma en cuenta como un activo estratégico para mejorar la

competitividad de la PYME. Aquí radica la importancia y el medio en el cual se guarda esta información y el gran impacto que tendría en la PYME en caso de ser la información alterada, robada o extraviada.

El impacto de los datos y la información en el ambiente empresarial se puede entender con un estudio publicado por la consultora PwC, en donde se presenta en un ranking a las compañías con un mayor crecimiento de capitalización bursátil del último lustro. Dentro del top 10 se encuentran compañías (como Apple y Amazon) que afirman y consideran el dato como un activo estratégico, y a partir allí, construyen su modelo de negocio referente a este para poder ofrecer productos y servicios de mayor valor añadido. En los últimos años en las grandes compañías se viene creando un nuevo puesto ejecutivo, el de Chief Data Officer (CDO), quien se encargaría de gestionar los datos e información y convertirlos en un activo estratégico para las compañías. Según San Martin (2017) afirma que las empresas que logren considerar y posicionar al dato como un activo estratégico, serán las que tengan más oportunidad de prosperidad y desarrollo en los siguientes años, además que será uno de los factores clave en su ventaja competitiva.

Como se ha evidenciado, la información y los activos de información de las organizaciones son esencialmente importantes, así que protegerlos y gestionarlos de manera adecuada debería ser vital para cualquier organización.

Las noticias sobre ataques cibernéticos, robos de activos de la información, suplantación de identidad digital, virus, hackers aumenta año a año en las organizaciones, de las cuales las más susceptibles son aquellas con poca o ningún sistemas de gestión de seguridad de la información. La compañía tecnológica IBM publica sus investigaciones en “IBM X-Force Threat Intelligence Índex”, donde resume los resultados de las

amenazas en seguridad de la información más importantes año a año, en la publicación actual (2019) tenemos los sectores de la industria que más han sufrido ataques, robos y perdidas de información en el año 2018.

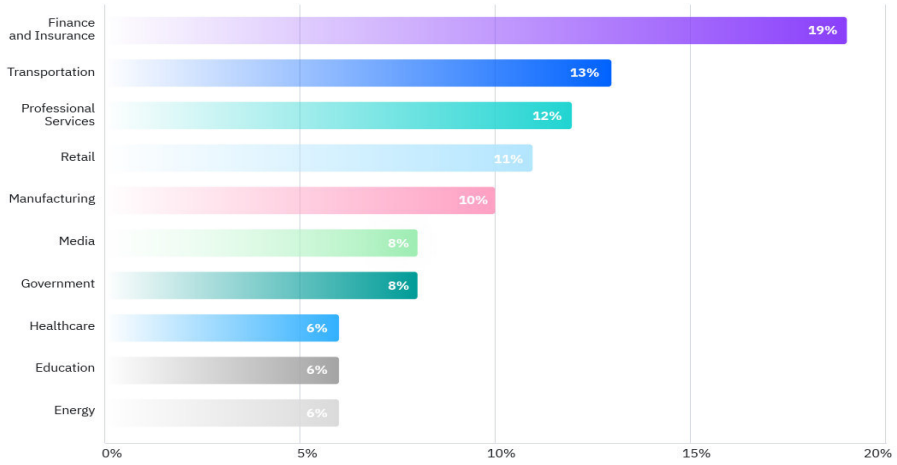

Figura 1.1 Sectores de Industria atacados con mayor frecuencia. Extraído de: "X-Force Threat Intelligence Index.", por IBM, 2019

Como se observa en figura 1.1 el sector de servicios profesionales, donde se incluyen las consultorías, se ha incrementado el riesgo de ciberataques y amenazas, por lo tanto, sería necesario una gestión adecuada de sus activos de información a fin de proteger las compañías. En la figura 1.2 se observa el tamaño de información que ha sido filtrada o robada a empresas en los últimos 3 años, mientras más grande el circulo, más grande el impacto y costo económico que ocasiono, cabe mencionar que en su mayoría los registros son de texto plano vulnerados por un factor de error humano (43%) más que por seguridad o políticas de sistemas de seguridad, esto también hace hincapié en la

importancia de comprometer y capacitar a los trabajadores ya que son la principal vulnerabilidad frente a ataques externos o internos.

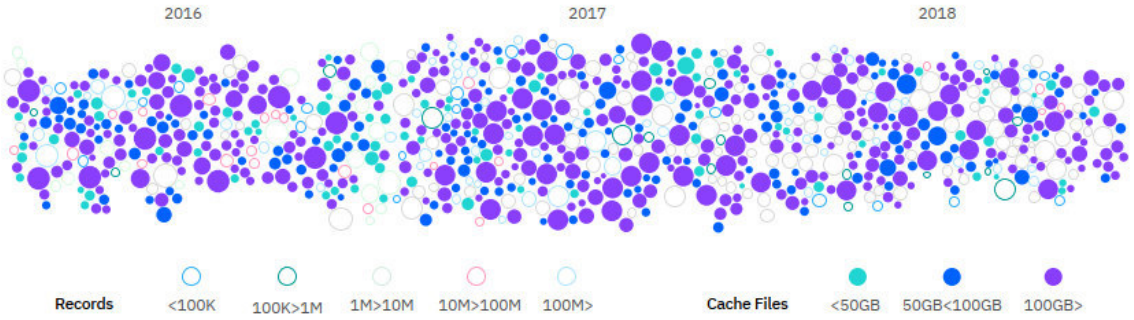

Figura 1.2. Muestreo de los incidentes de seguridad de impacto por registros de archivos. Extraído de: "X-Force Threat Intelligence Index.", por IBM, 2019

Activos de información más valiosos.

Los activos que más quieren proteger las organizaciones es la información personal del cliente, la financiera y los planes estratégicos. En la figura 1.3 se visualiza un gráfico estadístico de la empresa consultora EY sobre un estudio de Encuesta global de Seguridad (2018-2019), donde se muestra en porcentajes el tipo de información más valiosa a cuidar por las organizaciones y las principales amenazas cibernéticas encontradas en los últimos 2 años.

Los 10 tipos de información más valiosos para los crímenes cibernéticos	Las 10 mayores amenazas cibernéticas para las organizaciones
1. Información del cliente (17%)	1. *Phishing* (22%)
2. Información financiera (12%)	2. *Malware* (20%)
3. Planes estratégicos (12%)	3. Ataques cibernéticos (para interrumpir operaciones) (13%)
4. Información del Consejo (11%)	4. Ataques cibernéticos (para robar dinero) (12%)
5. Contraseñas del cliente (11%)	5. Fraude (10%)
6. Información de I&D (9%)	6. Ataques cibernéticos (para robar IP) (8%)
7. Información de fusiones y adquisiciones (8%)	7. *Spam* (6%)
8. Propiedad intelectual (6%)	8. Ataques internos (5%)
9. IP no patentada (5%)	9. Desastres naturales (2%)
10. Información de proveedores (5%)	10. Espionaje (2%)

Figura 1.3. Información más valiosa y principales amenazas en las Organizaciones. Extraído de: "Encuesta Global de Seguridad", por EY, 2019

Asimismo, se vuelve a mencionar la principal vulnerabilidad sobre la exposición de riesgos de la seguridad de la información, esta vez la consultora EY, al igual que anteriormente se mencionó en el reporte de IBM. EL factor humano es el principal objeto vulnerable para filtrar o robar información valiosa como se muestra a continuación figura 1.4.

Figura 1.4. Vulnerabilidades con mayor riesgo. Extraído de: "Encuesta Global de Seguridad", por EY, 2019

La necesidad de la implementación de un sistema de seguridad de información se origina en base a las amenazas internas y externas que aprovechan vulnerabilidades para el robo, filtrado de información, a continuación, se detalla en la tabla 1.1 algunos datos referentes a la seguridad de información en los últimos 3 años, también se referencia la empresa que realizo el estudio.

Tabla 1.1. Estadísticas sobre seguridad de la información en Empresas. Fuente: Elaboración propia.

Estadísticas	Organización - Fuente
Al menos un 70% en las Empresas estiman que el riesgo en el	Cyber Security Risk

ámbito de su seguridad informática creció en periodo de 2016-2018	Report, 2019. Ponemon Institute
Los pequeños negocios representan el 43% de los ciberataques dentro del estudio	Intenet Security Threat Report, 2018. Small Business Trends
El tiempo de detección de alguna brecha de seguridad en los sistemas de las compañías es de un promedio de 6 meses	ZD Net
La pérdida de los datos de las organizaciones representa el 43% de los costos cuando son afectadas por ataques de ciberdelincuentes.	Accenture's Report, 2018
Ataques más utilizados por los ciberdelincuentes son los ataques a malwares y basados en la web.	Accenture's Report, 2018
75% de las organizaciones infectadas por rasomware tenían protección activa	Informe de Transparencia, 2019. Sophos
En un 56%, el phishing es el mayor riesgo de seguridad informática al que temen las organizaciones.	Encuesta sobre Seguridad Informática a profesionales de TI, 2018. CyberArk
En 2017, Equimax fue susceptible a una brecha de seguridad, la cual le terminó costando más de $4 billones a la organización	Reporte CyberSeguidada,2017. Time

En el ámbito nacional, según Ricchi, socia de PriceWaterhouseCoppers (PwC) en una entrevista para el diario Gestión declara que: "Desde el punto de vista de procedimientos, la empresa peruana está muy inmadura en lo que es la gestión de manejo de la información y no presenta una estrategia de seguridad corporativa". Una gran cantidad de delitos informáticos no están siendo reportados porque las empresas no los están registrando debido a la falta protocolos y estrategias para identificar y cuantificar la

perdida ocasionada por algún delito informático. En informes de Panda Security concluye que los ataques a nivel global se concentran hasta en un 43% a PyMES debido a sus pocas medidas en seguridad; según el informe de IT Security Risks Report(2017) señala que en la región menos del 36% de PYMES cuenta con medidas preventivas para evitar el mal comportamiento de su personal, conducta que pudiese generar un ciberataque con pérdida o filtrado de información sensible.

Ante las constantes amenazas de seguridad, ciberataques, fraudes informáticos y robo de información; actualmente se ha vuelto cada vez más relevante la seguridad de la información que manejan las empresas, tanto para proteger sus propios recursos y activos, como para proteger información confidencial de sus clientes. Según la normativa ISO 27001, los 3 pilares fundamentales a tener en cuenta son la disponibilidad de los datos, la confidencialidad de los documentos y la integridad de la información; y mediante la gestión de riesgos de seguridad de la información se enfoca en proteger cada uno de estos pilares fundamentales para cada activo de información.

En las conclusiones y recomendaciones del Reporte Anual de Ciberseguridad de Cisco (2018), identifican la importancia de realizar análisis profundos y avanzados de posibles filtros de información, también revisar procedimientos de respuesta frente a ataques o perdidas de información y de continuidad del negocio, así como el resguardo a activos de información. Esto obedece a algunos procedimientos de la gestión de riesgo en seguridad de la información.

Debido a esto se aplica metodologías y técnicas para salvaguardar los activos de información. Un medio clave para minimizar estos incidentes y ataques es la gestión de riesgos de seguridad de la información.

1.2 Definición del problema

¿Cómo gestionar y salva guardar eficientemente los activos de información de una empresa consultora de sistemas frente a riesgos de pérdida, divulgación, indisponibilidad o alteración?

1.3 Importancia del problema

Los incidentes y ataques a los activos de información de las empresas son recurrentes, por lo que la pérdida o divulgación de los mismos pueden llegar a afectar en aspectos económicos, legales o de imagen a la cualquier empresa.

Dentro del caso evaluado, se identificó los siguientes problemas dentro de la empresa, en torno a la seguridad de la información

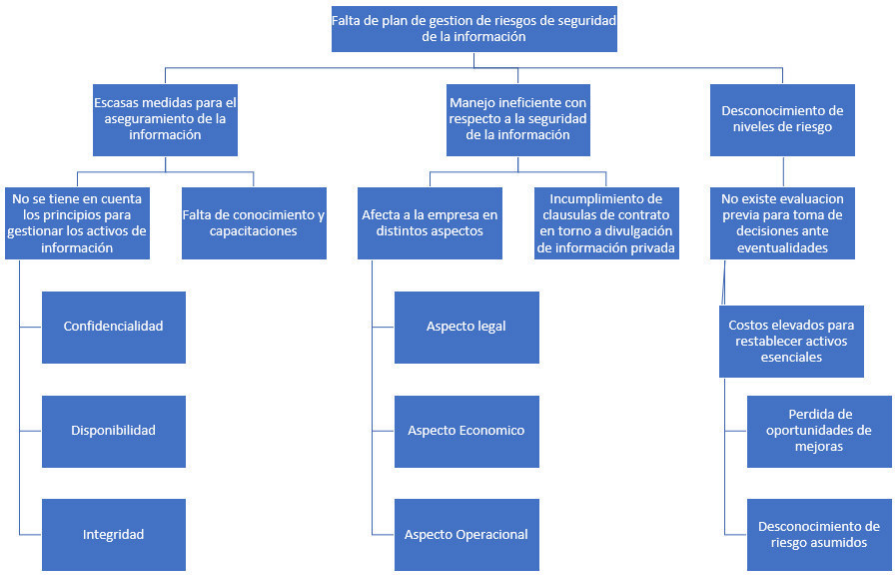

Figura 1.5. Problemáticas identificadas en la Consultora de Sistemas. Elaboración Propia

1.4 Objetivos

1.4.1 Objetivo General

Desarrollar una aplicación web y móvil para la Gestión de Riesgos de Seguridad de la Información de acuerdo con una metodología adecuada para el sector empresarial de consultoría de sistemas.

1.4.2 Objetivos Específicos

- Seleccionar una metodología adecuada luego de analizar comparativamente las ya existentes
- Modelar el uso de la metodología de gestión de riesgos en el tipo de empresa seleccionada
- Desarrollar una propuesta de una aplicación web y móvil.
- Planificar el desarrollo, implementación y despliegue de la propuesta tecnológica en la empresa seleccionada.
- Establecer políticas y procesos de evaluación de riesgos de seguridad de la información de acuerdo al modelo seleccionado de gestión de riesgos de la información y aplicado a la empresa de consultoría de sistemas.

1.5 Justificación

1.5.1 Justificación Teórica

En el desarrollo e implementación del modelo, se va a contribuir con el conocimiento sobre el uso de buenas prácticas y estándares de calidad para la gestión de riesgo de seguridad de la información en el sector de consultorías de sistemas para ante cualquier eventualidad se tenga mapeado de manera formal las acciones para proteger los activos de información y también saber el nivel de exposición al riesgo en el que nos encontramos.

1.5.2 Justificación Práctica

En la experiencia propia se ha identificado continuos problemas de falta de seguridad de información en empresas de consultorías de sistemas, por esta causa existe la necesidad

de desarrollar la gestión de riesgos, y que sea aplicada de manera correcta, rápida y segura a fin de salvaguardar los activos de la empresa.

1.7 Alcance

Esta investigación se desarrolla para una empresa del rubro de consultoría de tipo PYME, por lo tanto, el alcance del desarrollo se ve ajustado por factores limitantes tanto económicos como de recursos humanos. Bajo este criterio se tendrá en cuenta recurrir a un desarrollo ágil, rápido y optimizando los recursos necesarios.

CAPITULO II

MARCO TEÓRICO

El objetivo de este capítulo es realizar una revisión exhaustiva de la literatura disponible, tanto en la región como a nivel mundial, y plantear los lineamientos teóricos referentes a la Gestión de riesgos de seguridad de la información.

2.1 Activos de Información

Según la norma ISO/IEC 27001(International Organization for Standardization / International Electrotechnical Commission), nos menciona que un activo de información es aquello que es protegido por las organizaciones debido a que lo considera de gran valor. La administración y gestión de los activos de información involucra el diseñar, establecer e implementar de los diversos procesos que convoquen a la identificación, clasificación, valoración y el tratamiento de los activos de información más relevantes del negocio.

Según el Instituto Colombiano de Normas Técnicas (ICNTC), el activo de información se puede definir como cualquier elemento de hardware o software con tareas de procesamiento, almacenamiento, procesos, bases de datos asociados siempre con el manejo de datos y de la información específica gestionada por cada organización o entidad.

En este sentido, estos elementos hacen referencia a la información que se recibe, transforma y produce en la entidad u organización.

Valoración de los Activos:

Cada activo tiene sus propias características o estados. En la mayoría de las metodologías encontramos 3 características, pero en otras como MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) se puede encontrar hasta cinco.

- Confidencialidad: Previene la divulgación no autorizada de los activos de información. En casos de información de personas físicas se relaciona con la Ley Peruana de Protección de Datos Personales (Ley 29733).
- Integridad: Vela por salvaguardar el contenido del activo, de manera que la información se mantenga fiel y completa. En algunos activos un daño o alteración menor los haría completamente inútiles. por ejemplo, alterar o borrar archivos parte un software, lo volvería afuncional.
- Disponibilidad: Habilita el activo a la persona correcta en el momento y lugar adecuados para su uso y necesidad. También se asocia a la fiabilidad técnica de todos sus componentes.
- Autenticidad: Identifica a los actores con la autorización necesaria para visualizar, editar o eliminar la información, y sea el actor quien tenga que ser en el momento correcto.
- Trazabilidad: Se refiere al completo control referente al uso que se le da a los activos, implica también el quien y el cuándo, para así asegurar la calidad.

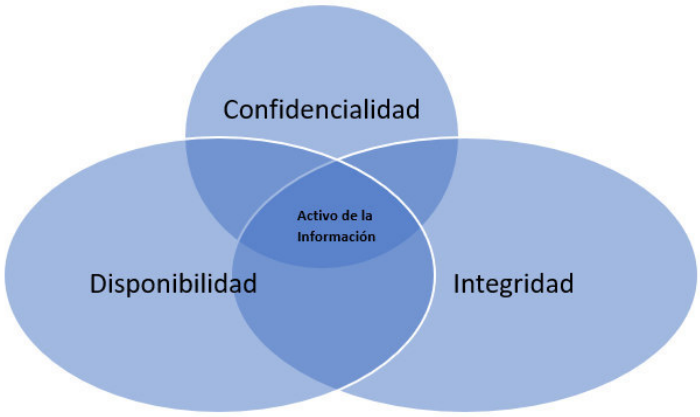

Figura 2.1. Dimensiones de activos de información según ISO 27000. Elaboración Propia

2.2 Seguridad de la Información

La seguridad de la información nace ante la necesidad de la información de una empresa, institución u organización se encuentre integrada y resguardada bajo buenas medidas de seguridad. Según el ISO 27001(2013), la seguridad de la información tiene como objetivo mantener un nivel alto de preservación de la confidencialidad, integridad y disponibilidad de los sistemas de información y de los demás sistemas implicados en su tratamiento.

Estos tres términos constituyen el eje principal en que se basa todo el ámbito referente a a seguridad de la información. Dado que la información es vital para las empresas, esta se clasifica de acuerdo con su nivel de importancia:

- Crítica: Es necesario o requerido para distintas operaciones esenciales de empresa.
- Valiosa: Es un activo perteneciente a la organización de gran valor.
- Sensible: Solo puede ser conocida y accedida por personas autorizadas y en el tiempo autorizado.

Se debe enfatizar que la seguridad de la información difiere al termino de seguridad informática, este último sólo se encargaría de la seguridad en el medio informático y digital, pero la información se podría encontrar incluso en las personas o trabajadores de las organizaciones, de esta manera la seguridad de la información engloba lo que es la seguridad informática.

Con el fin de garantizar que la seguridad de la información es gestionada de manera correcta, es necesario hacer uso de un proceso sistematizado, ordenado y documentado, y obedecidos por toda la organización, este proceso se considera un Sistema de Gestión de Seguridad de la Información (SGSI).

Sistema de Gestión de Seguridad de la Información.

Según ISO 27002(2013) define el SGSI como todo esfuerzo para proteger los activos de información de una organización basados en un conjunto de políticas, procedimientos, directrices, y recursos gestionados por un orquestador. Para alcanzar los objetivos propuestos en un SGSI, deberá representarse mediante un único enfoque sistematizado, el cual le permita establecer, desarrollar, operar, supervisar, mantener y mejorar la seguridad de la información dentro de la organización.

Para Heasuk (2011), “conciben que un sistema de gestión de seguridad de la información ha sido desarrollado para la administración eficaz de la seguridad de la información en una organización. Donde los SGSI son capaces de hacer frente a una variedad de incidentes de seguridad.”

En un SGSI, ayuda a establecer y definir diversas políticas y procedimientos relacionado con los objetivos de negocio de la organización, con el único objetivo de conservar un nivel de exposición bajo y siempre menor al nivel de riesgo que se ha decidido asumir;

De esta manera la organización va a poder reconocer los riesgos asumidos y puede tomar decisiones como minimizarlos, transferirlos o controlarlos, así de una manera ordenada y documentada.

Figura 2.2. Contexto de un SGSI. Extraído de: "SGSI – Topic Inf.", por ISO 27000.ORG, 2015

2.3 Gestión de Riesgos de Seguridad de la Información.

Riesgo

Según Luhmann (1996), define el riesgo como conjunto de posibilidades de daños y perjuicios en el futuro debido a las distintas decisiones tomadas. Las decisiones tomadas en el presente van a condicionar lo que sucederá en el futuro, aunque no se sepa de qué manera.

Para Mir (1999), el riesgo se refiere a diversas acepciones, tal como una contingencia desfavorable a la que se está expuesto un individuo, una organización o alguna eventualidad, También se considera como una incertidumbre que es derivada del desarrollo de alguna actividad empresarial, peligro incierto, etc.

Según el Programa de las Naciones Unidas para el Desarrollo (PNUD), se genera la siguiente pregunta: "¿por qué se deberá adoptar nuevas tecnologías?", y detalla 3 razones a considerar:

- Posibles beneficios. Las posibilidades de promover el desarrollo humano mediante las actuales transformaciones tecnológicas son inmensas en los países en desarrollo. En algunos casos, los beneficios previstos, son, cuando menos, tan grandes como los riesgos.
- El costo de la inercia frente al costo del cambio. Las nuevas tecnologías suelen ser una mejora de aquellas que reemplazan.
- Medios para asumir la gestión de riesgos. Es posible asumir la gestión de muchos posibles riesgos y reducir la probabilidad de que ocurran mediante la investigación científica, la reglamentación y la capacidad institucional.

Gestión de riesgos de Seguridad de la Información

Para el Departamento de Seguridad Informática de la Universidad Nacional de Luján, la gestión de riesgos se exhibe como la actividad clave para el resguardo de los activos de información dentro de una organización y por consecuente tiende a proteger la cualidad de cumplir sus principales objetivos. También lo define como un esfuerzo constante que se apoya en la administración con el fin de equilibrar los costos operacionales y económicos causados por la suspensión de las actividades y el perjuicio de activos, con los costos de las acciones de protección a aplicar sobre los sistemas de información y los datos que dan soporte vital a la operatividad de la organización, mitigando los riegos que presentan los activos de información a niveles viables y aceptables para la misma.

Según Instituto Nacional de Ciberseguridad de España (2017), la gestión de riesgos de seguridad de la información es un proceso que consiste en:

- **Comunicación:** Se realizan actividades para informar continuamente al equipo, la dirección y a la plantilla. A la par, se continúa recibiendo información desde distintos procesos y de los stakeholders. El objetivo de estas acciones es lograr difundir la información requerida para conseguir la venia de los responsables y los afectados por las decisiones que se adopten.
- **Establecimiento del contexto:** Se definen los aspectos y criterios básicos para la gestión de riesgos de seguridad de la información. Además, sirve para ser conocedor y prudente de las leyes que se deben cumplir, así como

obligaciones de contratos con terceros y normativa aplicable. Cada área independiente deberá hacer valer sus expectativas, bienes y recursos aprovechables y cómo se estimará y calificará las posibles consecuencias de los riesgos.

- **Valoración del riesgo:** Se considera la fase central y más relevante, en esta se identifica, analiza y evalúa los riesgos.
- **Tratamiento y aceptación del riesgo:** Se tendrá un listado ordenado de riesgos o una lista como la del ejemplo con su posición. Luego se deberá seleccionar y estimar qué hacer con cada uno de ellos de acuerdo a su particularidad de su valoración y de los criterios establecidos. Es decir, se deberá de posicionar la «línea roja» de nuestro limite o grado de tolerancia al riesgo
- **Revisión y monitorización:** Se deberá de revisar y corroborar continuamente los valores de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles modificaciones que hayan impactado.

Figura 2.3. Gestión de Riesgo de Seguridad de la Información. Extraído de: "SGSI – Topic Inf.", por ISO 27000.ORG, 2015

2.4 Marco Referencial

Para el marco referencial de esta investigación se presenta de manera breve y conceptual las normas y guías internacionales de buenas prácticas y destrezas para la gestión de seguridad de la información. Estas normas de la Organización Internacional para Estandarización (ISO) tienen el objetivo de orientar, simplificar y unificar criterios con el objetivo de aumentar la efectividad en las organizaciones.

La norma ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Para esta investigación se tomará como referencia la 27001 y la 27005 que están más orientadas al tema que se desarrolla.

2.4.1 ISO/IEC 27001

Esta norma certificable fue publicada en 2005 y la versión vigente en septiembre de 2013, en la cual las versiones tienen diferencias en su estructura en la parte principal. Esta norma es la primordial de la serie y detalla las condiciones necesarias para sentar, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Debido a su alineamiento con otros procesos de Gestión, se incluye procedimientos de valoración y gestión de los riesgos involucrados mediante el Modelo de Mejora Continua de Deming (PDCA) Planificar, Hacer, Verificar y Actuar.

La norma consta con 11 apartados enumerados desde el 0 al 10, y un anexo donde contempla los objetivos de control. En los apartados del 4 al 10 se encuentran definidos los requerimientos y se describen brevemente a continuación.

- **4.Contexto de la organización:** Trata referente a la empresa, La repercusión de comprender la organización su contexto. Se determina el alcance del SGSI.
- **5. Liderazgo:** En este título refiere que la organización debe mostrar su liderazgo y compromiso con la implementación del plan de GSI, así como la asignación de responsabilidades y roles y también construir una política de seguridad de la información.

- **6. Planificación:** Tiene como objetivo que la organización planifique el SGSI determinando los riesgos y amenazas a los que se encuentra comprometida.
- **7. Soporte:** Define los recursos que serán necesarios para la implantación, implementación y actualización del SGSI. También incluye especificar la necesidad de comunicaciones internas y externas.
- **8. Operación:** Este Este título refiere sobre el desarrollo del bosquejo, así como de ejecutar y controlar los procesos y objetivos para cumplir con los requerimientos del SGSI.
- **9. Evaluación del Desempeño:** Mide el rendimiento y eficacia del SGSI.
- **10. Mejora:** Este título refiere a las acciones y/o medidas que se deberán ejecutar al producirse una disconformidad u oportunidad de mejora.

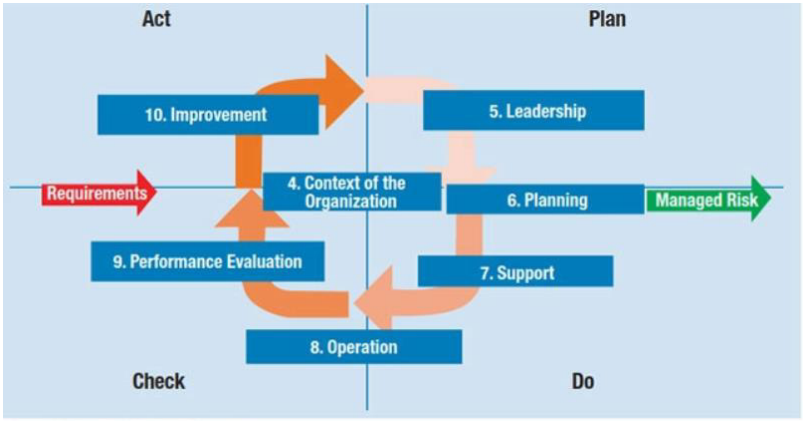

Figura 2.4. Mapeo de los Apartados del ISO 27001 – PDCA. Extraído de: "Isaca Journal 2017, vol 4", por T. Mataracioglu, 2017

2.4.1 ISO/IEC 27005

Esta norma no certificable fue publicada en 2008, actualmente la tercera edición vigente se actualizó en Julio 2018. Esta norma proporciona las instrucciones para la administración del riesgo en la seguridad de la información. Asimismo, muestra los conceptos universales y está diseñada para apoyar a la aplicación exitosa de la seguridad de la información orientada en una perspectiva de gestión de riesgos. En esta norma no se

especifica o recomienda alguna metodología de evaluación y gestión de riesgos, e incluye ejemplos de amenazas, vulnerabilidades e impactos.

La estructura de esta norma consta de 12 apartados, de los cuales los primeros 6 apartados son de carácter estructural y teórico, y desde el apartado 7 al 12 se evidencia mejor las directrices que recomienda la norma. En la siguiente figura se muestra cómo se establece la secuencia de funcionalidad de la normativa donde cada recuadro es un apartado definido y explicado dentro del documento.

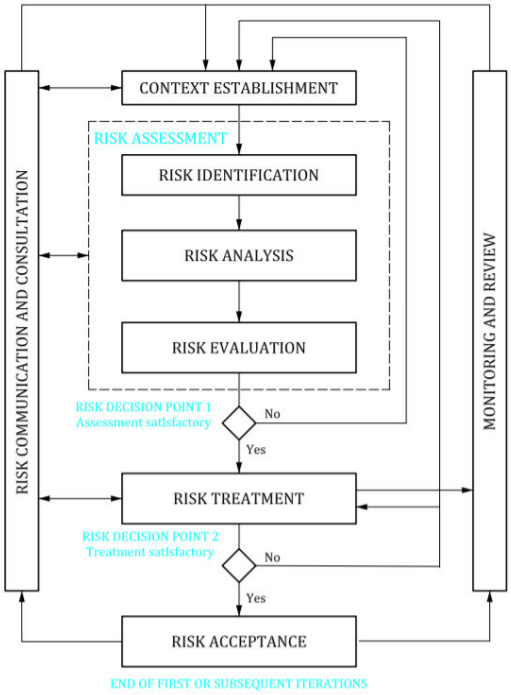

Figura 2.5. Proceso de Gestión de riesgos de Seguridad de la Información. Extraído de: Gestión del Riesgo - Directrices, por ISO.ORG, 2018

2.4.3 ISO 31000

Esta norma fue publicada en noviembre de 2019 por ISO. Tiene por objetivo que cualquier organización puedan administrar los riesgos de las organizaciones de manera efectiva, y que su desarrollo, implante y mejoren de forma continua un marco de trabajo que integre la gestión de riesgos a lo largo de cada uno de sus acciones. Esta norma no está creada como un sistema especifico de gestión, más bien se refiere como a una guía

de buenas herramientas y prácticas para las actividades en relación con la gestión de riesgos.

En cuanto a la estructura de la norma consta de tres elementos clave para su eficacia.

- Principios para la Gestión del Riesgos: Brinda 11 principios básicos para cumplir a lo largo de la implementación.
- Estructura o Marco de Trabajo: Tiene como objetivo incorporar los procesos de gestión de riesgos para desarrollar una mayor responsabilidad en la implementación.
- Proceso de Gestión de Riesgos: Se desarrolla mediante 3 fases. Establecimiento del contexto, valoración del riesgo y tratamiento de estos.

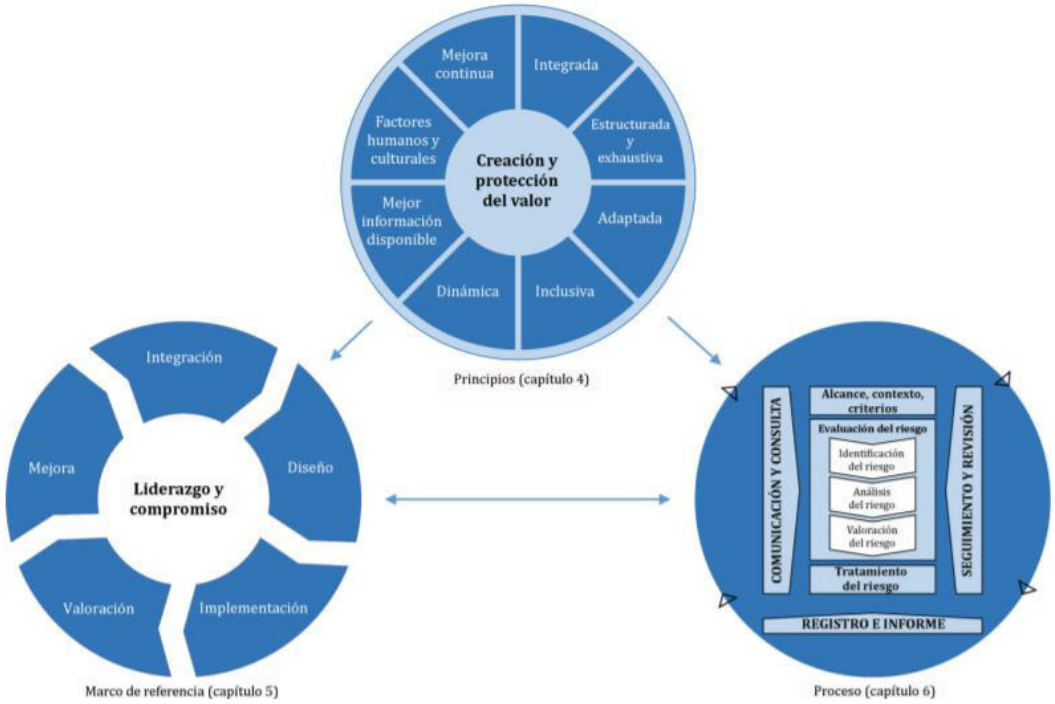

Figura 2.6. Estructura ISO 31000. Extraído de: Gestión del Riesgo - Directrices, por ISO.ORG, 2018

2.5 Marco Legal Nacional

Dado que la investigación se realiza en el ámbito nacional, está regulada y regida por distintas normas técnicas peruanas (NTP), por leyes y demás normativas del ámbito peruano. A continuación, se detalla algunas de las más representativas.

2.5.1 NTP-ISO 27001:2014

Norma Técnica Peruana aprobado y publicado en enero de 2014. Adopta las normas y recomendaciones del ISO 27001 con el fin de asegurar la confidencialidad e integridad de la información y de los sistemas inmersos. En cuanto a la implementación se hace obligatorio para las organizaciones públicas del Sistema Nacional de Informática, con excepción a aquellas ya certificadas en el ISO 27001. Así mismo nombra a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) como referente de asistencia técnica y consultor de las entidades que lo requieran.

Esta normativa recomienda designar e implementar un consejo de gestión de seguridad de Información, cuyas funciones son establecidas por cada entidad de acuerdo con la norma. En cuanto a la estructura es similar a la ISO 27001 detallada anteriormente en este capítulo.

2.5.2 Ley de Protección de Datos Personales

Ley 29733, Ley de Protección de Datos Personales fue publicado en Julio del 2011 y promulgado mediante reglamento en marzo de 2013, en la cual se establecen los principios, derechos y obligaciones que deben adoptar las instituciones públicas y privadas con el tratamiento de datos personales. En esta ley se decreta las obligaciones a las empresas con el fin de que estas garanticen el apropiado tratamiento de los datos personales y privados de sus clientes, proveedores, trabajadores y demás personas relacionadas a sus actividades.

Principales Obligaciones para la empresa:

- Registrar ante la autoridad los Bancos Datos Personales (BDP) que posea la empresa. La ley define un BDP como un grupo asociado y ordenado información de personas naturales. Dicha información se puede encontrar registrada y almacenada en diversos medios electrónicos y automatizados (por ejemplo: Archivos de texto plano, Archivos de Microsoft Word, Excel, PDF, en imágenes, audios o diverso contenido audiovisual, almacenados en ordenadores, dispositivos

de almacenamiento no volátil o servidores de la empresa, archivos en la nube, etcétera). Para inscribir un BDP se presenta un formulario ante la autoridad registrando en este las propiedades, atributos, la naturaleza de los datos, la finalidad, su tratamiento, entre otros.

- Conseguir y registrar el consentimiento debidamente comunicado de los propietarios de los datos personales. El titular del dato personal debe dar su consentimiento y/o autorización a que la empresa pueda tratar sus datos personales.
- Desarrollar e implementar medidas de seguridad competentes y eficaces. Las empresas tienen la obligación de proteger y resguardar íntegramente la información personal que ha sido confiado en ellas. Algunas de las medidas es establecer protocolos, gestionar procesos en la seguridad de la información, establecer salvaguardas, etc.
- Implementar un procedimiento y acciones de vigilancia de los derechos de las personas naturales. Las empresas que posean la información privada deben garantizar que las personas naturales tengan la facilidad de ejercer los siguientes derechos respecto a sus propios datos:
  - ✓ Acceso.
  - ✓ Rectificación.
  - ✓ Cancelación
  - ✓ Oposición.
- Informar el tráfico transfronterizo. Cuando la empresa transfiera datos personales desde su BDP a un destinatario en el extranjero deberá comunicar el nombre y la ubicación del destinatario, así sea del mismo grupo empresarial o almacenamiento de cloud computing.

Consecuencias si se incumple las obligaciones referidas en la ley:

En la Ley, se exige el apropiado y correcta manipulación y gestión de datos personales de clientes, proveedores, colaboradores, trabajadores y demás personas asociadas o vinculadas a las actividades de la sociedad; y aquellas que no lo cumplan serán

fuertemente sancionadas por la autoridad competente. La multa máxima puede ser hasta 100 UIT dependiendo de la transcendencia de la falta cometida y el tamaño de la empresa. Según el Ministerio de Justicia, que es la Máxima Autoridad Nacional de Protección de datos Personales, en el 2018 realizó 283 inspecciones de fiscalización a organizaciones públicas y privadas en datos personales y, viendo distintas falencias, interpuso sanciones con multas por encima de 700 000 soles por infringir esta ley.

En la imagen a continuación se ejemplifica a manera de resumen los principales requerimientos de la Ley, así como objetivos y alcance.

Figura 2.7. Principales Requerimientos Ley 29733. Extraído de "Ley de Protección de Datos Personales", por Deloitte, 2016.

2.5.3 NTP-ISO 17799

En la norma técnica peruana NTP-ISO/IEC 17799 se encuentran las distintas sugerencias y recomendaciones de buenas prácticas requeridas para lograr gestionar un Sistema de Seguridad de la Información (SSI). Se define como una guía práctica en la cual se encuentra detallado los estándares organizacionales de la seguridad y logra producir prácticas efectivas en el transcurso de la gestión de la Seguridad de la Información.

Dentro de esta norma define distintos conceptos referidos a la seguridad de la información, se establece de una manera más teórica y de conocimiento respecto a la 27001.

2.5.4 Ley de Delitos Informáticos

La ley N°30096 Ley de Delitos Informáticos fue originada con el fin de luchar contra la ciberdelincuencia, ciberdelito o cibercrimen en el Perú. La Ley N°30071 modifica la anterior en los artículos 2,3,4,5,7,8 y 10. Según esta ley, considera como bienes jurídicos a la confidencialidad, integridad y la información; y se califica como delitos cuando estas se infringen.

Según una investigación del diario La República (2019) identifica en el Perú algunos de los delitos informáticos más frecuentes. Estos son el fraude informático, hacking, ataque de virus, clonación de tarjetas, extorsión online, estos ataques se realizan comúnmente mediante llamadas falsas, mensajes de texto de extraños, envió de correo (donde aplican phishing para obtener información sensible como claves de cuentas, datos personales y empresarial, etc.), otros.

Dentro de la Ley de delitos informáticos se establece explícitamente penas y sanciones para aquellas personas que atenten contra la integridad de datos, sistemas informáticos, a la alteración de información restringida y personal, contra la intimidad y el secreto de las comunicaciones como el tráfico ilegal de datos, el hackeo de datos personales, robo de identidad personal o empresarial, y fraude informático.

A continuación, se resume en la tabla algunas de las penas más significativas que sanciona la afección esta ley.

Tabla 2.2. Delitos Penados por Ley 30096. Ley de Delitos Informáticos, recopilado de gob.pe.

Delitos	Penas (Rango)
Contra datos y sistemas informáticos: Comprende la obtención indebida y no autorizada de la información, violación de la integridad de los datos o de sistemas informáticos.	1-4 años
Contra la intimidad y el secreto de las comunicaciones: Comprende la comercialización no autorizada de datos e	3-6 años

información de terceros, obtención de información privilegiada por distintos medios de intercepción.	
Contra el patrimonio: Fraude informático	3-8 años
Contra la fe pública: Comprende la usurpación o falsificación de identidad	3-5 años
Disposiciones comunes: Comprende el uso indebido de medios informáticos con fines delictivos	1-4 años

2.6 Aplicación Web

De acuerdo a la Ingeniería de Software, una aplicación web, es toda herramienta informática que distintos usuarios, desde diferentes conexiones pueden utilizar conectándose a un servidor web a través de Internet o Intranet con la ayuda de cualquier navegador.

Según Benjamín (2010, pg. 26), la define como una agrupación de recursos web y aplicaciones integrado de diversos y esenciales componentes como servidores dinámicos (Servlets, JSPs), elementos web estáticos (páginas web) y bibliotecas de clases utilitarias entre otros independiente de la tecnología utilizada.

Dentro de las ventajas del uso de aplicaciones web encontramos lo siguiente:

- Ahorro de tiempo, al ser apps sencillas en su gestión permite realizar tareas de manera fácil y rápida.
- Actualización continua e inmediata, mediante el desarrollador y los usuarios que gestionen contenido.
- Compatibilidad, en los distintos dispositivos y navegadores en lo que utilicen.
- Alta disponibilidad.
- Colaborativo.

2.7 Web Services

Dentro de la arquitectura del software se hará referencia a servicios web consumidos por una ampliación móvil, por lo cual se define de forma teórica. Según la World Wide Web Consortium (W3C), un servicio web lo define como aquel sistema de software asignado

con el objetivo de permitir y facilitar la interacción de máquina a máquina Inter operativa mediante una red. Adicionalmente se determina como un conjunto de protocolos con el propósito de intercambiar diversos datos por medio de aplicaciones de software, la idea general es que diversas aplicaciones de software desarrollados en distintos lenguajes de programación y ejecutadas sobre cualquier plataforma, pueda consumir los servicios web con la finalidad de intercambiar cualquier dato de manera íntegra en redes de computadores.

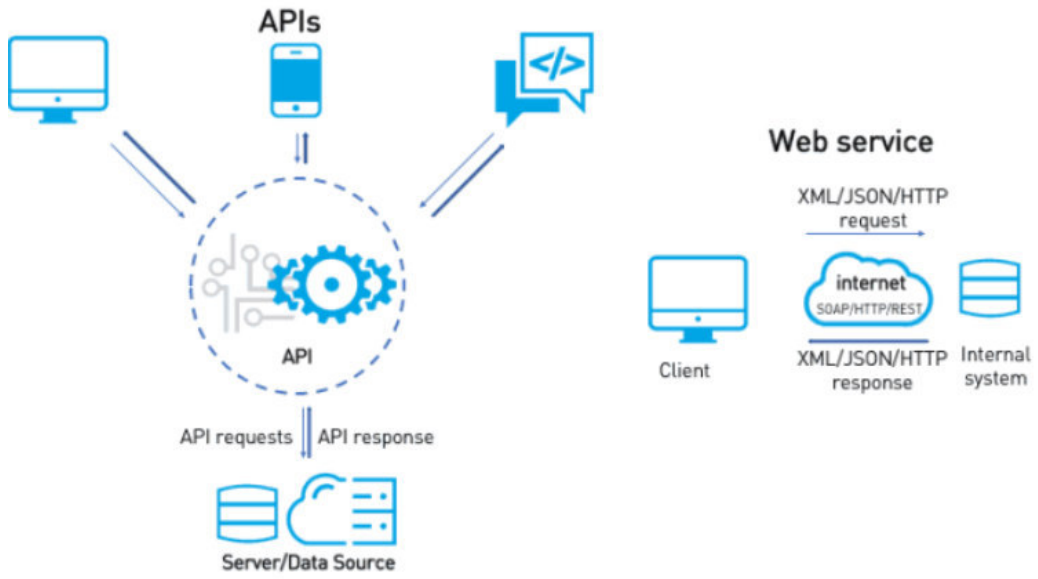

Figura 2.8. Diagrama básico de Web Services. Extraído de "Web Service and API", por Beltran C. - Dawood Ansar, 2019

Dentro de los webs services tenemos algunos tipos y definiciones que se necesitaran detallar.

2.7.1 SOAP

Simple Object Access Protocol, según IBM en su definición

IBM Knowledge Center (2018), SOAP es un formato de mensaje XML que es empleado en procesos de servicios web. Generalmente se utiliza HTTP o JMS para enviar los mensajes SOAP, aunque también se pueden utilizar otros protocolos. El uso de SOAP en un servicio web específico se describe mediante la definición WSDL. Dentro de sus características más resaltantes encontramos que debido a que funcionan mediante el

protocolo TCP, se podrían emplear diversos protocolos de aplicación como HTTP, SMTP, JMS, y de igual proporciona la posibilidad de generar una secuencia de cliente/servidor entre diversos lenguajes de programación.

2.7.2 REST

REpresentational State Transfer, esta tecnología permite realizar API con web services, esta tecnología es una definición de arquitectura que indica como se debería efectuar el intercambio y manejo de datos mediante los servicios web, estos servicios se conoce como RESTful Web Services. Una característica resaltante es que las APIs REST se basan en el protocolo HTTP para generar métodos y códigos de respuesta.

Comparado con SOAP, la tecnología REST genera APIs menos seguras y puede generar menor cantidad de bloque de datos, además que, aunque es conocido REST no existe como estándar a comparación de SOAP.

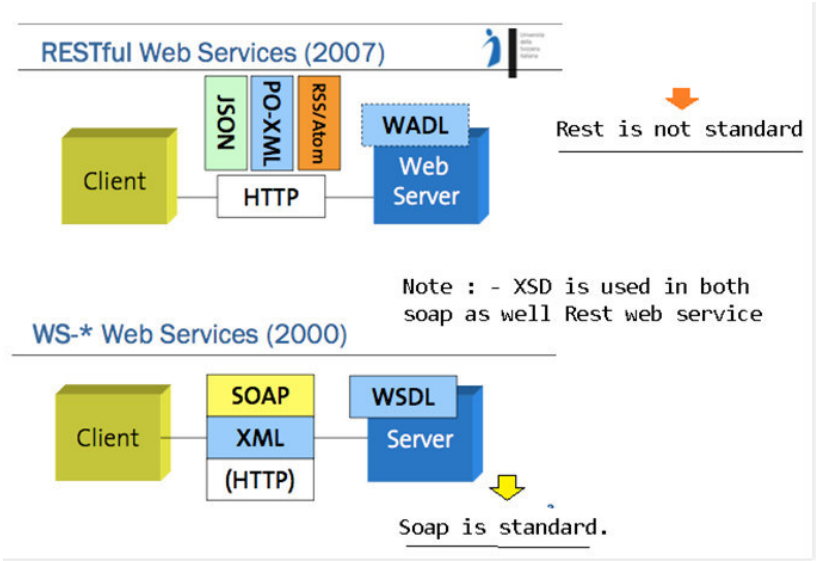

Figura 2.9. REST vs SOAP. Extraído de: "Annual SOA Symposium", por Cesare Pautisso, 2010.

2.8 Aplicación móvil

Una aplicación móvil o app es una aplicación informática o un software desarrollada y proyectada a ser desplegada o interpretada en teléfonos inteligentes, tabletas y otros dispositivos móviles. Comúnmente se encontrarán disponibles para su adquisición y descarga mediante las diversas plataformas de distribución, gestionadas por las

compañías poseedoras de los sistemas operativos móviles como Android, IOS, etc. De acuerdo al desarrollo de este software existen 3 tipos de apps móvil

- Aplicaciones nativas: Son aquellas que se desarrollan ad hoc para un sistema operativo móvil determinado, los cuales se denominan software development kit o SDK. Entre los más conocidos son iOS y Android Una de las más grandes desventajas para el desarrollo de apps nativas es su coste más elevado con respecto a las demás
- Web apps: El desarrollo y despliegue del software para estas aplicaciones está orientado para poder ejecutarlo en un dispositivo o navegador, de manera que se encuentra programado de manera muy independiente del sistema operativo que lo ejecute y su fin es llegar a diversos dispositivos. Este tipo de apps no necesitan instalación, por lo que solo es necesario crear un acceso directo y servirá para poder ejecutarla. Dentro de algunas contras es su restricción a acceso de ciertas características de los dispositivos y debe tener de manera obligatoria conexión a internet para su utilización.
- C apps interpretadas: es un tipo de app que combina las apps nativas y las web apps. Su desarrollo se basa en los lenguajes más populares de las aplicaciones web como son HTML y CSS, lo cual permite su utilización en distintas plataformas. Adicionalmente permite acceder a las características de los dispositivos, por lo que se representa como una mayor experiencia del usuario.

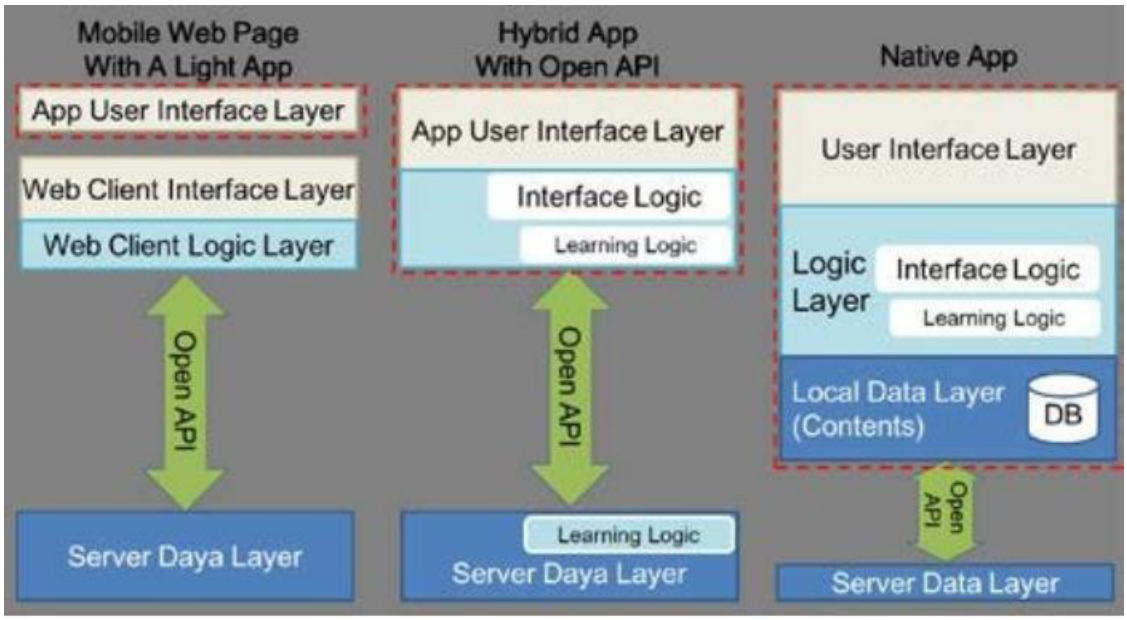

Figura 2.9. Arquitectura de apps móvil. Extraído de: "Mobile apps Arq.", por H. Al-Harrasi 2015

2.9 Android

Según definición por Gonzales Alejandro (2012), Android es un sistema operativo móvil orientado a dispositivos personales y teléfonos móviles. Su principal característica es que está basado sobre Linux, cuyo núcleo de sistema operativo es abierto y multiplataforma.

Se pueden desarrollar aplicaciones en lenguaje de programación java o kotlin, y acceder a las funcionalidades del propio teléfono (por ejemplo, agenda, llamadas, fotos, archivos, etc.) mediante las interfaces requeridas que brinda el sistema operativo. Fue desarrollado por Android Inc., empresa que Google patrocinó económicamente y que posteriormente compró en 2005. Su código fuente primordial de Android se conoce como Android Open Source Project (AOSP), el cual se encuentra registrado bajo la Licencia Apache. Android fue presentado en 2007 ligado a la fundación del Open Handset Alliance (un consorcio de compañías de hardware, software y telecomunicaciones) con el propósito de continuar con la tendencia del open source.

2.9.1 Actividades Android

Una actividad Android se define como una agrupación de construcción delegado cuando una ventana se crea, la cual nuestra aplicación que usa para dibujar y recibir eventos del sistema (gestos táctiles como tap, press and hold, hold, etc.). Se define como el componente más común dentro de las aplicaciones para Android. Los componentes Activity evidencian cuando una aplicación se ha llevado a cabo por una actividad, y que es asociada comúnmente con una ventana o interfaz de usuario; es relevante indicar que no solo está incluido el aspecto gráfico, sino que éste constituye una sección del componente Activity mediante vistas interpretadas por clases como View y sus derivadas. Este componente se implementa a través de la Activity.

De acuerdo al diseño del S.O Android, cada actividad puede representar distintos estados.

ESTADO	¿En Memoria?	¿Visible al usuario?	¿En primer plano?
Inexistente	No	No	No
Detenida	Si	No	No
Pausada	Si	Si	No
En marcha	Si	Si	Si

Cada estado puede ser ejecutado mediante tipo de callback llamados por Android.

- Método onCreate() . Es ejecutado en el instante de que el sistema crea una nueva instancia en memoria de la actividad. Ejecuta tareas como: Agregar fragmentos, crear instancias de componentes, iniciar consultas a fuentes de datos, etc.
- Método onStart(). Es disparado inmediatamente despues del método onCreate(), en el cual se puede programar sentencias asociadas a la UI.
- Método onRestart(). Este es llamado en el momento en que una la actividad ha alcanzado el estado detenido. Se ejecuta antes de onStart y después de onStop. Contribuye en la diferenciación de una recreación y un reinicio.
- Método onResume(). Es llamado en el instante antes de que la actividad sea puesta en marcha para ejecutar con el usuario de primer plano. Se suele ejecutar animaciones, interacciones con la aplicación de la cámara, actualizaciones, etc.
- Método onPause(). Se llama en el momento de que el sistema retira del primer plano a la actividad, y entra en el estado pausado.

- Método onStop(). Se llama antes de seguir con el estado Detenido y donde el usuario no podrá visualizar la actividad.
- Método onDestroy(). Se llama antes de destruir la instancia de una actividad. Se añade instrucciones de limpieza de recursos.

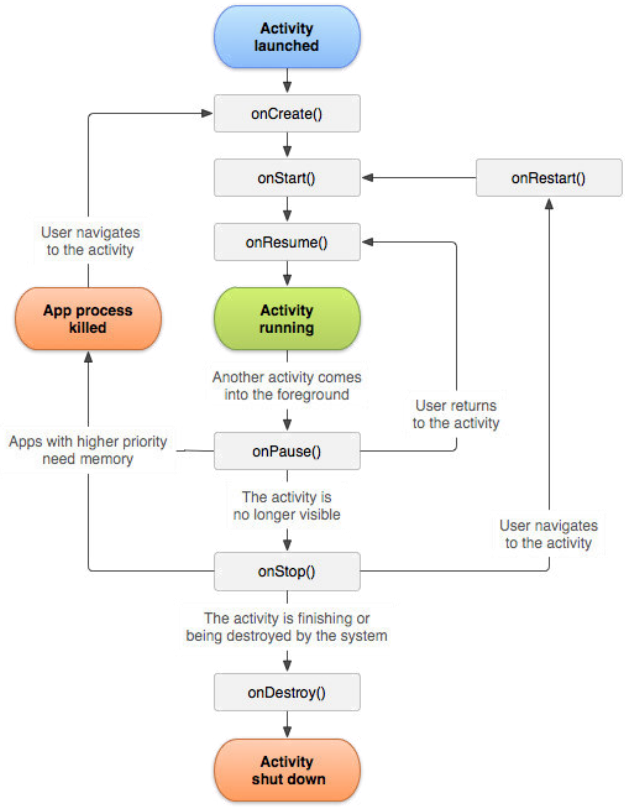

Figura 2.10. Ciclo de vida de una actividad Android. Recuperado de: "Devolper's Guide - Lifecicle", por Developer.Andorid.com, 2013

CAPÍTULO III

ESTADO DEL ARTE

En este capítulo se va a identificar los antecedentes históricos más significativos de los modelos de gestión de riesgos según su origen, autores, objetivos y aportaciones. Cada uno de los modelos está debidamente resumido, estructurado y evaluado con el aporte que podría ofrecer a esta investigación. Al final del capítulo se presenta una evaluación mediante un cuadro comparativo de los modelos investigados.

3.1 Investigaciones relacionadas

3.1.1 MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA PYMES PERUANAS

Garcia Porras J., Huamani Pastor S. Revista Peruana de Computación y Sistemas 2018

En esta investigación publicada en la edición 2018 -1 de la Revista Peruana de Computación e Informática los autores proponen un modelo de gestión de riesgos de seguridad de la información enfocado al sector de pymes y orientado en un enfoque cualitativo. La propuesta del modelo se basa sobre las buenas prácticas de la metodología OCTAVE-S y las normas ISO/IEC 27005; y consta de las 3 fases de OCTAVE al cual se le añade la lista de vulnerabilidades y escenarios, y se incluye el cálculo y tratamiento del riesgo de la ISO/IEC 270005. Adicional a esto al modelo planteado se adiciona un enfoque cuantitativo, el cual permite calcular el riesgo residual en base a la efectividad de los controles generados.

La metodología propuesta en esta revista se resume en la imagen 3.1 y consta de 3 fases. Se tiene en cuenta los documentos de entrada (información de la empresa, situación del S.I y T.I, políticas, informes) antes del inicio de las fases. La primera fase se centra en la construir el perfil de las amenazas, para esto se divide en 2 procesos, el primer proceso es identificar la información organizacional de la empresa, y el segundo proceso crea el pefil de la amenaza que va relacionado con el riesgo y se añade la lista de vulnerabilidades y escenarios mapeados previamente. En la fase 2 se encarga de identificar los componentes

o procesos críticos relacionados con la tecnología y sus vulnerabilidades. En la fase 3 se encarga de analizar el riesgo y de acuerdo a su evaluación, elaborar un plan de protección y mitigación del mismo.

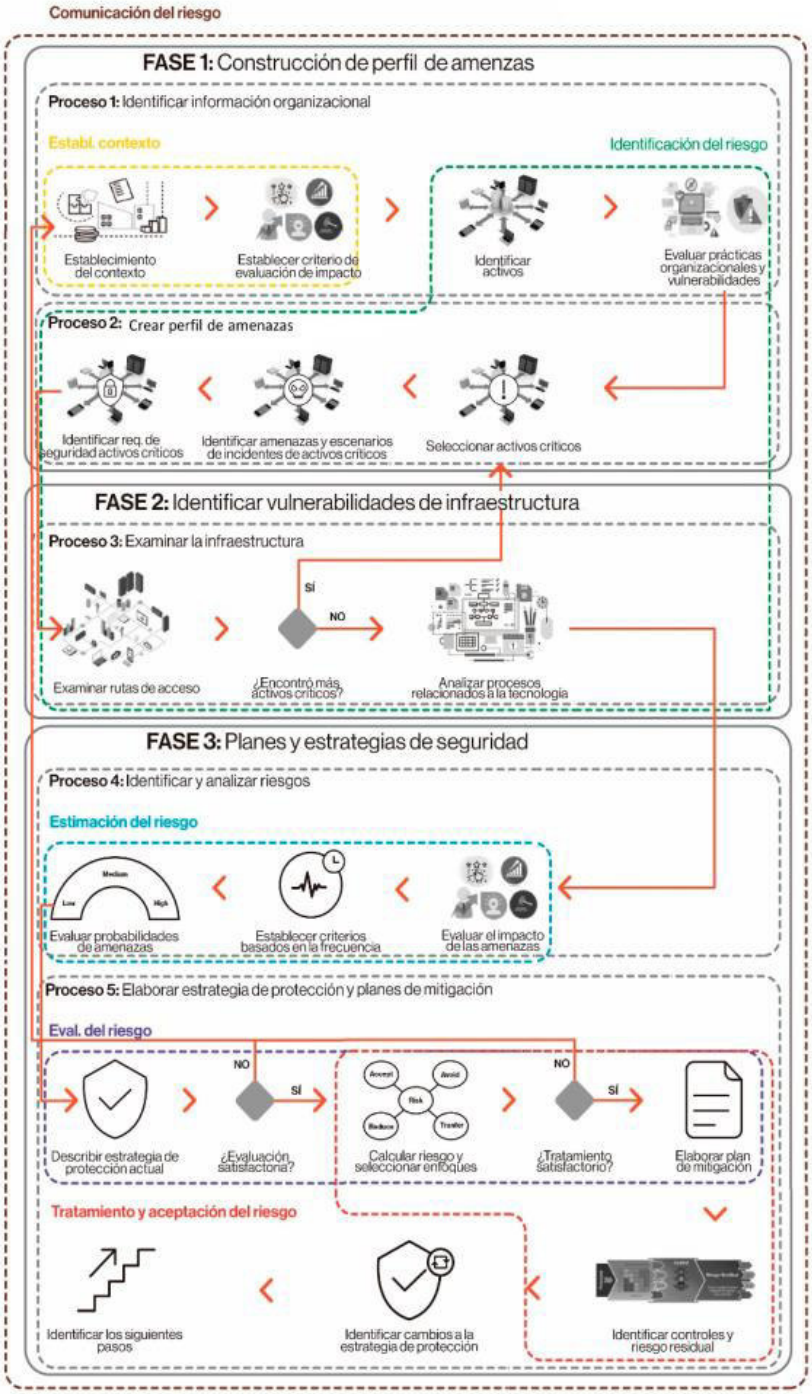

Figura 3.1. Modelo de Gestión de Riesgos de Seguridad de la Información para PYMES peruanas. Garcia Porras J, 2018.

Este modelo ha sido implementado en una PYME peruana desarrollando exitosamente las 3 fases del modelo propuesto. Como resultado de la implementación del modelo los autores afirman haber reducido en un 53% el nivel de riesgos dentro de la empresa mencionada.

Este paper es de mucho apoyo para tomar como referencia ya que se centra en aplicar un modelo de gestión de riesgos de seguridad de la información de manera rápida y eficiente, desarrollando solo los procesos principales para la evaluación del riesgo, pero al mismo tiempo cumpliendo con las buenas prácticas, por este motivo aporta significativamente a la presente investigación. Por otro lado, no menciona ninguna herramienta tecnológica que apoye la metodología empleada y está no se ha implementado en el sector de consultoría, los cuales son un rubro de negocios distintos.

3.1.2 INFORMATION SYSTEMS SECURITY RISK MANAGEMENT MODEL IN KENYAN PRIVATE CHARTERED UNIVERSITIES

Salesio M. Kiura. European Journal of Computer Science and Information Technology. 2017

Esta es una investigación de formato paper publicado por la revista europea de ciencias de la computación y tecnología de la información. En esta investigación, el autor propone un modelo de Gestión de riesgos que las universidades pudieran implementar con el fin de un seguro sistema de información. Dentro de su investigación, refiere la importancia en los stakeholders en el éxito de la gestión de riesgos, el lineamiento con la ISO 27001, un estado actual de la gestión de seguridad de los sistemas de información mediante encuesta e investigaciones, la frecuencia de violaciones a la seguridad del sistema de información, entre otros indicadores.

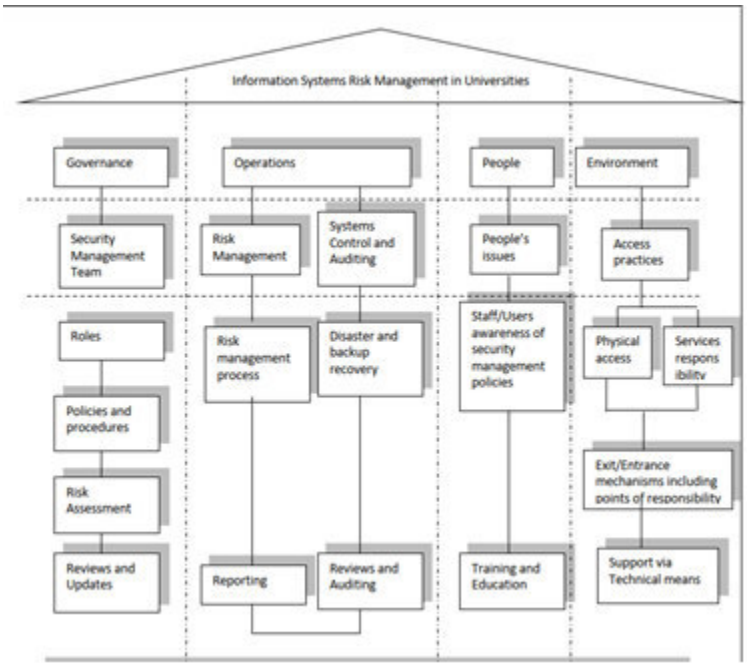

Figura 3.2. Modelo propuesto de Gestión de Riesgos de Seguridad de la Información. Salesio Kiura, 2017.

En su modelo propuesto divide por pilares los principales factores de éxito a tener en cuenta para la gestión de riesgos. Describe de manera funcional, teórica y no técnica la función y procedimiento de cada pilar. Como conclusión el autor hace referencia a los retos de implementar el modelo en las universidades por en entorno diverso de las mismas. Esta contribución es más de un aspecto no técnico, no menciona alguna tecnología o herramienta informática a utilizar, ya que sería de manera complementaria al modelo planteado.

3.1.3. A RISK MANAGEMENT TOOL FOR COMPUTING ENVIRONMENTS

Adelmeyer Michael. Osnabrück University, Alemania. 2018

Esta investigación en formato paper tiene como objetivo principal diseñar e implementar una herramienta informática o software para la gestión de riesgos de información de servicios en la nube, de esta manara plantea el diseño de la herramienta de forma modular, iterativa y flexible. Para esto primero se define un framework de sistemas de información al cual servirá de guía. Luego define por categorías (técnica, organizacional,

legal y otros) los riesgos a los que estará expuestos sus activos de información en la nube, esto mediante una tabla de análisis.

En el desarrollo de la herramienta informática, primero realiza un análisis modular del software a desarrollar (módulos de evaluación, monitoreo, reportes, tratamiento e incidentes del riesgo, entre otros), además de establecer los requerimientos funcionales para el desarrollo del software y realiza el diagrama de casos de uso con UML según su análisis. Por el lado más técnico para el software propone un desarrollo con bases de datos SQL, un gestor de contenido con DRUPAL para las funcionalidades básicas descritas en los requerimientos y por el lado del cliente desarrollo con HTML, CSS e incluso librerías de Google, tal como se verifica en el siguiente diagrama conceptual técnico del software.

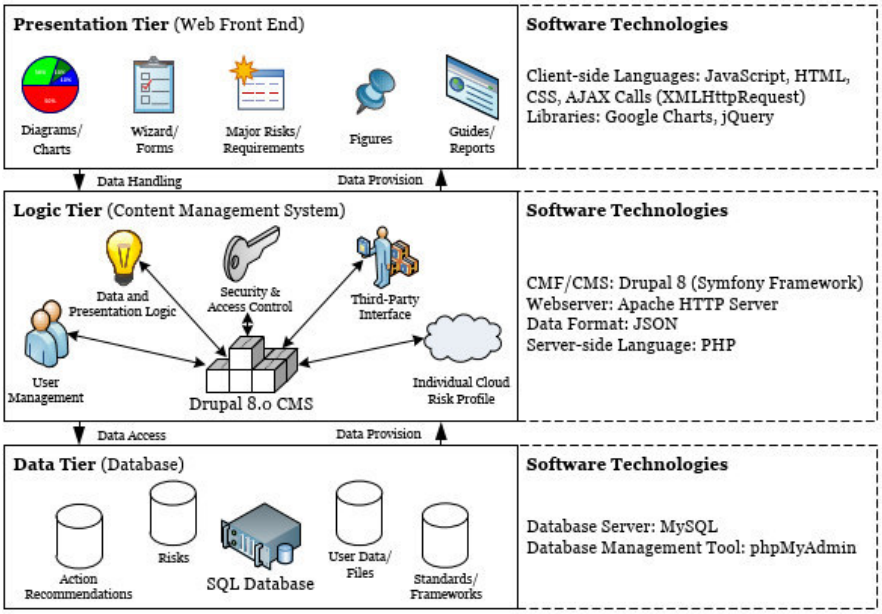

Figura 3.3. Technical Concept of software Riscc. Adelmeyer Micahel, 2018.

En el artículo también especifica el modelo de base de datos y algunas interfaces gráficas, siendo estas últimas, a consideración, muy atractivas en el diseño para el usuario. En el nivel de aporte es significativamente alto ya que refiere y menciona muchos aspectos técnicos en el desarrollo del software que podría ser útil para la investigación además de adaptar una metodología de riesgos muy sencilla y rápida de implementar; Por otra parte, es limitante esta propuesta ya que solo estaría dirigida a gestión de riesgos de información para servicios en la nube y no en general.

3.1.4. AN INTEGRATED CONCEPTUAL MODEL FOR INFORMATION SYSTEM SECURITY RISK MANAGEMENT BY ARCHITECTURE MANAGEMENT

Aubert Jocelyn. Luxembourg Institute of Science and technology, Alemania. 2019

En este artículo, los autores tienen como objetivo desarrollar y valorar un modelo integrado de la gestión de riesgos de la información con aspectos de gestión de arquitectura empresarial relacionando diagramas de casos de uso, diagramas de componentes, modelado de bases de datos entre otros. Esta investigación desarrolla un aspecto más desde el punto de vista del negocio, pero con herramientas tecnológicas y propios del desarrollo del sistema como diagrama UML y estados de procesos. En la figura a continuación se visualiza la propuesta mediante un diagrama conceptual del sistema de gestión de riesgos donde los activos están de color gris, los relacionados a la gestión de riesgos de color blanco y los de color negro relaciona a los conceptos adicionales desde el punto de vista de negocio.

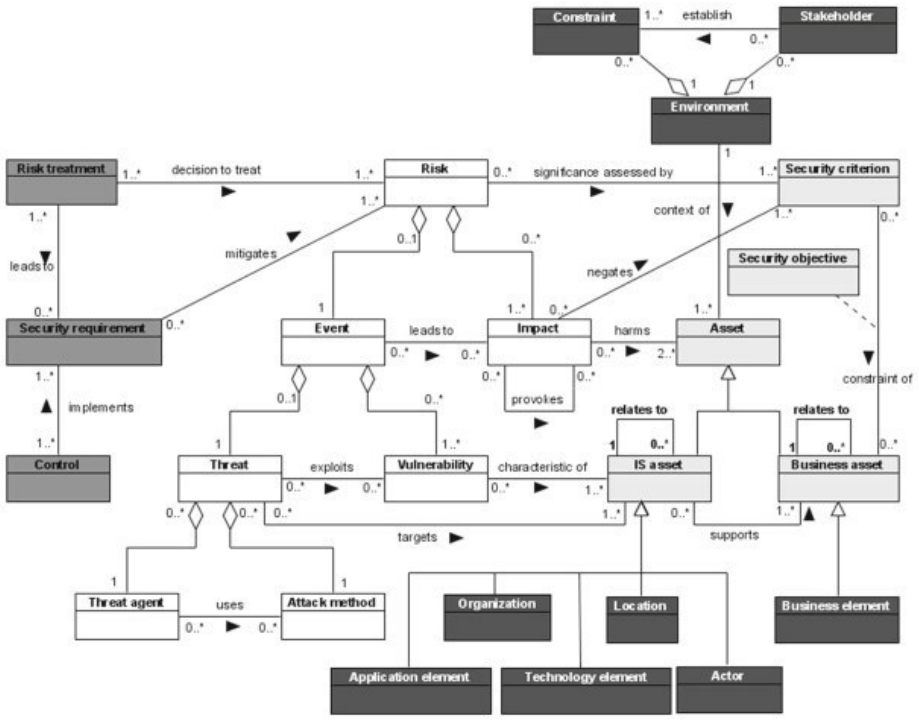

Figura 3.4. Diagrama Integrado conceptual propuesto. Aubert Joselyn, 2019.

En cuanto a la aportación a la investigación, se resalta los diagramas de UML diseñados, el enfoque añadido con el punto de vista del negocio, y aunque no se muestran muchos recursos técnicos que se utilizarían, ayuda más con los diseños y las fuentes de encuestas que tiene como apéndice.

3.1.5. INFORMATION SECURITY RISKS MANAGEMENT FRAMEWORK

Umesh Kumar Singh. Vikram University, India. 2017

En este paper, los autores analizan la importancia de proteger los activos de información de las Universidades, de este modo analiza las posibles amenazas que enfrentan estos activos. Para esto proponen un framework de trabajo de gestión de riesgos de la información mediante 3 fases y cada una de estas diversas actividades.

- Fase 1: Identificar puntos vulnerables. En esta fase también identifica los stakeholders y activos, así como define los requerimientos mínimos aprobatorios de seguridad.
- Fase 2: Priorizar los activos de información de mayor relevancia. Mediante análisis, encuestas de opinión y conversatorios se define aquellos activos más relevantes para la organización.
- Fase 3: Mejorar la seguridad: Se implementarían lo que se llama salvaguardas y gestiona planes en caso de aceptación del riesgo.

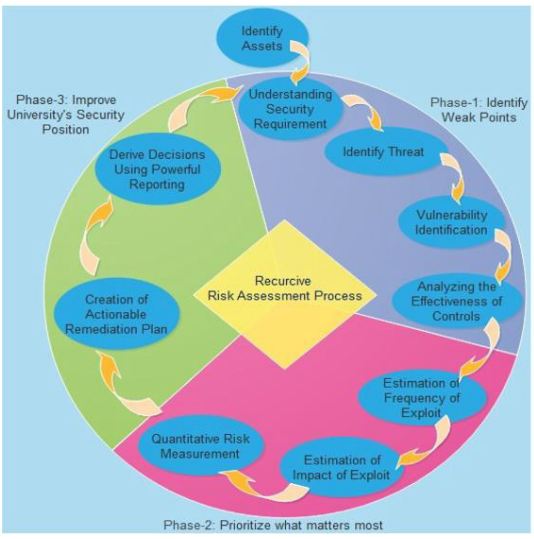

Figura 3.5. Propuesta de Framework para gestión de riesgo de la información. Umesh Singh, 2017.

Como conclusión es una investigación más enfocada al análisis de la red para las Universidades y el modelo propuesto es bastante interesante en lo referente a la agilidad que menciona en su implementación y desarrollo.

3.1.6. METODOLOGÍA PARA LA IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA FAMILIA DE NORMAS ISO/IEC 27000

Valencia-Duque Francisco, Revista Ibérica de Sistemas y Tecnologías de Información, 2017.

En este paper, los autores proponen una metodología para la implementación de un SGSI basándose en las normas ISO/IEC 27000. En base a esto buscan abordar un proyecto de implementación sobre la metodología propuesta siguiendo las buenas prácticas y estándares internacionales.

La metodología que se propone contempla 5 fases secuenciales con sus respectivas etapas y están basadas en la norma ISO/IEC 27001 y se trata de incorporar una serie de elementos prácticos que faciliten la implementación de la misma. Estas fases se detallan en la siguiente tabla.

Tabla 3.1. Fases de metodología para la implementación de un SGSI basado en ISO/IEC 27000. Valencia Francisco, 2017.

Fases	**Descripción**
Fase 1. Obtener la aprobación de la Dirección para iniciar el proyecto	Fase de inicio, comprende las etapas de establecer prioridades para el desarrollo de un SGSI, definir alcance del SGSI, y creación del plan de proyecto a ser aprobado.
Fase 2. Definir el alcance, los límites y la política del SGSI.	En esta fase se centra en la definición de alcance y límites del SGSI y de las tecnologías y comunicaciones disponibles, así como la aprobación de las políticas y definición de roles y responsabilidades para el SGSI.
Fase 3. Realizar el análisis	Dentro de esta fase se inicia el trabajo referido al análisis

de los requisitos de seguridad de la información	en sí de los componentes a evaluar, se deberá definir previamente los requisitos, identificar y definir los activos, así como realizar y detallar su evaluación de acuerdo a varios tipos, características, procesos predefinidos con anterioridad.
Fase 4. Valoración de riesgos y planificar el tratamiento de riesgos.	Es la fase principal dentro del SGSI, dentro de esta fase contempla la preparación de elementos del contexto (políticas, objetivos, parámetros de evaluación de riesgo, alcance). Se establece los parámetros de probabilidad (probabilidad de ocurrencias), parámetros de impacto (niveles de amenazas), se establece la vulnerabilidad y los criterios de aceptación y valoración del riesgo; así como también el tratamiento del riesgo.
Fase 5. Diseñar el SGSI	Esta fase contempla básicamente 3 componentes, la documentación, la implementación de los controles previos al plan de tratamiento de riesgos y el monitoreo de la seguridad de la información.

En este paper se evidencio el aporte en la construcción de un proceso metodológico que surge con el propósito de dar respuesta a una necesidad de desarrollar metodologías ajustadas a los estándares internaciones y en contexto de las organizaciones. Si bien en la metodología que proponen se alinea a los estándares y buenas prácticas, apercepción y objetivo del desarrollo de esta tesis no es una metodología ágil como la que se busca. Tampoco se evidencia alguna implementación real de la misma en alguna institución u organización, ni se muestra alguna tecnología que apoye la implementación de dicha metodología.

3.2 Otras Investigaciones

3.2.1 METODOLOGIA DE SEGURIDAD DE LA INFORMACION PARA LA GESTION DE RIESGO INFORMATICO APLICABLE A MPYMES.

Crespo Martínez Paul. Universidad de Cuenca, Ecuador. 2016

En esta tesis de maestría, el autor revela la importancia de la información como ventaja competitiva en las empresas MPYMES, para esto es necesario la protección de dicha información. El autor propone una metodología de seguridad de la información de gestión de riesgos en MPYMES de Ecuador. Para esto realiza un análisis cualitativo de las principales metodologías existentes como Security Risk Management (Microsoft), Magerit, CRAMM, evalúa su alineación con las normas ISO, y con la realidad de las MPYMES y regulaciones legales ecuatorianas.

1. Parte A: La introducción al manejo de riesgo
2. Parte B: El marco de gestión de riesgo
3. Parte C: El proceso de gestión de riesgo
4. Parte D: Recursos

Figura 3.6. Propuesta Metodológica de Gestión de Riesgo. Crespo Paul, 2016.

Su propuesta metodológica se divide en 4 secciones y forma como un hibrido de las metodologías antes detalladas, cada una la específica a detalle con diversos formularios semejantes a un framework que ayuda a guiar para quien requiera implementar. Como conclusiones hace notar la importancia de tener un plan de continuidad de negocio, y este modelo ayudaría en gran medida a esto.

Esta metodología es no técnica, con diversos modelos de formularios a llenar y considerar para la marcha, pero a criterio personal un poco extensa y no muy ágil para el fin del sector empresarial.

3.2.2 ESTABLECIMIENTO, IMPLEMENTACION, MANTENIMIENTO Y MEJORA DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION, BASADO EN ISO 27001:2013, PARA UNA EMPRESA DE CONSULTORIA DE SOFTWARE.

Santos Llanos Daniel. PUCP, 2016.

En esta tesis, el autor desarrolla un modelo para el Sistema de Gestión de Seguridad de la Información (SGSI), teniendo como referencia el ISO 27001 y los 3 pilares que son integridad, confidencialidad y disponibilidad de la información, y permitiendo que opere bajo el principio de mejora continua. Se centra en las buenas prácticas en general y no solo a la gestión de riesgos, que sería parte del SGSI. No se menciona el uso de herramientas de tecnología para el apoyo del registro del SGSI ni el desarrollo de un software o sistema ad hoc.

En cuanto a sus resultados y conclusiones, el autor hace alusión a la importancia que se da al requerimiento de la Ley de Datos Personales en énfasis de detallar una Autoridad de Protección de datos personales, siendo consecuente con las buenas prácticas documentales del ISO 27001. También concluye que se ha elaborado una propuesta innovadora referente a la metodología de gestión de riesgos, así como normalización de la ruta de planes del SGSI. Una de las recomendaciones del autor implica como sugerencias e investigación a futuro el diseño de una metodología ágil para la elaboración y operación del SGSI, teniendo en cuenta la manera a veces engorrosa de llevar a cabo todas las actividades que exige la normativa.

3.2.3. GESTION DE RIESGOS DE TECNOLOGIAS DE INFORMACION DE LAS EMPRESAS DE NEPHILA NETWORKS

Llontop Diaz Cesar. UCV, 2018

En esta tesis de maestría, el autor propone un modelo para mejorar la eficiencia de la gestión de riesgos de TI en empresas que da soporte Nephila. En su metodología propone 4 fases de estudio, estas adaptadas de “La Gestión de riesgo TI” y la efectividad de los sistemas de información, definido por el autor Celi, Lambayeque, Perú.

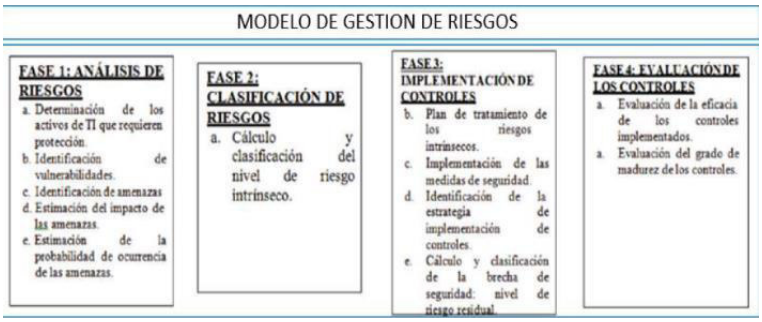

Figura 3.7. Metodología propuesta para análisis de Gestión de riesgo. Llontop Diaz Cesar, 2018.

El modelo propuesto se divide en 4 fases. La primera fase se refiere a todo el análisis de riesgos, la identificación de todos los activos de T.I, las vulnerabilidades, amenazas y estimaciones de impacto. La segunda fase indica la clasificación de los riesgos de manera numérica, con ponderación desde riesgo muy bajo hasta riesgo muy alto. La tercera fase se refiere a la implementación de controles para el tratamiento del riesgo en general. La cuarta fase indica en cuanto a la evaluación de controles, así como la eficacia de estos frente a las salvaguardas implementadas.

Las conclusiones este autor las evaluó de acuerdo a encuestas a los trabajadores de la empresa en mención. El autor consideró que la empresa del estudio tiene un nivel de aceptación y valoración de más 65% por parte de los trabajadores en referente a la gestión de riesgos de T.I. El autor consideró que la empresa del estudio tiene un nivel de aceptación y valoración de más 65% por parte de los trabajadores en referente a la gestión de riesgos de T.I. El autor considera que para empresas comerciales se podría continuar empleándose el modelo de gestión de riesgos debido a los altos índices de buenos resultados en general, pero en empresas de servicios se tendría que reevaluar el modelo añadiendo y modificando algunos parámetros con el fin de adaptarlo mejor al sector empresarial. Identifica también la importancia de políticas de la empresa que mantengan procesos de identificar, priorizar, evaluar, y supervisar los riesgos oportunamente.

3.2.4. SISTEMA PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS.

Cavalcanti Garay Antton. Universidad Ricardo Palma, 2012.

En esta tesis el autor se plantea como objetivo seleccionar o desarrollar alguna herramienta informática para la gestión de riesgos en general; Para esto analiza diversas metodologías de gestión de riesgos existentes seleccionando por comodidad la metodología MAGERIT. También analiza diversos softwares existentes como RISK, Risk Simulator y Cristal Ball, y analiza la factibilidad de adquirir alguno de ellos.

Asimismo, desarrolla la metodología de desarrollo de software RUP mencionando diagramas y requerimientos funcionales a tener en cuenta. Por último, realiza las pruebas del despliegue del software con resultados exitosos y cumpliendo el objetivo propuesto al inicio.

En cuanto al aporte de esta tesis a la presente investigación es relevante porque es muestra un aspecto más técnico, empezando con seleccionar una metodología de gestión de riesgos adecuado a su rubro empresarial y desarrolla el despliegue de un software adecuado con la metodología seleccionada. En cuanto a la metodología de desarrollo de software no se concuerda con utilizar una metodología RUP debido a su extensa documentación y demora en tiempos.

3.2.5. HERRAMIENTA DE SOFTWARE DE APOYO A LA GESTIÓN DE RIESGOS EN PROYECTOS.

Bravo Rojas Andrea. PUCP, 2017.

En esta tesis, la autora se propone como objetivo desarrollar un artefacto de software y que se base en la gestión de riesgos con el fin de reducir la incertidumbre de eventos perjudiciales. Para esto define todo el planeamiento de gestión de riesgos según el PMI, y realiza un análisis comparativo de las herramientas de software existentes en el mercado, entre esas @Risk, Primavera Risk Analisis y Deltek Active Risk Manager. Menciona también los módulos requeridos que deberán estar incluidos en el software a desarrollar. En el desarrollo del software realiza el análisis y diseño según la metodología RUP, listando así requerimientos funcionales, actores del negocio, diagramas de base datos, de componentes, etc. Como conclusiones dispone que se logró implementar la herramienta de software y se llegó al análisis cuantitativo y cualitativo de la gestión de riesgos.

El aporte de esta tesis es alto debido a que brinda más recursos técnicos de los cuales pueden ser beneficiosos para la investigación, aunque la metodología en el desarrollo y despliegue de la herramienta es no ágil por lo que demoraría más el proyecto del mismo.

3.2.6. MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL E-GOBIERNO

Mercado Rojas Joel. UNMSM, 2016.

Esta tesis de maestría, se realiza un análisis de diversos modelos existentes y propuestos asignados a la gestión de seguridad de la información, incluyendo la gestión de riesgos dentro de esta. El autor propone un modelo extenso relacionado más a la gestión pública. Cuando se aborda el subtema de gestión de riesgos se toma como controles y con una metodología genérica que incluye el inventario de activos de la información, valoración de sus activos, análisis y evaluación de riesgos, y una planificación de tratamiento de riesgos; generando así lo controles dentro de su modelo mayor de gestión de la seguridad. Esta tesis es de un enfoque más al modelo teórico de una gestión completa de la seguridad de la información, por lo tanto, no tan aplicable para la investigación actual.

3.3 Modelos de Gestión de Riesgos de Seguridad de la Información

3.3.1 Magerit

El Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) ha sido elaborada por el consejo director de administración electrónica (CSAE) del gobierno español, como una solución al concepto de que la Administración, y, en general, toda la sociedad, necesitan de manera cada vez más progresiva de las tecnologías de la información para concretar sus objetivos. El motivo de esta metodología está estrechamente relacionado con la globalización del empleo de las tecnologías de la información, que se evidencia para los ciudadanos; aunque a la vez está expuesto a algunos riesgos, de los cuales requieren que sea minimizado el impacto a fin de brindar confianza.

Según el Portal de Administración electrónica de España (2013), indica que la metodología MAGERIT puede brindar apoyo a todos los trabajadores que se relacionan directamente con información digital y sistemas informáticos. En caso de que la información o los servicios que brindan, se consideran valiosos, MAGERIT facilita conocer el valor cuantificable que se está operando y apoya a protegerlo y salvaguardarlo. Es muy relevante e imprescindible conocer el riesgo al que se encuentran sometidos los componente o elementos de trabajo con el fin de poder manejar una gestión optima de los mismos. Asimismo, con la aplicación y uso de MAGERIT se busca una aproximación metódica que no deje opción a la improvisación, ni dependa de la arbitrariedad o subjetividad del analista.

La versión actual de esta metodología es la versión 3.0 y consta de 3 volúmenes:

- Volumen I – Método: Comprende 8 capítulos y 6 apéndice.
  - Capítulo I: Fase introductoria
  - Capítulo II: Visión de conjunto.
  - Capítulo III: Método de análisis de Riesgos.
  - Capítulo IV: Proceso de Gestión de Riesgos.
  - Capítulo V: Proyecto de Análisis de Riesgos
  - Capítulo VI: Plan de Seguridad.
  - Capítulo VII: Desarrollo de sistemas de Información.
  - Capítulo VIII: Consejos prácticos y recomendaciones.
- Volumen II – Catalogo de Elementos: Este volumen tiene el objetivo de simplificar y agilizar las tareas de las personas involucradas en el proyecto, con el fin de ofrecer elementos estándar para que puedan adoptar con familiaridad y forma rápida. También promueve una nomenclatura y aspectos uniformes que permitan relacionar e integrar el análisis de distintos equipos.
- Volumen III – Guía de Técnicas: En este volumen se describen algunas técnicas empleadas en el análisis y gestión de riesgos, algunas técnicas son análisis mediante tablas, análisis algorítmico, análisis coste beneficio, entre otros.

En cuanto al análisis y gestión posterior del riesgo, MAGERIT comprende los siguientes procesos y actividades para su correcto desarrollo:

A. Identificación y valoración de los activos de información: Para este proceso, según Crespo & Cordero (2016), la ISO sugiere identificar, analizar y clasificar los activos (Ejm: hardware y software) teniendo en cuenta aspectos de su valor, sensibilidad, importancia y criticidad para las organizaciones. Se guía de la metodología que contiene cuadros de clasificación, tipificación y tasación de los activos de información.
B. Identificación y valoración de las amenazas: Se refiere a identificar las amenazas que pudiera afectar a cada activo. Las amenazas son las "cosas que ocurren" y afectan a los activos causándoles daños cuantificables. Contiene cuadros de apoyo para evaluar su clasificación determinadamente.
C. Cálculo del riesgo: Se determina la magnitud y tamaño del probable daño a un sistema. Una vez de conocido el impacto de las amenazas sobre los activos, se deberá derivar el riesgo teniendo cuenta la probabilidad de ocurrencia.
D. Identificación de las contramedidas: Se refiere a las actividades o mecanismos tecnológicos que ayudan a reducir el riesgo. Dependiendo del caso de cada amenaza se podría accionar simplemente organizándose adecuadamente, en cambio hay otras que requerirán factores técnicos (programas o equipos), otra seguridad física y, no se debe de olvidar de la política de personal.
E. Cálculo del riesgo residual: Luego de desplegarse todas las salvaguardas necesarias, aun quedaría un riesgo menos al q se le denomina riesgo residual. Se infiere que se ha modificado el riesgo, de un valor potencial a un valor residual.

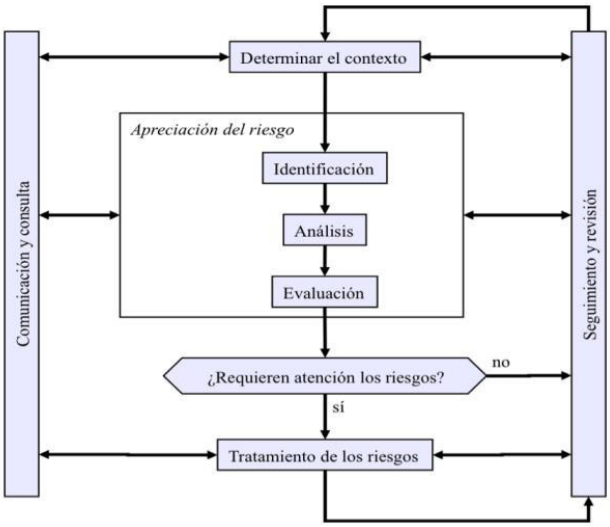

Figura 3.8. Procesos de la Gestión de Riesgos. Recuperado de: "Magerit v3 , Libro I", por Ministerio de Hacienda de España, 2012.

3.3.2 Octave – S

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) es una metodología de análisis de riesgos creada por la Universidad Carnegie Mellon a principios del 2001. En esta metodología se analizan los riesgos basándose en 3 principios Confidencialidad, Integridad y Disponibilidad, y es utilizada por diversas agencias gubernamentales, así como el Departamento de defensa de Estados Unidos.

Según Ana y John A. (2013), La metodología OCTAVE ayuda con la evaluación de los riesgos de seguridad de la información y plantea una planificación de mitigación de los mismos dentro de la organización. Aporta, a partir del equilibrio de factores de riesgos operativos, prácticas de seguridad y tecnología, a que los entes empresariales puedan tomar decisiones de protección de información sobre la base de los fundamentos de la seguridad de la información.

Existen 3 versiones de la metodología:

- OCTAVE: versión general
- OCTAVE - S: Versión para pequeñas empresas.
- OCTAVE – Allegro: Herramienta de la Versión simplificada

Para la versión OCTAVE -S es requerido un grupo corto, recomendado de entre 3 y 5 colaboradores quienes comprendan y se comprometan en la amplitud y profundidad de la organización. En esta versión no se detalla los conceptos o conocimiento, sino que empieza con el desarrollo de talleres con el fin de captar toda la información posible de los elementos relevantes, los requerimientos de seguridad, las amenazas y las prácticas de seguridad, además que incorpora una inspección limitada sobre la infraestructura informática.

La metodología OCTAVE se constituye de 3 fases que se detalla brevemente a continuación.

- Fase I – Construir perfiles de amenaza de activos: Se refiere a las evaluaciones que se realizan en la empresa, para esto primero se desarrollan los distintos perfiles activo-amenaza, inventariando los activos más apreciados, de la misma manera sus amenazas y otros requisitos como imperativos legales, los cuales podrían impactar negativamente a los activos, las cuestiones de seguridad implementadas en los activos y las debilidades a nivel de la organización.
- Fase II – Identificar las vulnerabilidades en la infraestructura: En esta fase se tiene como primer objetivo determinar las vulnerabilidades tecnológicas, las cuales al ejecutarse sin autorización tendrían impactos negativos en los activos críticos, para esto se deberá evaluar puntualmente los artefactos organizacionales. Esta fase da como resultado un listado resumido de componentes clave (vinculados directamente con los activos críticos).
- Fase III - Desarrollar el plan y estrategia de seguridad: Se refiere a la creación y ejecución de la mitigación práctica basada en la política de protección y riesgo, planeamiento para amparar la misión de la organización y las preferencias tácticas.

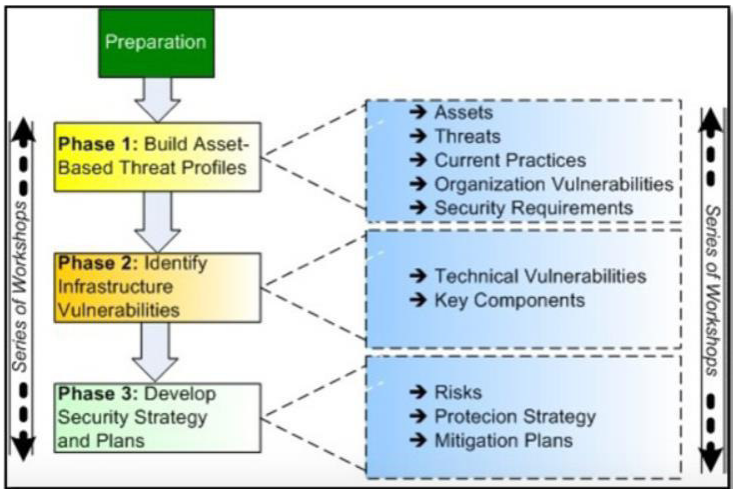

Figura 3.9. Fases de Metodología OCTAVE. Recuperado de: "Security at Work- Metodologías de Riesgos II", por Antonio Huerta, 2012.

.

3.3.3 CRAMM

CCTARisk Analysis and Management Method (CRAMM) es una metodología de análisis de riesgos desarrollado por el Centro de informática y la Agencia Nacional de Telecomunicaciones (CCTA) del gobierno del Reino Unido. Su versión inicial se publicó en 1987, y la versión actual es la 5.

Según Yazar (2012), CRAMM tiene la facilidad de poder desplegar en casi todo tipo de sistemas y redes de información y también se puede desplegar en todas las fases del ciclo de vida del sistema de información, empezando desde la planificación hasta la viabilidad, mediante el reforzamiento e implementación de este. Si se requiere conocer y medir la seguridad y medidas que tiene de respaldo los sistemas de información o una red, entonces es óptimo utilizar CRAMM ya que esta desarrollado para dicho motivo.

CRAMM proporciona un enfoque amplio y organizado que consta de componentes técnicas y no técnicas. Con respecto a la evaluación de estos componentes, se divide en 3 etapas.

- Identificación y Valoración de Activos: Esta primera etapa recoge la definición global de los objetivos de seguridad, como los que se encuentra la definición del alcance, la identificación y evaluación de los activos físicos y software relacionados, la estimación objetiva del valor de los datos referentes a impacto en el negocio y sus características.
- Amenazas y evaluación de la vulnerabilidad: Para la segunda etapa ya se ha analizado la magnitud de los posibles potenciales problemas, ahora se necesita calcular la probabilidad que estos problemas vayan a producirse. Algunas de las amenazas predefinidas por CRAMM son la piratería, virus, daños intencionales, error humano, fallo de hardware o software, entre otros.
- Identificación y selección de contramedidas: Se identifica y selecciona algunas de entre las diversas medidas de seguridad aplicadas por la organización, para luego obtener el riesgo residual. Una característica adicional de CRAMM es que proporciona en su librería una gran cantidad de medidas de seguridad.

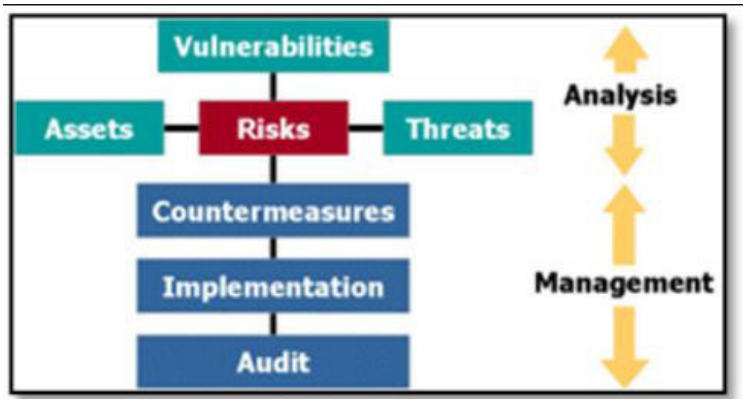

Figura 3.10. Etapas de Metodología CRAMM. Recuperado de: "Security at Work- Metodologías de Riesgos I", por Antonio Huerta, 2012.

3.3.4 Metodología de Gestión de Riesgos de Seguridad de la Información – Oficina de Tecnología de la Información – Ministerio de Economía y Finanzas.

En el año 2016, el Ministerio de Economía y Finanzas de Perú aprueba mediante decreto supremo y Resolución Ministerial una metodología de gestión de riesgos de seguridad de

la información, la cual será aplicada y desarrollada en todo el ministerio y servirá de guía a otros ministerios.

Según la misma resolución 120-2016-EF, esta metodología surgió con el objetivo de: "Establecer y describir criterios, prácticas y procedimientos para la adecuada gestión de riesgos y oportunidades relacionadas con la seguridad de la información en el Ministerio."

Esta metodología tiene similitud en estructura con la metodología MAGERIT, pero con un aspecto más ágil y rápido de implementar comparada con está, al solo desarrollar en su propuesto los principales procesos. Su proceso metodológico se resume en la figura 3.8, donde además se visualiza las fases y actividades que se implementan.

Proceso	Fases	Actividades
Gestión de Riesgos	Preparación	Parametrización
	Valoración	Inventario de Activos
		Análisis de Riesgos
		Evaluación de Riesgos
	Tratamiento	Tratamiento de Riesgos

Figura 3.11. Proceso Metodológico MEF Perú. Recuperado de: "Metodología de Gestión de Riesgos de S.I.", por Ministerio de Economía y Finanzas - Perú, 2016.

- **Fase1.** Preparación: En esta fase se centra en la preparación previa a la evaluación de riesgos. Esta preparación previa incluye la parametrización de características como el nivel de aceptación que tendrá los riesgos, y bajo qué criterios serán aceptados. Estas parametrizaciones se acordarán aplicar en una valoración numérica definida por los dueños del negocio.
- **Fase2.** Valoración: Dentro de esta segunda fase realiza el inventariado y evaluación de los activos de acuerdo a las características preconfiguradas de los activos de información. Para la segunda actividad de esta fase se ejecuta el análisis de riesgos, para esto se identifica los tipos de amenazas por cada activo y se evalúa sus controles existentes. En la última actividad se evalúa mediante puntuación los riesgos más elevados y no permitidos obteniéndose la matriz de riesgos que determina qué riesgos deberán ser tratados.

- **Fase3**. Tratamiento: Luego de obtener la puntuación de cada riesgo se identifica si este riesgo puede ser tolerable o necesita ser tratado, para esto se mide de acuerdo a un nivel mínimo tolerable. Para los riesgos altos, se deberá implementar una propuesta y un plan de tratamiento. También se da el caso de implementar la gestión de oportunidades de acuerdo al análisis del entorno externo e interno que pueda impactar de manera positiva a la institución o empresa.

3.4 Software existente para Gestión de riesgos

Dentro de los objetivos de esta investigación es proponer y desarrollar un software que se base en la gestión de riesgos, para esto se analizara algunas herramientas informáticas que se halla disponibles en el mercado para evaluar su integración o adoptación de este. Para esto se debe tener en cuenta el contexto de la empresa a aplicar; la factibilidad, flexibilidad y escalabilidad son aspectos importantes para el mismo.
En esta sección se hará uso de un cuadro comparativo para evaluar las distintas herramientas informáticas que existen en el mercado, las cualidades a evaluar serán entre características funcionales y técnicas.

- Open source: “Código abierto”. Es una característica del software que tiene una licencia que visualizar, utilizar, modificar, realizar mejoras al código fuente del programa o aplicación; independientemente del usuario final. Esta característica es muy relevante para poder utilizar un software base de desarrollo a fin de reducir el tiempo de codificación y sobre todo los costos del proyecto.
- Free software: Es un tipo software que se distribuye libremente y sin costo económico, pero tiene limitantes de copyright, de esta forma no se puede modificar o utilizar libremente, en comparación con el software libre.
- Software modular: Se refiere a aquel software que contienen una gestión modular, es decir que sean capaces de configurar mediante módulos, y cada uno de ellos destinado a cubrir alguna característica determinada y que podemos añadir, quitar, o incluso hasta modificar sus funcionalidades de acuerdo a la necesidad organizacional.

- Aplicación Móvil: Se refiere a que una parte o un módulo del software se pueda ejecutar mediante una aplicación informática destinada a smartphones.
- Integración: Se refiere a la facilidad de integrar el software con algunas otras herramientas como MS Excel, MS Project, etc.
- Diseño Responsive: : Involucra una técnica de diseño web que tiene como fin ofrecer una visualización de una misma página en distintos dispositivos de manera correcta y sin pérdida de información. Los elementos del sistema deben ser redimensionados de tal manera que se adapten al ancho de cada dispositivo con el objetivo de una correcta visualización y mejor experiencia de usuario.
- Metodología: Algunos de los softwares son asociadas especialmente a alguna metodología especifica.

En la tabla 3.3 se visualiza un cuadro comparativo de algunos de los mas representativos softwares existentes en el mercado entre privado y comercial. Se analiza y compara algunas características principales de lo cual se concluye que solo uno es escalable y de código abierto, y que también solo uno tiene una aplicación móvil como herramienta interactiva y de apoyo al sistema. Así, si bien el software comercial del mercado puede cumplir algunos requisitos básicos, no cumple con todas las interacciones y actividades que se propone en esta investigación, por lo cual es necesario desarrollar una aplicación ad hoc a lo requerido.

Tabla 3.2. Cuadro Comparativo de Software existentes. Elaboración Propia.

Software Característica	PILAR	SimpleRisk	@RISK	ISO TOOLS 27001	Global Suite
Descripción	Ofrece 4 distintas versiones dependiendo la organización	Ofrece versión básica gratuita y versiones PRO, de pago	Herramienta automatiza y adapta al Excel	Software especializado para cumplimiento del ISO 27001	Facilita la automatización y gestión de la norma ISO 27001 para optimización del SGSI
Desarrollado por	Centro Criptológico Nacional - España	Simplerisk Llc	Palisade	ISOTools	Global Suite EIRL
Metodología	Magerit	-	-	ISO 27001	ISO 27001
Open Source	No	Si	No	No	No
Free Software	Si	Si	No	No	No
Software modular	No	Si	No	Si	Si
Integración	-	-	M.S Excel, M.S Project	-	Excel
Escalabilidad	No	Si	No	No	No
Responsive	No	Si	No	Si	No
Tipo Versión	Aplicación de escritorio	Web	Herramienta plugin a MS Ofiice	Web	Web
App Mobile	No	No	No	Si	No

Idioma	Español	Ingles / español	Ingles / español	Ingles / español	Español
Matriz de Riesgos	Si	Si	Si	Si	Si
Gestión de usuarios	Si	Si	No	Si	No
Análisis cualitativo	Si	Si	No	Si	No
Gestión de alertas	No	Si (Versión pro)	No	No	Si
Gestión Reportes	No	Si	No	Si	Si
Gestión Evaluación	No	No	No	No	Si

CAPÍTULO IV

APORTE PRÁCTICO

4.1 Estructura Funcional de la Plataforma Web y móvil

Luego de seleccionar el modelo de gestión de riesgos a implementar, se ha analizado y determinado que la estructura funcional del sistema a desarrollar estará compuesta con distintos módulos para su mejor control y desempeño funcional, algunas características de dichos módulos son los siguientes:

- Tamaño pequeño: Para facilitar el impacto cuando se realice alguna modificación de tipo correctivo, optimización, o ampliación.
- Independencia: Permitirá la flexibilidad al trabajar en el desarrollo de un módulo independiente del resto, no se necesita conocer detalles técnicos de los otros módulos.

Tabla 4.1 Secciones propuestos para el desarrollo del Software. Elaboración Propia.

Fases	Sección	Descripción
Parametrizaciones	Gestión Usuarios	Administra y controla las definiciones correctas de los usuarios para que el usuario autorizado acceda en el momento adecuado a una información correspondiente.
	Atributos Activos	Gestiona los atributos o características principales que se le asignan a los activos de información
	Atributos Amenazas	Gestiona los atributos o características correspondientes a las amenazas identificadas.
	Nivel de Riesgos	Gestiona los niveles de riesgo aceptados, así como también la escala de calificaciones en las evaluaciones.
Valoración Riesgos	Gestión Activos	Primera fase operativa de la metodología de gestión, engloba tareas de identificación, inventariado y categorización de activos de la información. También se incluye la valoración de los activos por parte de los custodios y usuarios.
	Análisis Amenazas	Categoriza las amenazas identificadas por cada uno de los activos, así como su nivel de

		impacto, estimación de vulnerabilidad y ocurrencia dentro del negocio de la organización
	Gestión Riesgos	Engloba el proceso core de la metodología, en el cual se evalúa el impacto según la amenaza por cada activo, también obtiene el nivel de exposición al riesgo, así como la matriz grafica de riesgos.
Tratamiento Riesgos	Gestión Tratamiento	Se desarrolla el tratamiento respectivo sobre los riesgos altos, se identifica por nivel de aceptabilidad y opciones a tomar (transfiere, mitiga, acepta, evita)
	Oportunidad de Mejora	Se propone y evalúa posibles mejoras a implementar con el fin de fortalecer algún aspecto de la empresa.
Gestión de Proyectos	Seguimiento de Proyectos	Se desarrolla el registro y seguimiento básico de proyectos planteados como consecuencias a la gestión de tratamientos para reducir riesgos u oportunidades de mejora.
Soporte complementario	Gestión Reportes	Permitirá seleccionar, clasificar y sintetizar la data registrada en la BD mediante gráficos de acuerdo con los parámetros de elección solicitados. Además, permitirá exportar dichos informes en formatos XLS y PDF.
	Gestión Notificaciones	Se podrá realizar varias operaciones para una notificación automática del sistema como crear, visualizar, actualizar y borrar una notificación vía mail corporativo.
	Plataforma Móvil	Aplicación móvil sincronizada con el sistema. Se presentará el despliegue de algunas funcionalidades requeridas del sistema para usuarios específicos que requieran

4.2 Procesos del Negocio

Una vez seleccionada la metodología de gestión de riesgos a desarrollar por el software, se procede a identificar todos los procesos involucrados a este fin. Se ha desarrollado el workflow que se debería seguir, este será el modelo de proceso de negocio que se codificara en el software. En la figura 4.1 se presenta el diagrama de procesos BPMN principal que describirá los pasos y secuencia del proceso de gestión de riesgos de la información a aplicar a la consultora de sistemas. Este diagrama está en una visualización de alto nivel, ya que algunos procesos se encuentran encapsulados. En la figura 4.2 se

visualiza el subproceso de Configuración de parametrizaciones, necesario para iniciar el proyecto con lineamientos regulados. El diagrama cuenta con subprocesos de Inventariar Activos, Gestionar amenazas y evaluación Riesgos.

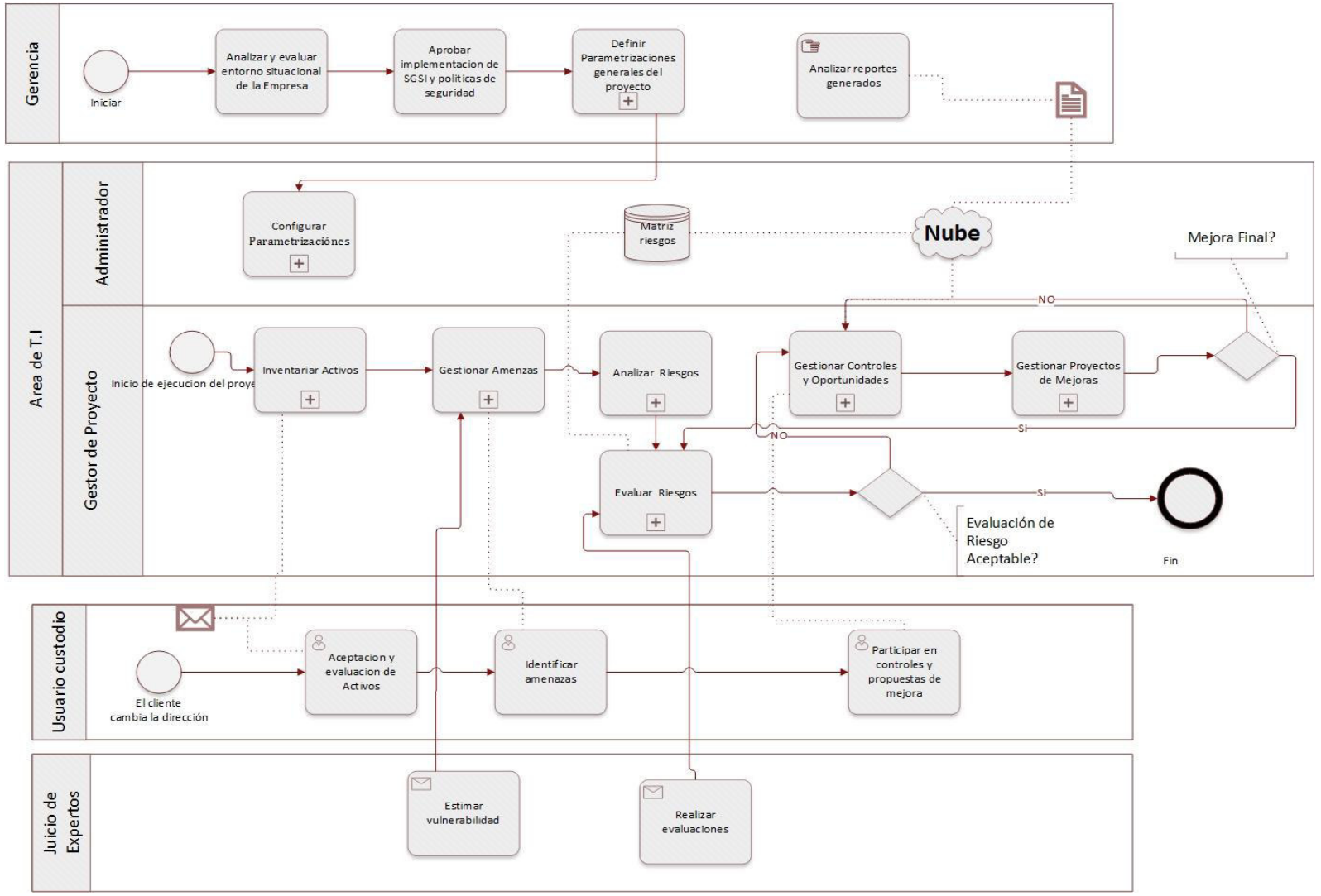

Figura 4.1. Diagrama de procesos BPMN para GSI. Elaboración Propia

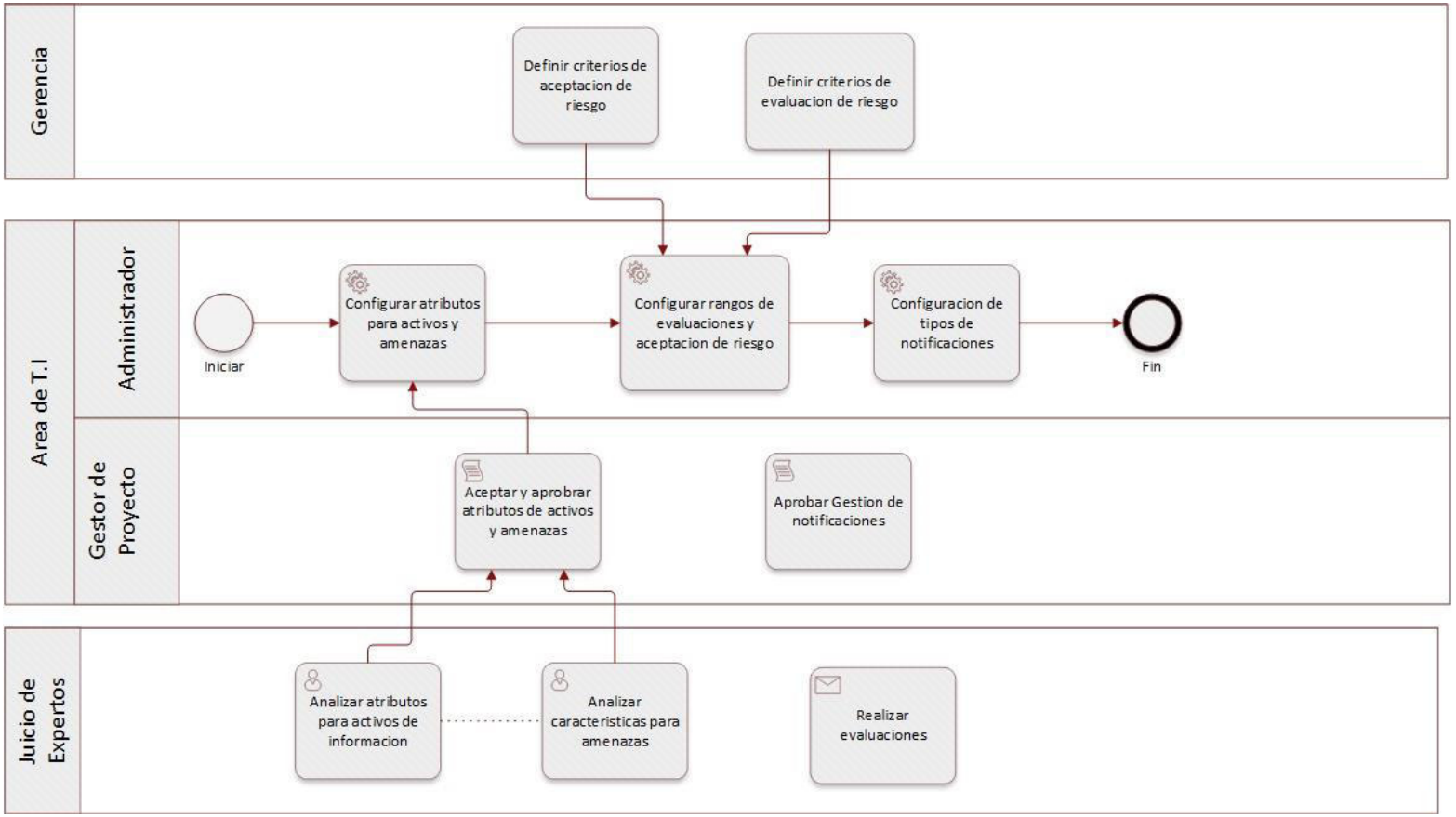

Figura 4.2. Diagrama BPMN – Subproceso Parametrizaciones. Elaboración Propia

4.3 Prototipo del Software

Según Salazar Emma (2012), define los prototipos de software como "…un mapa, esquema, dibujo, ejemplar, código o artefacto, una muestra de un proceso, producto o servicio, que será utilizado como parte del sistema para ilustrar ciertos aspectos de su vista, las funcionalidades y clarificar los requerimientos. Un prototipo llegar a ser una representación de un sistema, ya que posee las características del sistema, sin que ello signifique su operatividad total."

Se diseñó los prototipos del software a desarrollar a fin de sustentar visualmente a la consultoría de sistemas la usabilidad, la interacción y el flujo funcional de las aplicaciones propuestas.

En la figura 4.3 se muestra el diseño del prototipo que refleja uno de los procesos principales de la aplicación móvil.

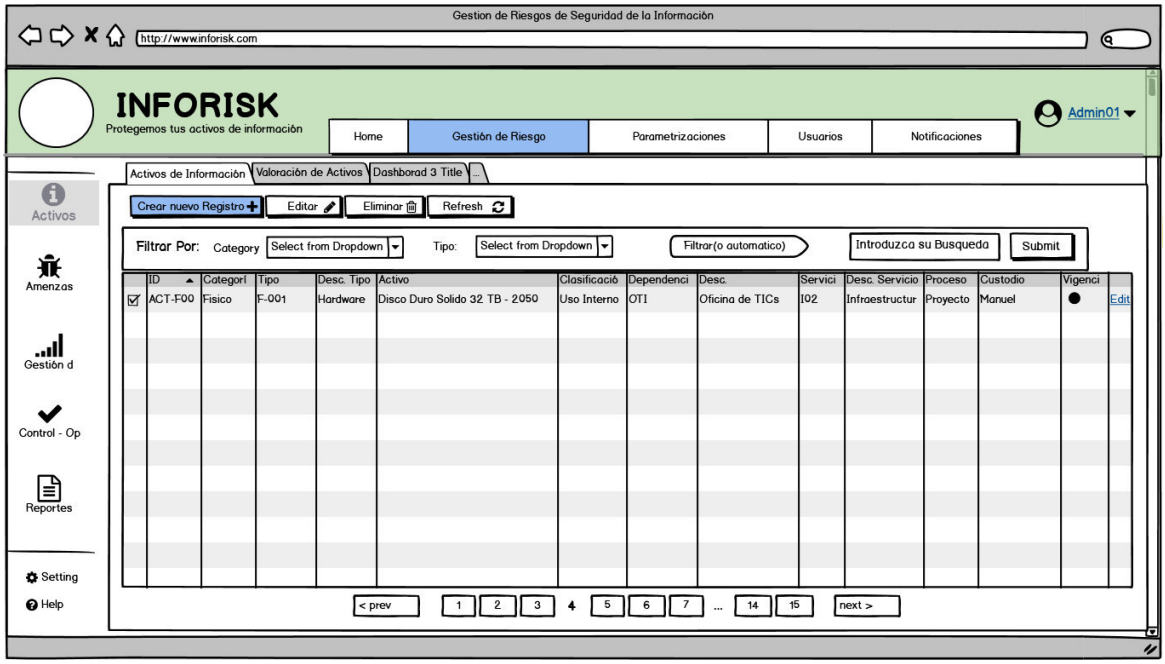

Figura 4.3. Prototipo vista Activos 1. Elaboración propia

4.4 Arquitectura del Software

Las aplicaciones web y móvil planteadas se desarrollan bajo las tecnologías mostradas en la figura 4.4. El patrón de arquitectura utilizado es el modelo, vista, controlador para la aplicación web. Para la base de datos se utiliza MYSQL, y se desarrollara la programación en PHP con ZendFramework.

La aplicación móvil se plantea desarrollar en Android con versión igual o mayor a 4.5. El desarrollo es completamente nativo y consumirá los servicios web implementados para enviar y recibir información mediante peticiones.

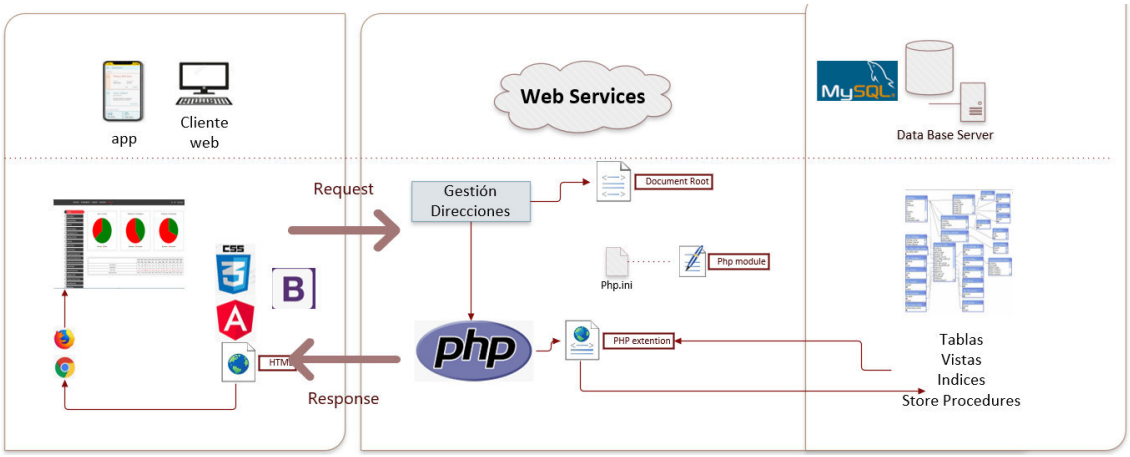

Figura 4.4. Arquitectura de software. Elaboración propia

Diagrama de Despliegue

A continuación, en la figura 4.5, se muestra el diagrama de despliegue desarrollado para el sistema INFORISK. Para el nodo de Cliente Web, este empaquetado el navegador web que es empleado por el usuario final, este se muestra mediante interfaz gráfica en HTML. En el nodo Cliente Móvil, se empaqueta la aplicación móvil desarrollada en Android, la cual tiene las operaciones básicas implementadas. Para el nodo Servidor Web, se encuentra el empaquetado del programa que se encarga de ejecutar las distintas operaciones de procesamiento solicitadas por el usuario. En el nodo de Servidor de aplicaciones se encapsula los servicios web, en total 8, empleados para los

procedimientos para el acceso y obtención de data a la base de datos. En el nodo Servidor de Base de Datos, se ejecutan las consultas solicitadas por el servidor de aplicaciones, en este caso se emplea MYSQL Server.

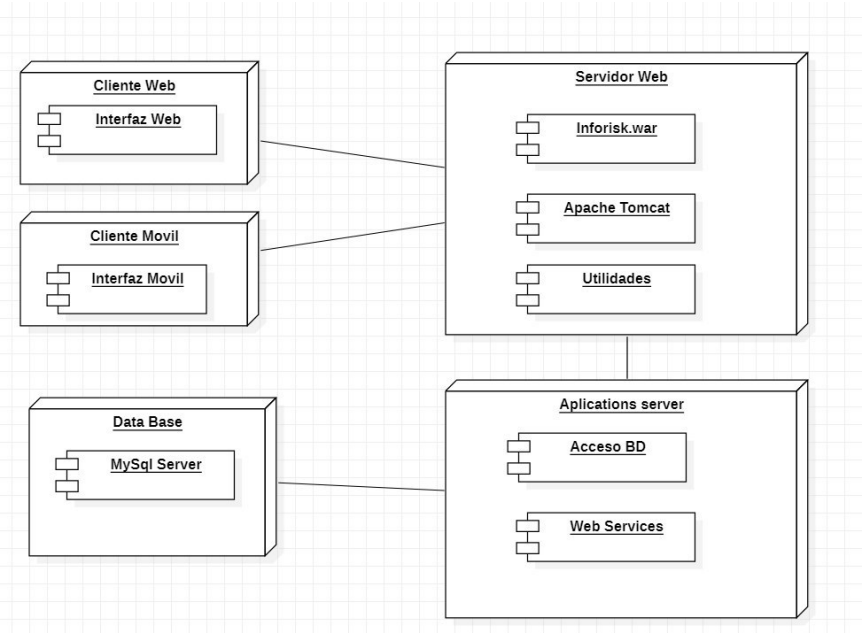

Figura 4.5. Diagrama de Despliegue. Elaboración propia

4.5 Metodología para el Desarrollo de Software.

Debido al dinamismo en las definiciones de los requisitos y al tiempo y recursos limitados para la implementación y despliegue, se ha elegido adoptar una estrategia incremental para el desarrollo del software planteado, por lo tanto, se selecciona una metodología de desarrollo ágil. Dentro de la experiencia del autor, la metodología de desarrollo ágil SCRUM será la que se empleará en el desarrollo del proyecto.

Según Luis Goncalves (2019), define SCRUM como una estructura en la que distintos colaboradores pueden abordar problemas adaptativos, siendo continuamente productivos y creativos para poder entregar productos de gran valor. La metodología SCRUM está fundada sobre la teoría empírica de control de procesos, lo que se refiere a que el conocimiento está basado nen la toma de decisiones y en las experiencias de factores

conocidos. Debido a esto en SCRUM se busca la manera de optimizar las tareas usando un método iterativo e incremental, y basado en 3 pilares fundamentales.

- Transparencia: El proceso en general necesita ser visible hacia los responsables de resultados.
- Inspección: Se requiere que de manera periódica se inspeccione los instrumentos scrum utilizados en las tareas.
- Adaptación: Tener la capacidad de adaptar de manera efectiva y eficiente diversos cambios y/o ampliaciones que se den en el desarrollo del proyecto

4.5.1 Roles de SCRUM.

En scrum el equipo de trabajo se define como auto organizados y multi funcionales, garantizando entrega de valor agregado en cada interacción o entregable del proyecto. Existen 3 roles:

- Product Owner: Es el responsable de rentabilizar y optimizar los recursos con el fin de entregar mayor el valor del producto o proyecto que esté llevando a cabo. Asimismo, coordina e interacciona regularmente con el cliente por lo que debe tener conocimiento sobre el negocio. Dentro de sus principales responsabilidades está gestionar el backlog del producto optimizando el valor de trabajo que realiza el equipo de desarrollo.
- Scrum Master: Es el responsable que la metodología SCRUM sea entendido y aplicado de manera correcta y efectiva en la organización. Se le considera un líder encargado de eliminar impedimentos y/o inconvenientes que se presenten durante la ejecución de un sprint. Colabora de la mano con el producto owner.
- Equipo de desarrollo: Es un equipo multifuncional y auto organizado, compuesto por profesionales, quienes son los encargados de realizar las tareas priorizadas por el product owner. Son los delegados de estimar las tareas del producto backlog y de su desarrollo. Es un equipo lineal, por lo que no existen jerarquías o especialistas dentro de este, para transmitir responsabilidad compartida.

4.5.2 Eventos SCRUM

Los eventos de scrum regulan y minimizan la necesidad de tener que llevar a cabo reuniones no planificadas, estos eventos son de tiempo limitado y garantizan que se gaste el mínimo de tiempo posible en los procesos.

- Sprint: Es la tarea principal de Scrum siendo el contenedor de los demás eventos, se recomienda sprints cortos, con duración máxima de 30 días.
- Sprint Planning: Es la reunión que se hace para el sprint, todo el equipo define qué tareas se van a realizar y el objetivo del sprint. Se responden preguntas como ¿Qué se va hacer en el sprint?, y ¿Cómo lo vamos a hacer?
- Daily meeting: Se refiere a la reunión diaria dentro del sprint, el cual no debe superar los 15 minutos de duración. Se reúne todo el equipo de desarrollo y e responden preguntas básicas como, ¿Qué hice ayer?, ¿Qué hare hoy?
- Retrospectiva: Es el ultimo evento de scrum por cada sprint, es la reunión del equipo en la que se evalúa e inspecciona como se está implementando scrum, y revisa el sprint.

4.5.3 Artefactos SCRUM

- Product Backlog: Es el listado de tareas que define todo el proyecto. Este listado cuenta con la estimación de recursos y tiempo, así como descripción y prioridad. Su gestión es total responsabilidad del producto owner.
- Sprint Backlog: Es la agrupación de tareas que se realizaran por el equipo de desarrollo durante un sprint.

En la figura 4.6 se muestran gráficamente los procesos de SCRUM adaptados al presente proyecto, cada sprint se ha definido con una duración media de 2 semanas con incrementales diarios. El Product backlog y los sprint se desarrollarán los siguientes puntos.

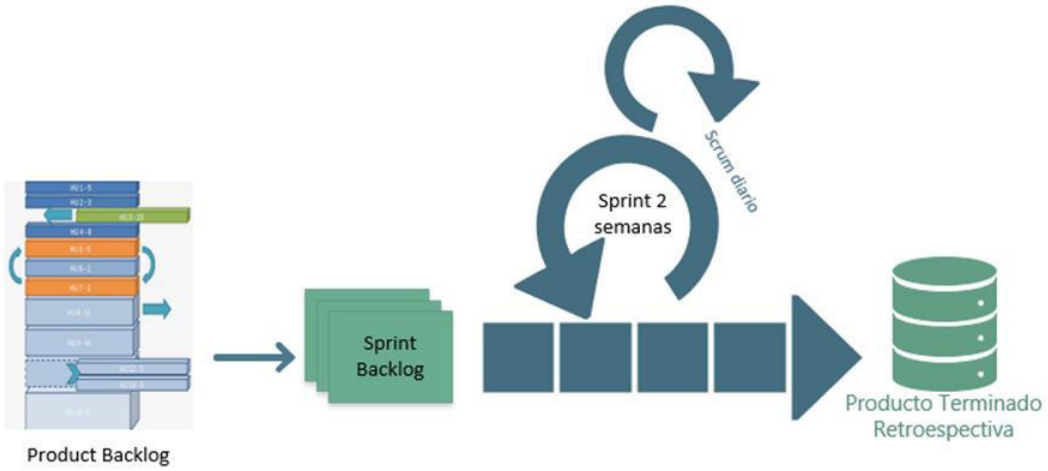

Figura 4.6. Procesos Adaptados de SCRUM. Elaboración propia

En las siguientes secciones del capítulo se ejecutará, detallará y documentará las tareas relacionadas al desarrollo del software, debido a que se ha aplicado el uso de la metodología ágil Scrum, se tiene detallada las historias de usuario en el producto backlog y cada desarrollo de tareas está comprendido en iteraciones o sprints.

4.6 Product Backlog

Tabla 4.2 Product backlog. Elaboración Propia.

Scrum - Fase 1: Qué hacer			
ID Historia	**Historia**	**Prioridad**	**Sprint**
H01	Como usuario Administrador quiero poder ingresar sesión en la plataforma web y móvil	Media	1
H02	Como usuario administrador quiero gestionar accesos y roles a distintos tipos de usuarios	Alta	2
H03	Como usuario administrador quiero poder gestionar las parametrizaciones de atributos de Activos de información	Alta	3
H04	Como usuario gestor de proyecto quiero poder gestionar los activos de información	Media	3
H05	Como usuario gestor de proyecto quiero poder asignar y aprobar la evaluación de los activos a su custodio o a un responsable	Media	3
H06	Como usuario custodio debo poder realizar la evaluación de los criterios a los activos que me asignaron	Media	3

H07	Como usuario gestor de proyecto quiero poder asignar categorías y tipos de amenazas a cada activo de información	Media	4
H08	Como usuario gestor de proyecto quiero poder realizar la estimación de la vulnerabilidad	Media	4
H09	Como usuario gestor de proyectos quiero poder visualizar la probabilidad de ocurrencia para las amenazas	Alta	5
H10	Como usuario gestor de proyectos quiero poder gestionar evaluación del impacto de los riesgos	Alta	5
H11	Como usuario gestor de proyectos quiero poder gestionar el nivel de exposición a los riesgos	Alta	5
H12	Como usuario gestor de proyectos quiero poder gestionar el tratamiento de los riesgos	Media	6
H13	Como usuario gestor de proyectos quiero poder gestionar las oportunidades de desarrollo	Media	6
H14	Como usuario gestor de proyecto o gerencia quiero poder visualizar los reportes de la gestión de riesgos	Media	7
H15	Como usuario custodio quiero poder visualizar mis activos asignados y su evaluación de riesgo	Baja	7
H16	Como usuario gestor proyectos, administrador, custodio, Gerencia, quiero poder buscar por palabras clave sobre los activos, amenazas y riesgos registrados en la BD.	Baja	8
H17	Como usuario Administrador, Gestor de Proyecto quiero poder editar el envío de emails genéricos a los usuarios y evaluadores	Baja	8

4.7 SPRINTS

4.7.1 Sprint n° 1

En la tabla 4.3 se visualiza la pila del primer sprint que se ha desarrollado. Se empieza mapeando modelo de base de datos para las entidades identificadas como Activo, categoría activos, amenazas, tipos amenaza, grupos amenaza, vulnerabilidad, etc. Este modelo de base de datos es el pilar para el desarrollo de la aplicación web y móvil. Se visualiza el detalle del modelo relacional de base de datos en los anexos.

Luego se procede a imprentar la base de datos y realizar las configuraciones respectivas y creación del proyecto para el desarrollo de la aplicación web y móvil, cabe destacar que se sigue el diagrama de arquitectura de software detallada en el capítulo anterior.

Para el desarrollo donde la funcionalidad de una historia de usuario implique un diseño de interfaz gráfica se tomará en lo posible como guía los prototipos en mockups diseñados y aprobados con anterioridad.

Por último, para este primer sprint se realiza el flujo lógico para el control de inicio de sesiones, así como la configuración técnica del web service que consumirá en el aplicativo móvil.

Tabla 4.3 Sprint 1: Sprint Backlog. Elaboración Propia.

ID	Historia Usuario	Tarea	Tiempo estimado (Días)	Tiempo Real (Días)	Proceso
H01. T01	Como usuario Administrador quiero poder ingresar sesión en la plataforma web y móvil	Desarrollar el modelo de base relacional sobre el cual se ejecutará el sistema.	1	1	Web Y móvil
H01. T02		Implementar la base de datos relación, crear tablas, entidades y realizar configuraciones generales de la base de datos.	2	1	
H01. T04		Diseñar interfaz de ingreso de sesión de usuarios	0.5	0.5	
H01. T05		Configurar la plataforma para los servicios web a implementar	2	3	
H01. T06		Desarrollar funcionalidad de inicio de sesión	0.5	0.5	
H01. T07		Validar y testear inicio de sesiones	0.5	0.5	

Resultados del Sprint

Dentro de este primer sprint se encuentra la tarea de desarrollar e implementar el modelo de base de datos a utilizar en el proyecto. En la figura 4.7 se visualiza el modelo de base de datos, cabe mencionar que con un fin visual se muestra solo las tablas y conexiones principales, así como los atributos.

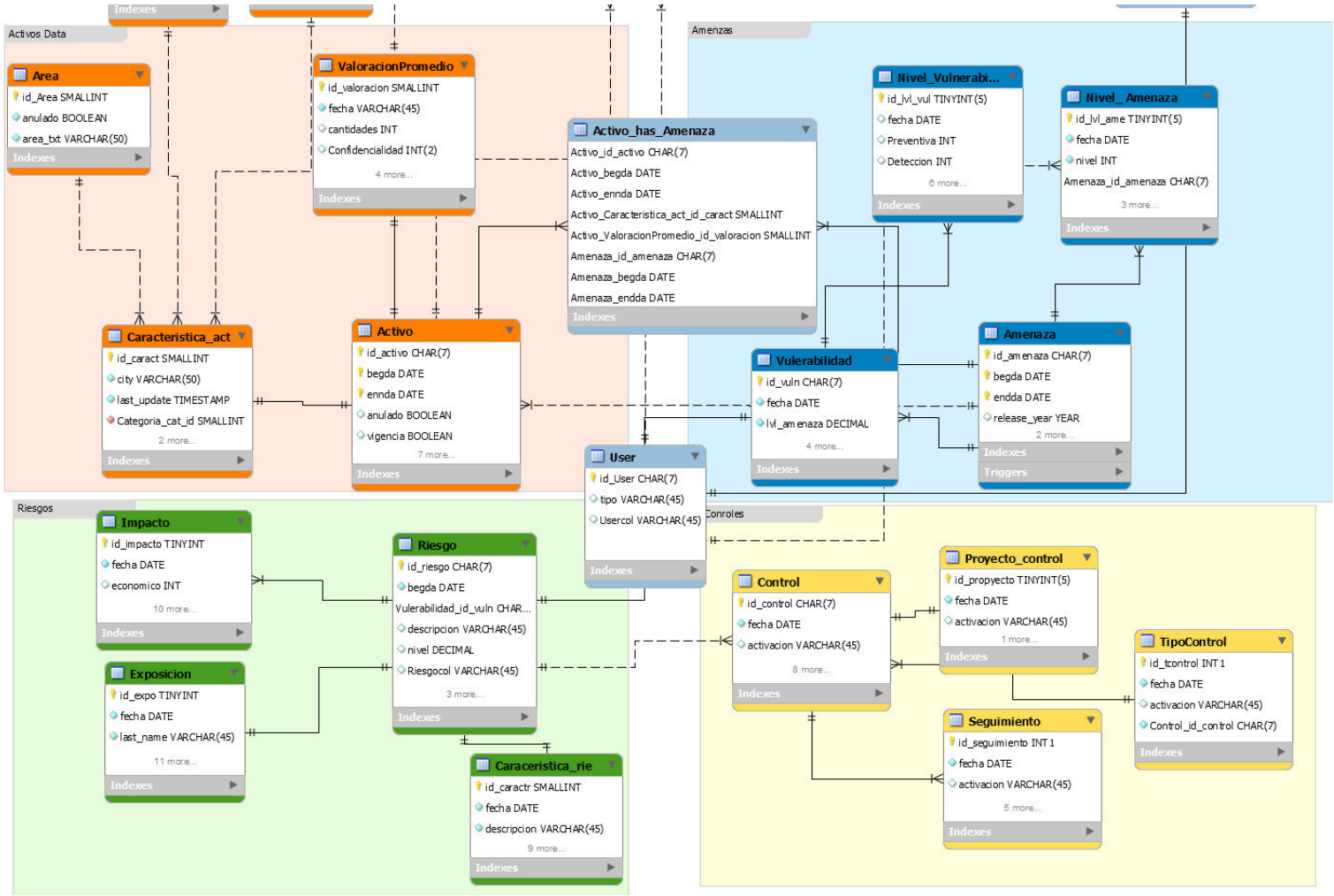

Figura 4.7. Modelo de Base de Datos. Elaboración propia

a. Web

La primera pantalla para ingreso al sistema muestra el logotipo de la aplicación y los datos acceso, así como una opción en caso el usuario olvide su contraseña o correo electrónico asociado. Para iniciar sesión se solicita los siguientes datos.

- Email o nombre de usuario
- Contraseña de usuario

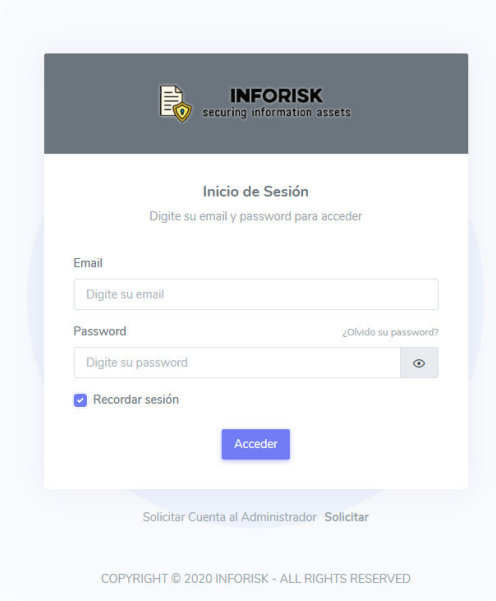

Figura 4.8. Pantalla de Inicio de Sesión. Elaboración propia

Luego de iniciada la sesión de manera exitosa, se debe mostrar la pantalla principal, las opciones en el menú o en la barra horizontal varían de acuerdo al tipo de usuario que se loguea. Dentro de la pantalla principal se muestra algunos términos y definiciones puntuales sobre la gestión de riesgos, también en la opción de Metodología se visualiza de manera gráfica un resumen sobre la metodología a utilizar a fin de servir de guía a los usuarios.

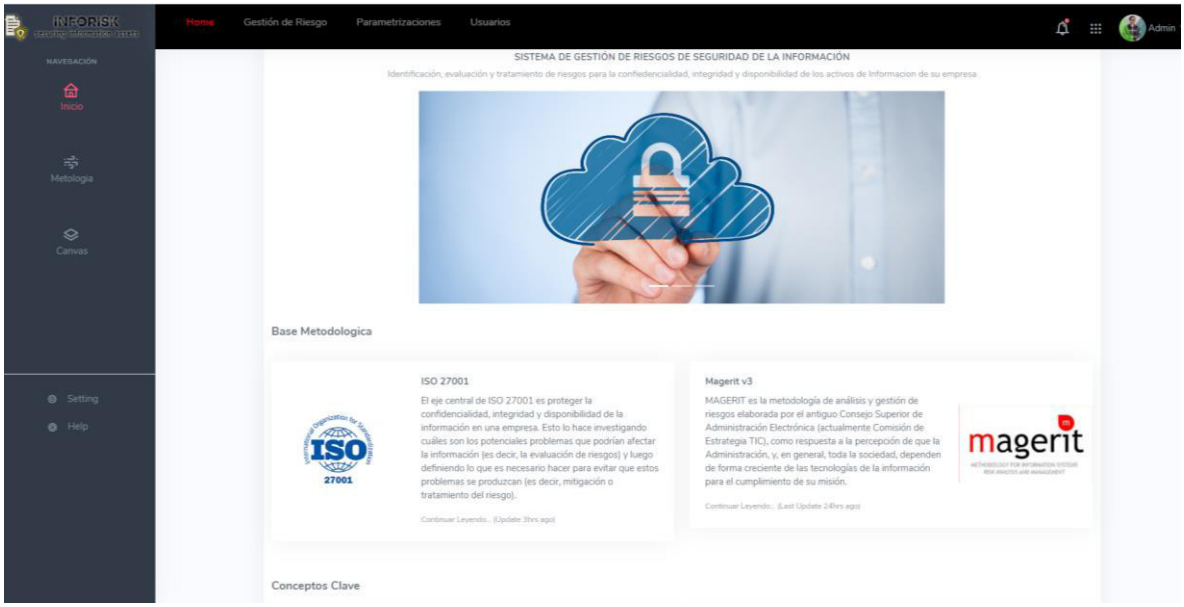

Figura 4.9. Pantalla de Inicio. Elaboración propia

b. Móvil

En primera pantalla para el aplicativo móvil, se muestra el logo, y lo datos de usuario y clave para iniciar sesión, así como opción “olvide mi contraseña”. Una vez iniciada sesión muestra la pantalla inicial, la cual contiene algunos accesos rápidos para registro de activos, reportes, evaluaciones; también se muestra un apartado con las bases metodológicas a tener en cuenta. En la siguiente pantalla se muestra el menú principal con las opciones de Gestionar Activos, Gestión Amenazas, Gestión Riesgos, Control y Reportes. Cada uno se desarrollará en los siguientes Sprint.

Figura 4.10. Pantalla móvil de Inicio de sesión. Elaboración propia

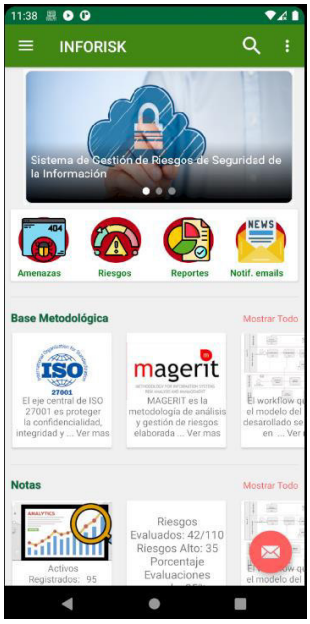

Figura 4.11. Pantalla móvil de Inicio. Elaboración propia

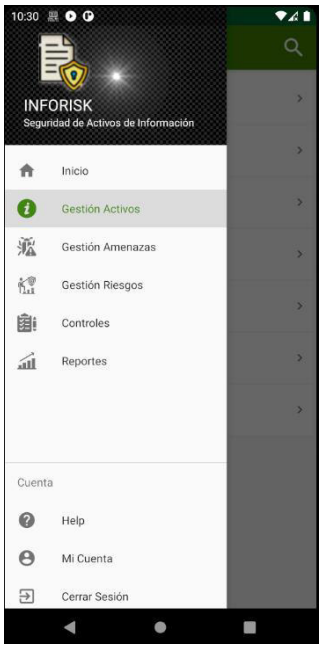

Figura 4.12. Pantalla móvil de menú principal. Elaboración propia

4.7.2 Sprint n° 2

La pila del segundo sprint se detalla en la tabla 4.4. En esta iteración se ha centrado en realizar las funcionalidades relacionado a la gestión de accesos, roles e identificación de usuarios, para esto se define que solo el usuario Administrador podrá añadir, eliminar, editar accesos de usuarios. Esta funcionalidad se limita solo a la aplicación web, debido a que no se encuentra dentro de las operaciones vitales de del producto y no sería tan recurrente.

Tabla 4.4 Sprint 2: Sprint Backlog. Elaboración Propia.

ID	Historia Usuario	Tarea	Tiempo estimado (Días)	Tiempo Real (Días)	Proceso
H02. T01	Como usuario administrador quiero gestionar accesos y roles a distintos tipos de usuarios	Diseñar interfaz gráfica para crear, editar y eliminar roles a usuarios de la aplicación	2	1	Web
H02. T02		Desarrollar la funcionalidad lógica para crear, editar y eliminar roles de usuarios (programación backend)	0.5	1	

H02. T03		Testear la funcionalidad de gestión de accesos y roles	0.5	0.5	

Resultados del Sprint

a. Web

El administrador puede crear y gestionar usuarios, además de consultar en auditoria las modificaciones que los distintos tipos de usuarios han realizado en el proyecto. La interfaz se visualiza en la siguiente figura. En el proyecto se ha definido 4 tipos de usuario:

- Administrador
- Gestor de Proyecto
- Usuario Experto
- Usuario Custodio

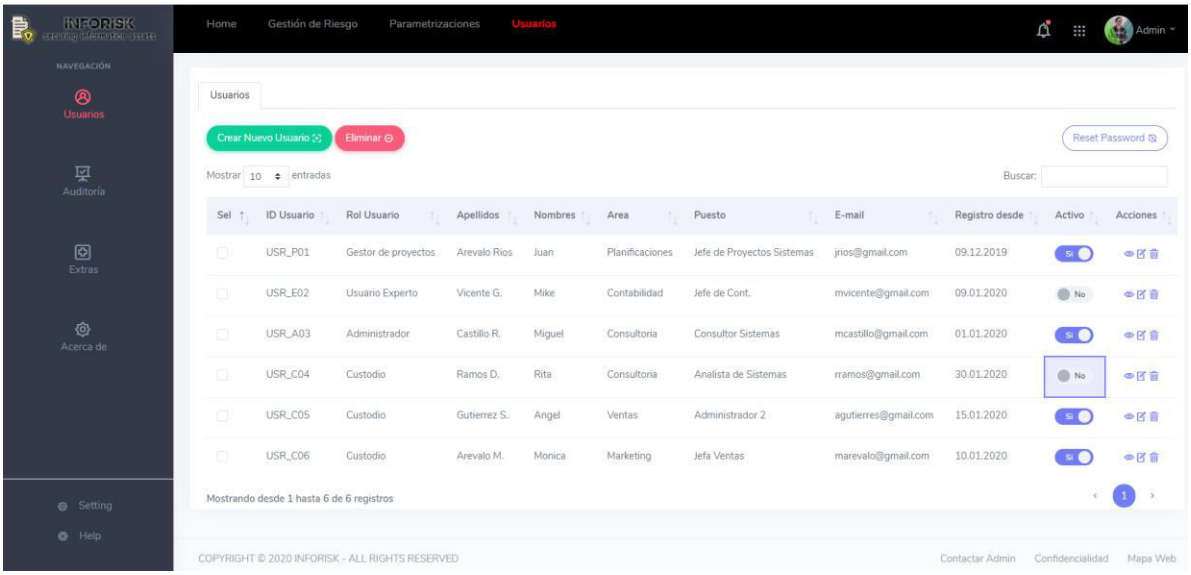

Figura 4.13. Pantalla de Gestión Usuarios. Elaboración propia

4.7.3 Sprint n° 3

La pila del tercer sprint se detalla en la tabla 4.5. En este sprint se empieza a desarrolla el primer módulo del aplicativo, que trata sobre la gestión de activos de información. Primero se programa la funcionalidad para realizar las parametrizaciones referentes a la gestión de activos de información, Estas son los listados de categorías, proyecto, tipo de

activo, clasificación y servicio, que se mostrara al editar cada activo. Estas configuraciones de parametrización están asociadas solo al usuario Administrador y, al no ser una funcionalidad recurrente, se ejecutará solo por aplicación web.

En las siguientes historias de usuario se centra en las funcionalidades de realizar el registro y edición de los activos de información. Cada modificación por parte del usuario se quedará grabado en el historial de cambios que también se muestra en la pantalla.

Para la asignación de un usuario custodio a un activo de información, se registrará mediante la misma interfaz de edición de activos, asimismo el usuario deberá estar registrado previamente en el sistema por el administrador. Las notificaciones de cada asignación a su usuario custodio se dará vía email, para lo cual también se programa y configura estas funcionalidades.

Por último, se programa la funcionalidad para poder registrar y editar las evaluaciones de cada activo de información, de acuerdo al tipo de usuario podrán evaluar solo su activo asignado, o en caso de usuario gestor de proyecto, podrá realizar la evaluación de cualquier activo.

Tabla 4.5 Sprint 3: Sprint Backlog. Elaboración Propia.

ID	Historia Usuario	Tarea	Tiempo estimado (Días)	Tiempo Real (Días)	Proceso
H03. T01	Como usuario administrador quiero poder gestionar las parametrizaciones de atributos de Activos de información	Diseñar interfaz gráfica para configuración de categorías de Activos	0.5	0.5	Web
H03. T02		Desarrollar funcionalidad y lógica para gestión de categorías de activos	1	1	
H03. T03		Validar funcionalidad en BD.	0.5	0.25	
H04. T01	Como usuario gestor de proyecto quiero poder gestionar los activos de información	Diseñar interfaz gráfica para crear, editar y eliminar activos de información	0.25	0.5	Web y móvil
H04. T02		Desarrollo de actividades para gestión de activos en móvil.	1	0.5	
H04 T03		Desarrollo integral para crear, modificar, eliminar y asignar usuarios a los activos de información	2	2.5	

H04. T04		Testear funcionalidades de registros de archivos competentes en la B.D	0.5	0.5	
H05. T01	Como usuario gestor de proyecto quiero poder asignar y aprobar la evaluación de los activos a su custodio o a un responsable	Diseñar interfaz gráfica de asignación y aprobación para las evaluaciones, diseño cuerpo y contenido de emails	0.25	0.25	Web
H05. T02		Desarrollar configuraciones parametrizables de envió de emails.	0.5	1	
H05. T03		Configurar plataforma para envío de e-mails	2.5	3.5	
H05. T04		Desarrollar lógica para editar y asignar activos a su responsable (backend)	2	1.5	
H05. T05		Testear funcionalidades de envío de email y lógica programable	0.5	0.5	
H06. T01	Como usuario custodio debo poder realizar la evaluación de los criterios a los activos que me asignaron	Diseñar interfaz gráfica de evaluación de activos acorde a categorías	0.5	0.5	Web y móvil
H07. T02		Analizar y codificar requerimiento funcional para generar evaluaciones de activos	2	2	
H06. T03		Testear funcionalidades de evaluación.	0.5	0.5	

Resultados del Sprint

a. Web

Se implementa la sección de Parametrizaciones para que el usuario gestor de proyecto pueda modificar distintos atributos de activos de información, estos son: Categoría de activos, tipo de activo, clasificación, servicio y dependencia. Cada uno de estos atributos de activos, tienen a su vez un código único, un nombre y una descripción. Se listan mediante grillas y permiten añadir, editar y eliminar cada registro.

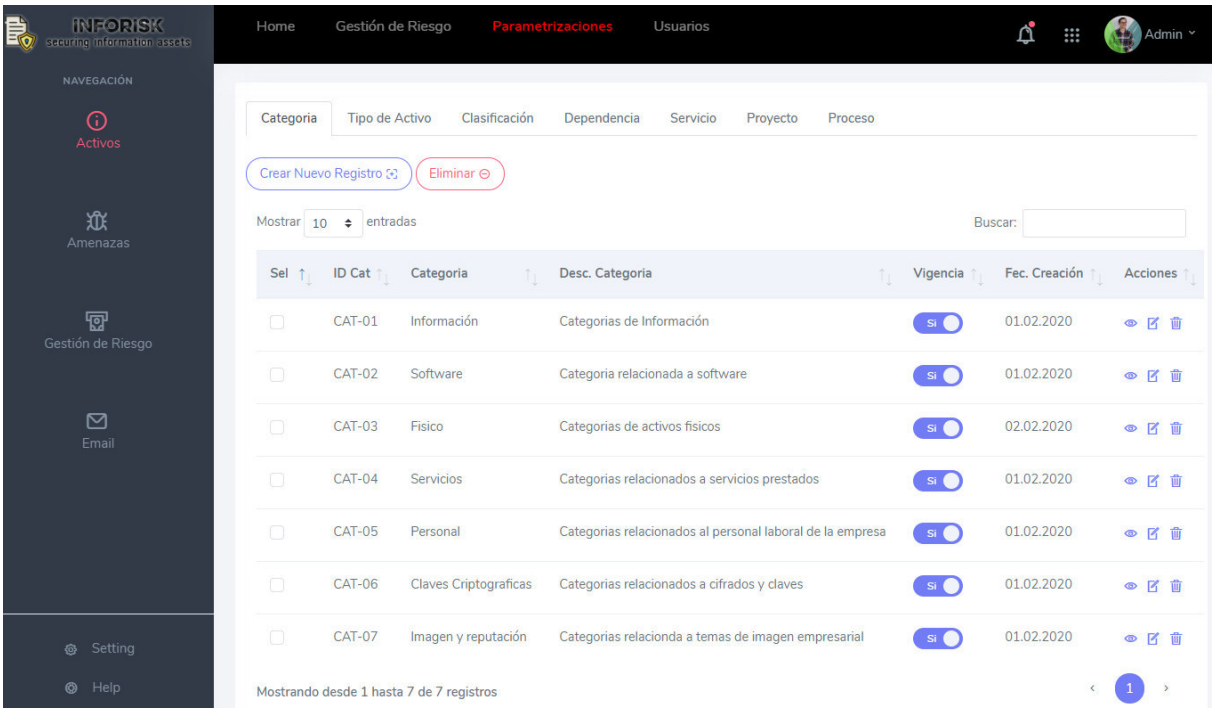

Figura 4.14. Pantalla de Parametrizaciones de Activos. Elaboración propia

En la figura 4.15 se visualiza en una tabla el listado de activos de información, y en esta tabla de datos maestros se visualizan sus atributos principales. En la parte superior se añade botones con las opciones de añadir registros, editar, eliminar y refrescar.

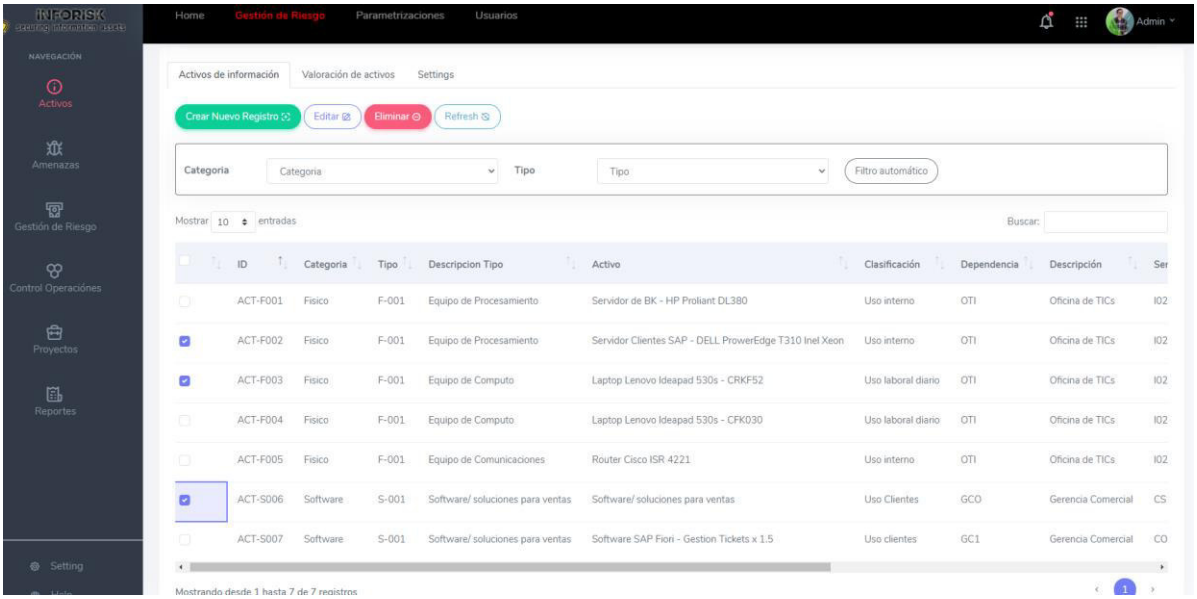

Figura 4.15. Pantalla de Gestión de Activos. Elaboración propia

Al dar clic en la opción añadir o crear nuevo registro se visualiza otra interfaz, con todos los datos a completar para un activo de información, así como la asignación de propietario y custodio del activo en modificación. Ver figura 4.16.

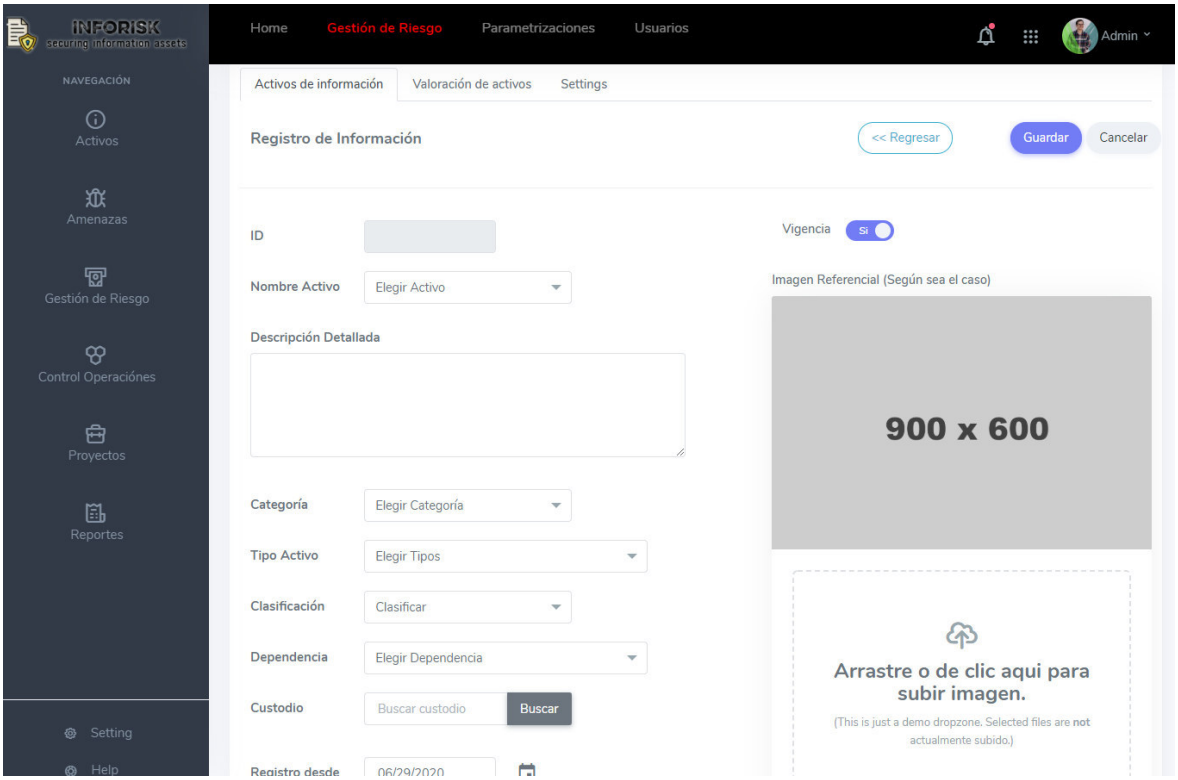

Figura 4.16. Pantalla de Registro de Activos. Elaboración propia

En la figura 4.17 se observa una tabla de activos con principales atributos y con las evaluaciones respectivas, también tiene un botón en la parte superior para notificar a los usuarios custodios sobre la evaluación de su activo y de esta manera se envía un email notificando al usuario. Para la evaluación se muestra en la figura 4.18 la manera que pueden evaluar los activos de información, mediante puntuación interactiva.

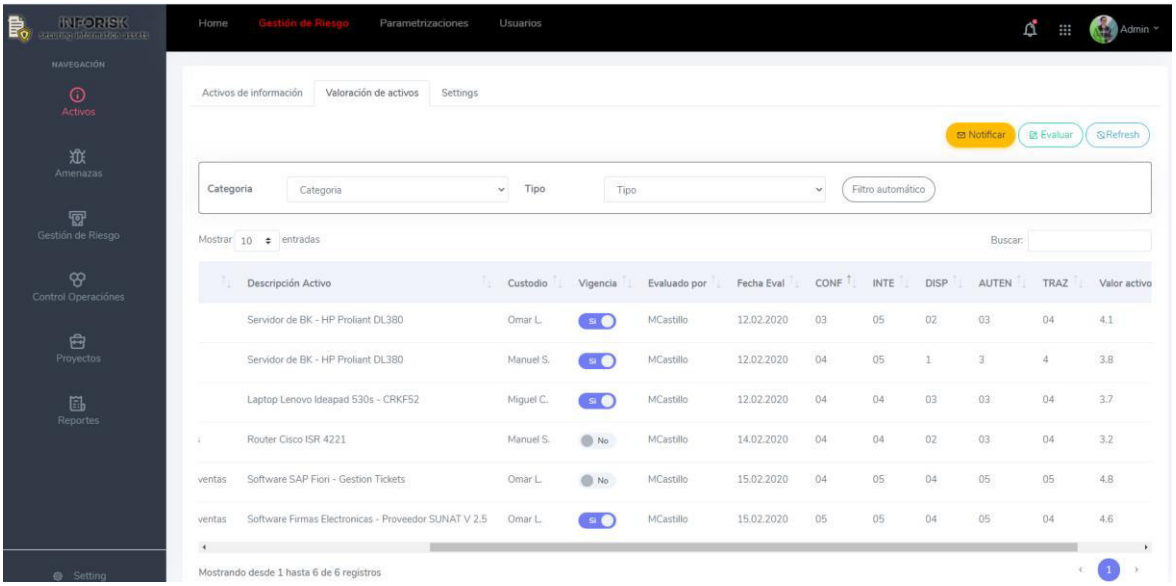

Figura 4.17. Pantalla de Activos y evaluaciones. Elaboración propia

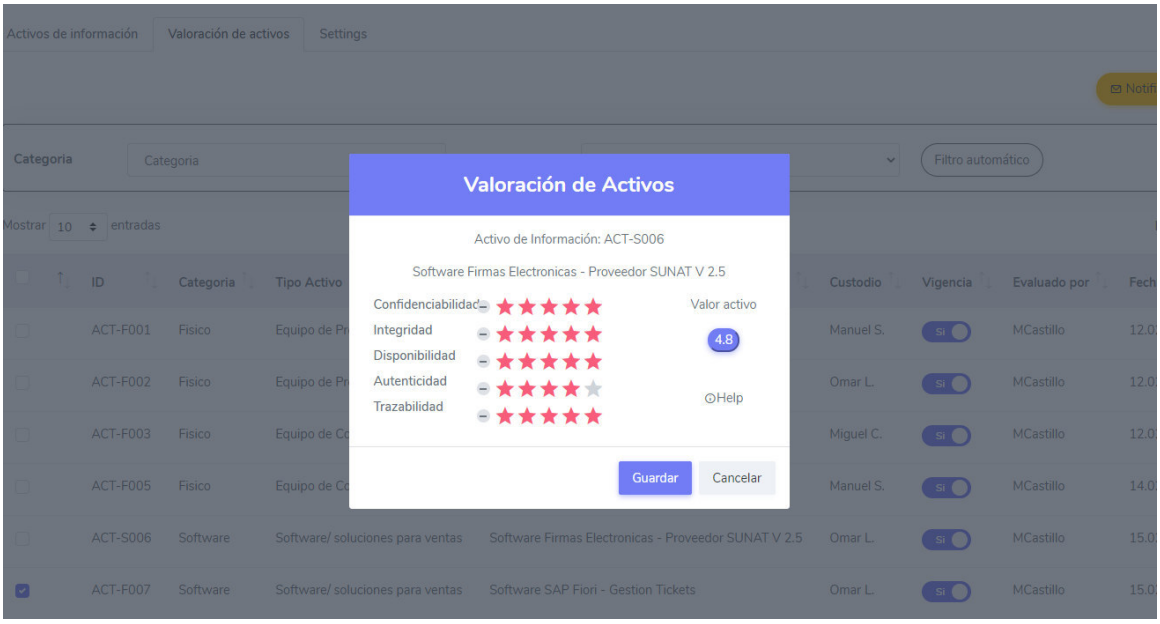

Figura 4.18. Pantalla de Valoración de Activos. Elaboración propia

b. Móvil

Para la aplicación móvil se ha considerado que tengan las funcionalidades que el aplicativo en de editar los activos de información y evaluar. En la figura 4.19 se muestra las opciones disponibles para la gestión de activos, dentro de las cuales están añadir, listar, evaluar y notificar activos.

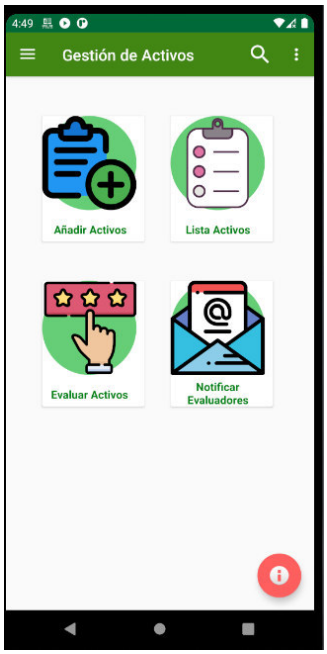

Figura 4.19. Pantalla móvil de Gestión de Activos. Elaboración propia

En la siguiente figura se visualiza la opción de registro de activos de información, para esta versión móvil permite añadir imágenes tomadas mediante el uso de recursos de cámara, así también como añadir archivos. En la figura 4.20 se puede visualizar el listado de activos con la opción a editar y mediante el desplegable, la opción de notificar a sus evaluadores.

Figura 4.20. Pantalla móvil de Registrar Activos. Elaboración propia

Figura 4.21. Pantalla móvil de Listado de Activos. Elaboración propia

4.7.4 Sprint n° 4

La pila del cuarto sprint se detalla en la tabla 4.6. En este sprint se desarrolla las funcionalidades principales para la gestión de amenazas. Se añade la interfaz de parametrizaciones para las categorías y tipos de amenazas.

En la aplicación web y móvil se añade el listado en tablas de los activos de información para poder añadir y/o editar amenazas identificadas, así como sus vulnerabilidades. Por último, se puede añadir la estimación de la vulnerabilidad identificada mediante 3 criterios, de acuerdo a la metodología implementada, que son:

- Capacidad de controles preventivos
- Capacidad de detección
- Capacidad de controles de corrección.

Luego de la evaluación, el sistema realiza un procedimiento interno para calcular el nivel de vulnerabilidad según la fórmula:

$$Nivel\ de\ vulnerablidad = 6 - \frac{\sum_1^n(\text{Cap. Preventiva} + \text{Cap. Deteccion} + \text{Cap. correcion})}{3n}$$

Luego del registro de la evaluación de vulnerabilidad, el sistema realiza un cálculo de la probabilidad de ocurrencia por cada amenaza identificada a cada activo. Estos registros se muestran en una tabla de actualización y consultas.

$$Probabilidad\ de\ Ocurrencia = Nivel\ de\ Vulnerabilidad * Nivel\ de\ Amenaza$$

Tabla 4.6 Sprint 4: Sprint Backlog. Elaboración Propia.

ID	Historia Usuario	Tarea	Tiempo estimado (Días)	Tiempo Real (Días)	Proceso
H07. T01	Como usuario gestor de proyectos quiero poder configurar las parametrizaciones de las amenazas	Diseñar interfaz de configuraciones de amenazas	0.5	0.5	Web
H07. T02		Programar registros, edición y eliminación de parametrizaciones con respecto a las amenazas.	1	1	
H08. T01	Como usuario gestor de proyecto quiero poder asignar categorías y tipos de amenazas a cada activo de información	Diseño de interfaz gráfica para seleccionar, editar, eliminar y añadir las categorías, grupos de activos de información; y tipos de amenazas	1.5	1	Web Y móvil
H08. T02		Diseñar funcionalidades de integración	1	0.5	
H08. T03		Desarrollar actividades para leer de categorías, grupos y tipos de amenazas	1.5	2	
H08. T04		Desarrollar servicios web para actualizar información de categorías, grupos y tipos de amenazas	2	2.5	
H08. T05		Desarrollar la funcionalidad para añadir amenazas a cada activo de información	1	1	
H08. T06		Testear funcionalidades web y móvil añadidas	0.5	0.5	
H09. T01	Como usuario gestor de proyecto quiero poder realizar la estimación de la vulnerabilidad	Diseñar interfaces web y móvil para estimación de vulnerabilidad	1	1.5	Web y Móvil
H09. T02		Desarrollar lógica para que permita realizar la estimación de manera numérica (escala de 1-5) por cada una de las amenazas de un activo de la información. Para esto solo se tomará en cuentas los activos que tengan la evaluación de amenazas completas	2	2	
H09. T03		Desarrollar actividad para leer y actualiza estimación de vulnerabilidad	1	1.5	
H09. T04		Desarrollar servicios web para poder actualizar información respecto a las estimaciones de vulnerabilidad	1	1	
H09. T05		Testear funcionalidad de guardado en tablas de la BD.	0.5	0.5	

Resultados del Sprint

a. Web

En la siguiente figura se visualiza las interfaces de parametrizaciones de amenazas que se tomaran en cuenta en cada proyecto, al no ser parte Core del sistema, solo se puede acceder mediante web.

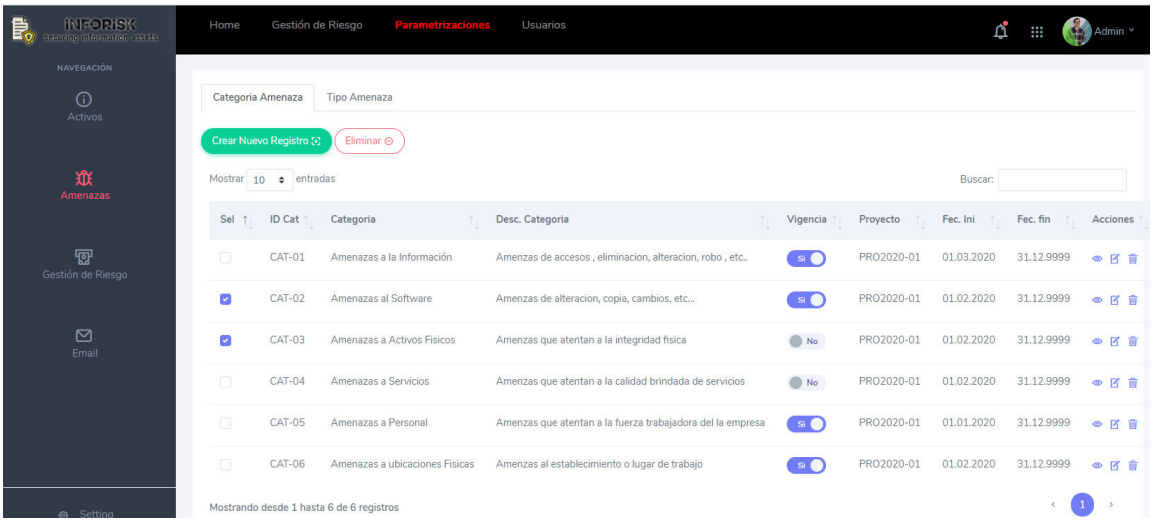

Figura 4.22. Pantalla Parametrizaciones de Amenazas. Elaboración propia

En la figura 4.23 se puede observar una tabla con identificadores de activos de información con sus respectivas amenazas asignados por el usuario gestor de proyecto. Al dar clic en desplegar, se puede editar y/o añadir cada amenaza.

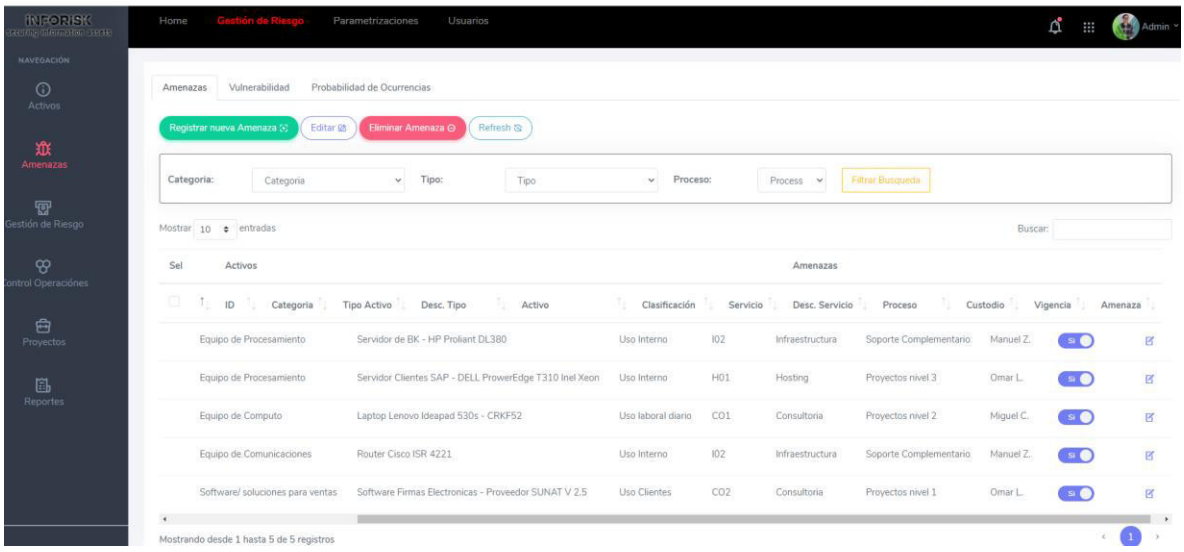

Figura 4.23. Pantalla de Gestión y asignación de Amenazas. Elaboración propia

En la figura 4.24 se observa un listado de activos con las amenazas y vulnerabilidades ya asignadas, y con la evaluación aún por definir. Dentro de esta interfaz se puede notificar a los usuarios custodios para que realicen la evaluación o evaluar según las capacidades. En la figura 4.25 se visualiza la interfaz de estimación de vulnerabilidades por cada registro.

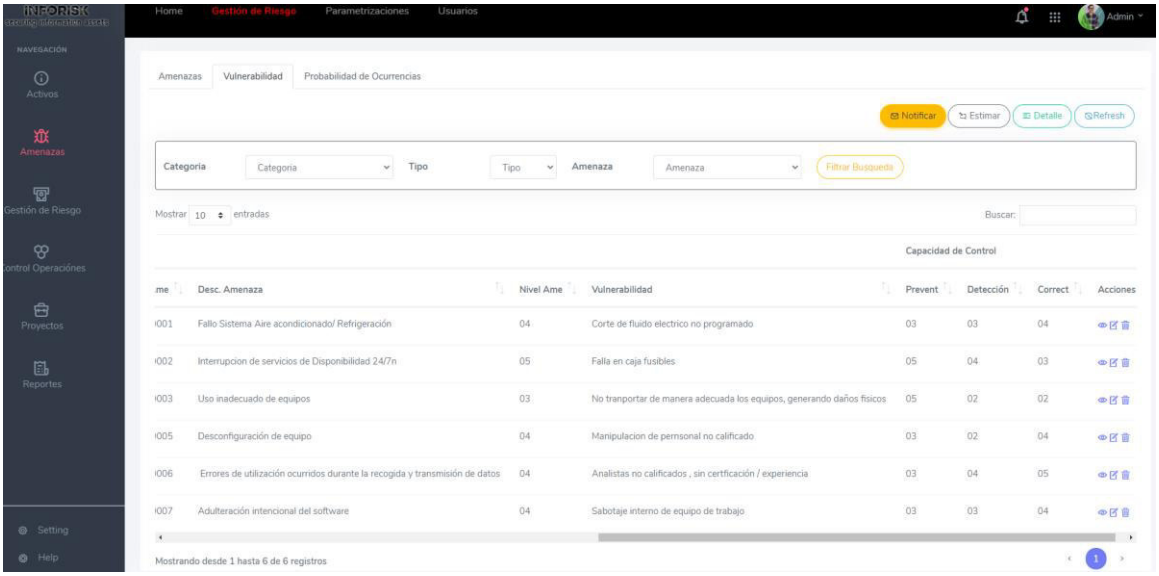

Figura 4.24. Pantalla de Amenazas y Vulnerabilidades. Elaboración propia

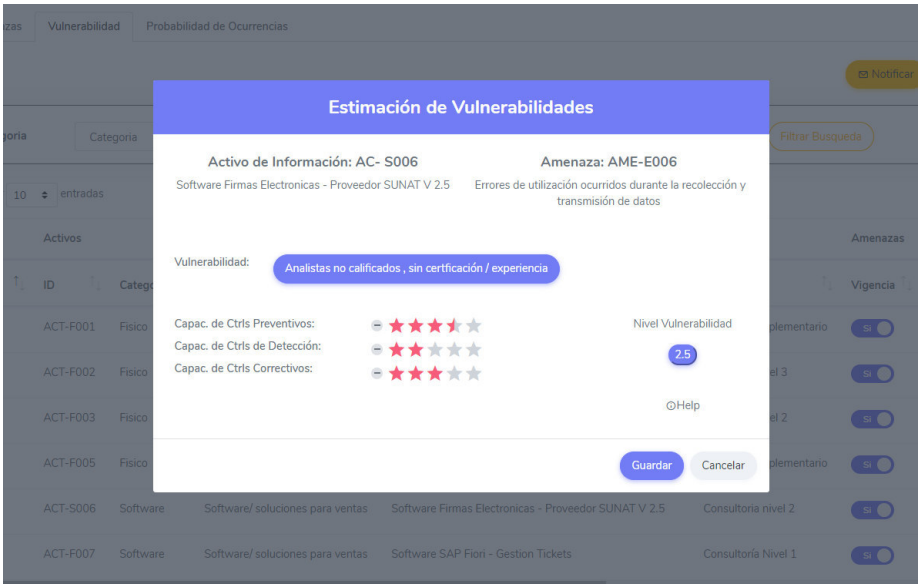

Figura 4.25. Pantalla de Estimación de Vulnerabilidades. Elaboración propia

En la figura 4.26 se observa un listado de las amenazas y vulnerabilidades ya evaluadas, y también el cálculo interno de la probabilidad de ocurrencia por cada amenaza. Dentro de la opción “Detalle histórico” se visualiza el historial de cada registro.

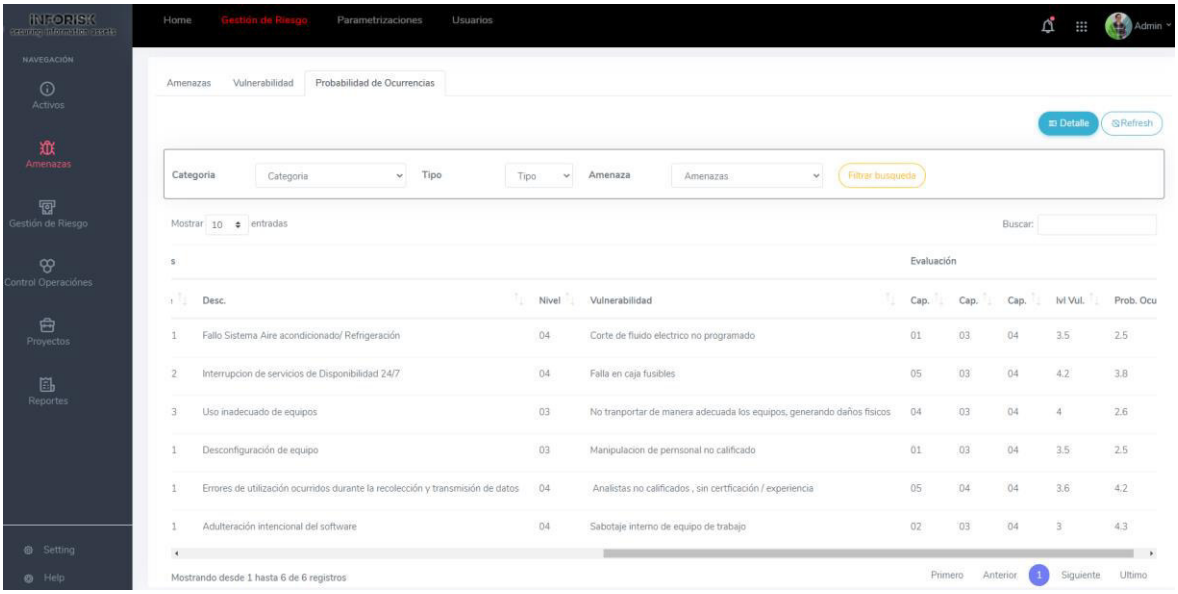

Figura 4.26. Pantalla Amenazas - Probabilidades de Ocurrencia. Elaboración propia

b. Móvil

En el caso del aplicativo móvil, tiene las mismas funcionalidades del aplicativo web a lo que se refiere en crear, editar y/o eliminar amenazas; y también en evaluar y obtener la probabilidad de ocurrencia de las amenazas. En la siguiente imagen se visualiza la pantalla de estimación de vulnerabilidades mediante el uso de calificaciones de 3 capacidades de control.

Figura 4.27. Pantalla móvil de Evaluación de Amenazas. Elaboración propia

4.7.5 Sprint n° 5

La pila del quinto sprint se detalla en la tabla 4.7. En este sprint se centra en la gestión principal del producto, que es la gestión de riesgos. Se elabora la funcionalidad de evaluación de impactos mediante el método de juicio de expertos, los cuales se asignaron en la gestión de amenazas y se les notifica por email. La evaluación de impacto sobre la empresa se rige mediante los siguientes aspectos

- Aspecto económico
- Aspecto Continuidad de negocio / operacional
- Aspecto legal
- Aspecto Imagen
- Aspecto contractual

El nivel de impacto se evalúa como promedio simple de todos los evaluadores en el juicio de expertos, incluido el usuario custodio y propietario.

$$Nivel\ de\ Impacto = \frac{P_1 + P_2 + P_3 + P_4 + P_5}{5}$$

Donde: cada P_n representa el promedio simple de cada aspecto de impacto evaluado en el juicio de expertos, cuya cantidad denotaremos por ‘m’ así quedaría:

$$Promedio\ Aspecto\ P_N = \frac{\sum_1^m ASPECTO\ (n)}{\text{m}}$$

Luego de obtener el promedio, se calcula internamente el nivel de evaluación de riesgos, cuya formula seria de la siguiente manera:

$$Nivel\ de\ Riesgo = (\ Prob.de\ Ocurrencia * Nivel\ de\ Impacto)$$

Una vez obtenida el nivel de riesgo, se crea la funcionalidad para visualizar mediante una tabla todos estos cálculos por cada activo, amenaza y riesgo. Adicionalmente se crea una por lógica programable la matriz de riesgo de acuerdo a la tasación de calificación preconfigurada para el riesgo.

Tabla 4.7 Sprint 5: Sprint Backlog. Elaboración Propia.

ID	Historia Usuario	Tarea	Tiempo estimado (Días)	Tiempo Real (Días)	Proceso
H10. T01	Como usuario gestor de proyectos quiero poder visualizar la probabilidad de ocurrencia para las amenazas	Diseñar de manera gráfica el campo de probabilidad de ocurrencia	0.50	0.5	Web
H10. T02		Desarrollar lógica para que el sistema calcule de forma automática la Probabilidad de ocurrencia, como un promedio simple entre el nivel de vulnerabilidad y el nivel de amenazas	1	1.5	
H10. T03		Testear cálculo de promedios se visualice y sea correcto	0.25	0.25	
H11. T01	Como usuario gestor de proyectos quiero poder gestionar evaluación del impacto de los riesgos	Analizar impacto de modificaciones de cálculos	1	1	Web y Móvil
H11. T02		Diseñar interfaz web y móvil para los formularios de evaluación	1	0.5	
H11. T03		Desarrollar funcionalidad para envío de mails de notificación a usuarios involucrados en la evaluación del impacto, mediante un link único que anexe al correo.	1	1.5	
H11. T04		Desarrollar funcionalidad de registro de impacto según aspecto legal, operacional y de imagen. Estas evaluaciones van asignadas a un evaluador o usuario dependiendo el activo.	2	2	
H11. T05		Desarrollar actividad de listado de evaluación de impacto.	1	1.5	
H11. T06		Validar generación de email, con URLs de evaluación, testear correcto guardado de evaluaciones en las BD.	1	1	

H12. T01	Como usuario gestor de proyectos quiero poder gestionar el nivel de exposición a los riesgos	Diseñar gráficamente campo de nivel de exposición del riesgo	0.5	0.5	Web
H12. T02		Desarrollar lógica que calcule el nivel de exposición del riesgo, se calcula mediante el nivel de impacto por la probabilidad de ocurrencia, se debe generar de manera automática al presionar botón de actualizar Valores	1.5	1.5	
H12. T03		Testear cálculo del sistema y generación de matriz de riegos.	0.5	0.5	

Resultados del Sprint

a. Web

En la figura 4.28 se muestra la interfaz de gestión de riesgos en una tabla con información puntual del activo, amenaza, vulnerabilidad y evaluación de impacto en caso se haya evaluado. Al seleccionar un registro y dar clic en evaluar se visualizará un popup de evaluación, como se muestra en la figura 4.29.

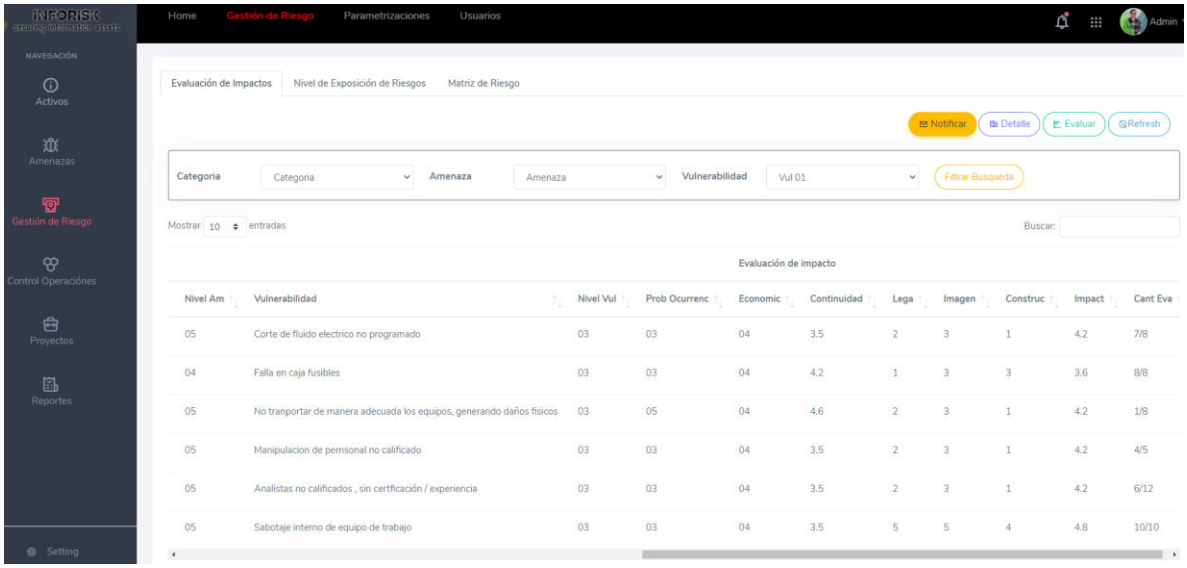

Figura 4.28. Pantalla de Impacto de Riesgos. Elaboración propia

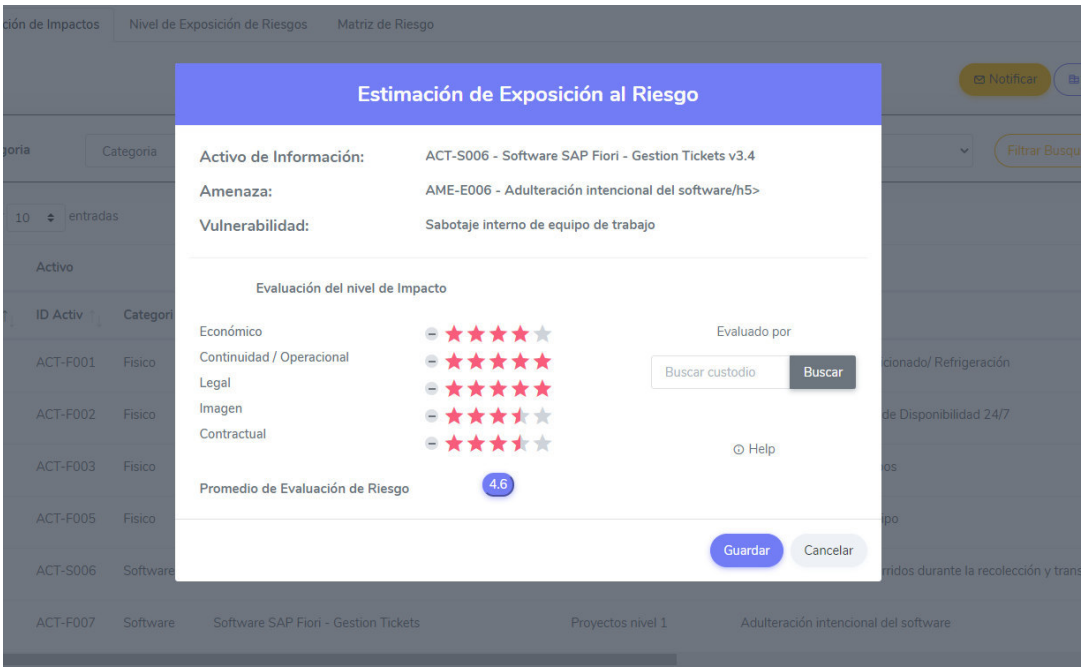

Figura 4.29. Pantalla de Evaluación de Impacto. Elaboración propia

En la figura 4.30 se visualiza la interfaz para el nivel de exposición al riesgo, con todos los datos ya calculados internamente, mediante una tabla con parámetros puntuales de activos, amenazas y riesgos. En la opción de "Historial o detalle" se visualizará el detalle histórico de la evaluación del registro seleccionado.

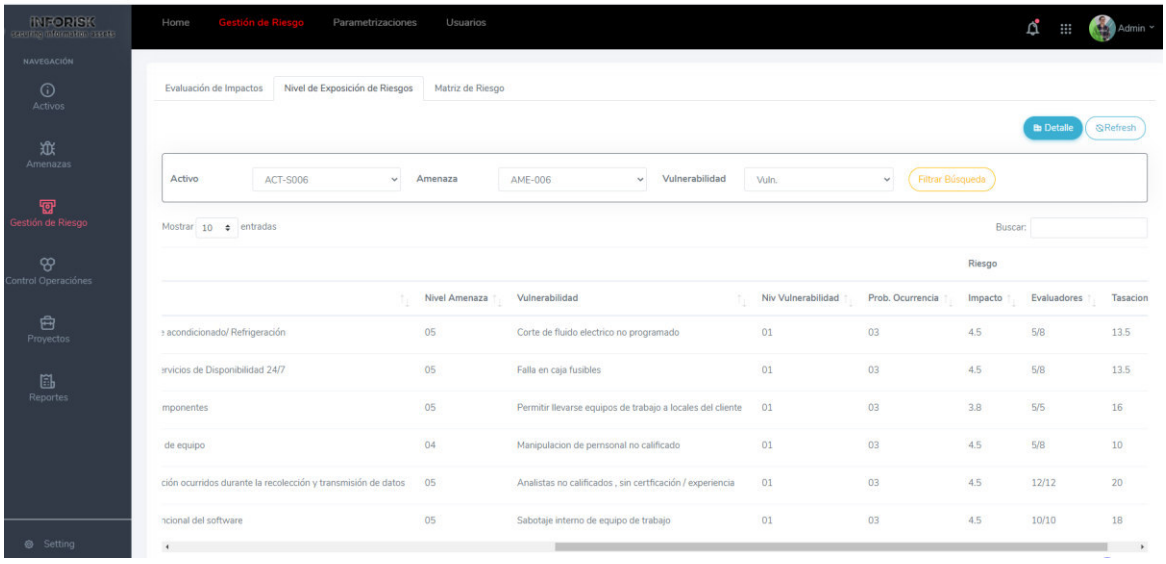

Figura 4.30. Pantalla de Nivel de Exposición de Riesgo. Elaboración propia

En la figura 4.31, luego del cálculo interno y automático se muestra, de manera resumida, la matriz de riesgos de seguridad de información, mediante un gráfico interactivo

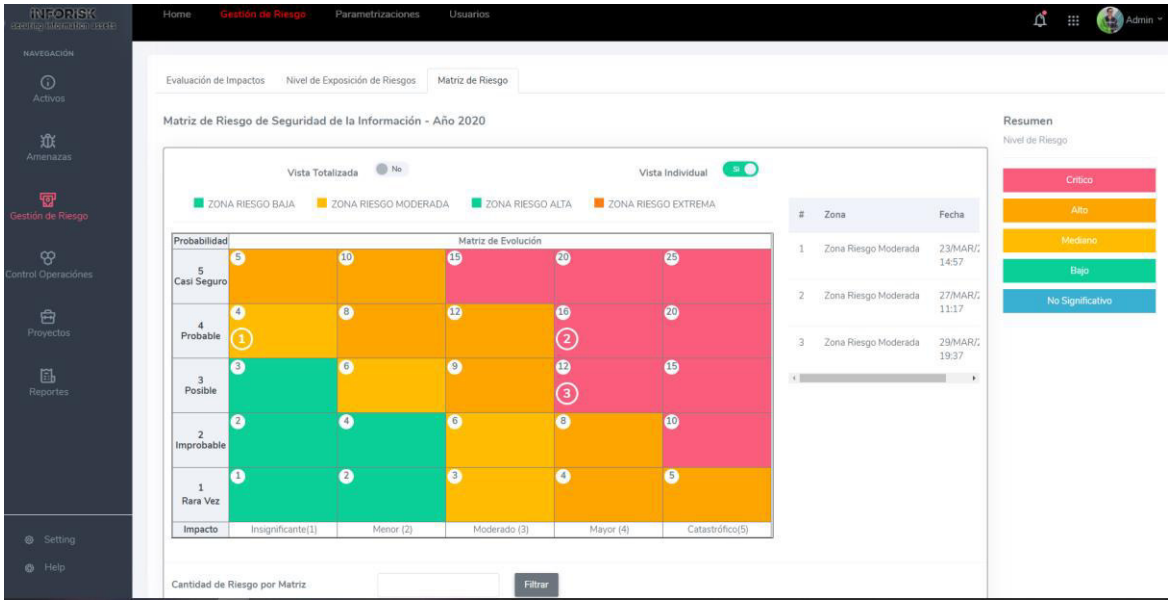

Figura 4.31. Pantalla de Matriz de Riesgos. Elaboración propia

b. Móvil

Para el caso del aplicativo móvil, se ha considerado que tenga las funcionalidades de poder visualizar y evaluar cada impacto de las amenazas al negocio de la empresa, así como de visualizar el nivel de exposición al riesgo. En la siguiente figura se visualiza la pantalla de evaluación del nivel de impacto, la cual permite evaluar de manera interactiva los distintos aspectos.

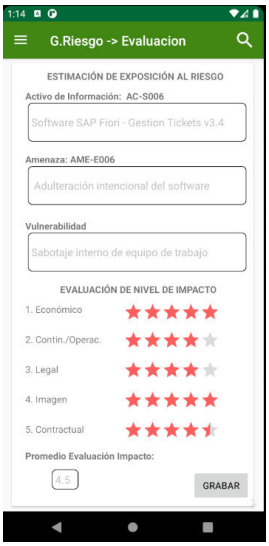

Figura 4.32. Pantalla móvil de Evaluación de Riesgos. Elaboración propia

4.7.6 Sprint n° 6

La pila del sexto sprint se detalla en la tabla 4.8. En este sprint se centra en las gestiones de tratamientos de riesgos(controles) y oportunidades de desarrollo. Luego de calcular el nivel de exposición de riesgo por cada activo, de acuerdo al nivel bajo o alto obtenido, se procede con la funcionalidad de tratar el riesgo. Se tiene la opción de calificarlo como Aceptable o No aceptable. En el caso de que el riesgo se encuentre en la valoración de no aceptable, se tiene que seleccionar una estrategia de actuación frente al riesgo, de las cuales son:

- Reducir
- Transferir
- Aceptar
- Evitar

Las funcionalidades de control de riesgos se definen mediante tablas y formularios a completar, con el fin de tener mapeado cada estrategia seleccionada. También se incluye el cálculo de los costos y/o proyectos de mejora que se pueden anexar al sistema.

Adicionalmente, de acuerdo al estudio realizado de cada activo de información, sus amenazas, vulnerabilidades y nivel de riesgo; Se puede identificar alguna oportunidad de mejora que impactaría en algún aspecto en beneficio de la empresa, también se ha implementado las funcionalidades para el registro y detalle del mismo.

Tabla 4.8 Sprint 6: Sprint Backlog. Elaboración Propia.

ID	Historia Usuario	Tarea	Tiempo estimado (Días)	Tiempo Real (Días)	Proceso
H13. T01	Como usuario gestor de proyectos quiero poder gestionar el tratamiento de los riesgos	Diseñar interfaz gráfica web y móvil de tratamiento de riesgos seleccionados	0.5	0.5	Web Y móvil
H13. T02		Desarrollar funcionalidades de gestión de proyectos anexos a cada control	0.5	0.5	
H13. T03		Desarrollar funcionalidad para gestionar los riesgos cuya medición en el proceso anterior hayan tenido un puntaje por encima de lo permitido. Se considera solo al finalizar el proceso de gestión de riesgos. Dentro del tratamiento del riesgo se considera aceptable o no aceptable.	2	2.5	
H13. T04		Desarrollar actividad para selección de riesgos y tratamientos	1	1	
H13. T05		Desarrollar servicio web para consultas y gestión de tratamientos de riesgos definiendo parámetros a enviar y a recibir	1	1.5	
H13. T06		Testear funcionalidades de grabación en B.D.	0.25	0.25	
H14. T01	Como usuario gestor de proyectos quiero poder gestionar las oportunidades de desarrollo	Diseñar interfaz gráfica de opciones de gestión de oportunidades	0.25	0.25	Web y Móvil
H14. T02		Desarrollar funcionalidad que guarde oportunidades encontradas para cada activo y riesgo identificado. Se activará solo después de haber completado la gestión de riesgos.	1	1	
H14. T03		Desarrollar actividad para visualizar y editar oportunidades de desarrollo dentro de las competencias de tratamientos de	1.5	2	

		riesgos.			
H14. T04		Testear funcionalidades de lógica y guardado de información en BD.	0.5	0.25	

Resultados del Sprint

a. Web

En la figura 4.33 se observa en la tabla el listado de riesgos evaluados que tienen un nivel alto o No aceptable, y que requieren un tratamiento de control, se puede seleccionar algún registro y dar clic en Registrar Control, para aquellos que no tengan aun ningún control asignado. La figura 4.34 muestra la interfaz para añadir un control; En la parte superior se observa todos los datos relacionados al riesgo en cuestión, como: Nombre de activo, valoración, amenaza, nivel de amenaza, vulnerabilidad, evaluación promedio de impacto y nivel de riesgo resultante. En la siguiente sección de la pantalla permitirá registrar el control adecuado para el riesgo seleccionado. Se añade nuevos responsables a los proyectos planteados y permite anexar documentos referentes a las propuestas.

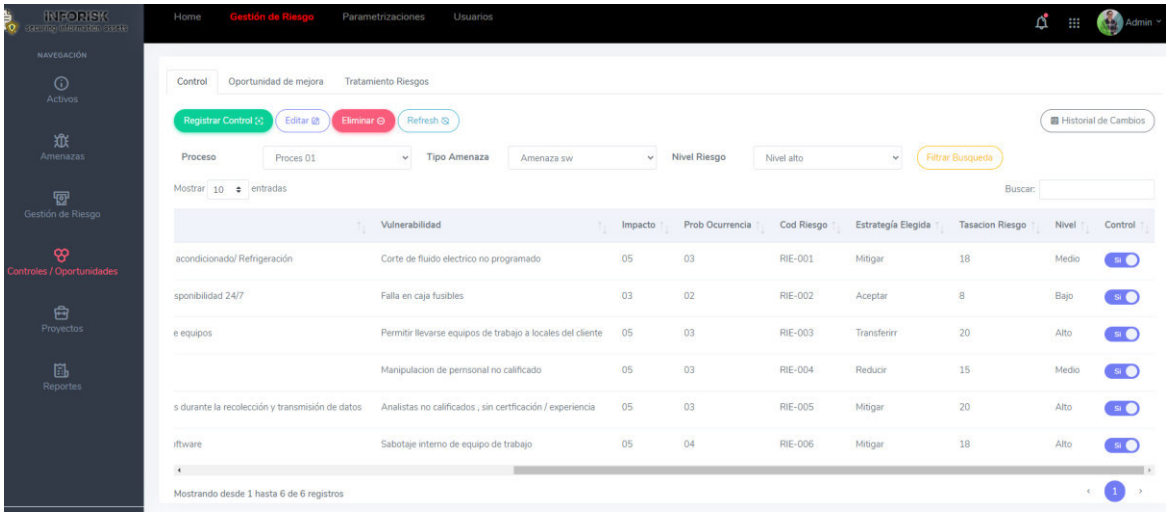

Figura 4.33. Pantalla de Matriz de Riesgos. Elaboración propia

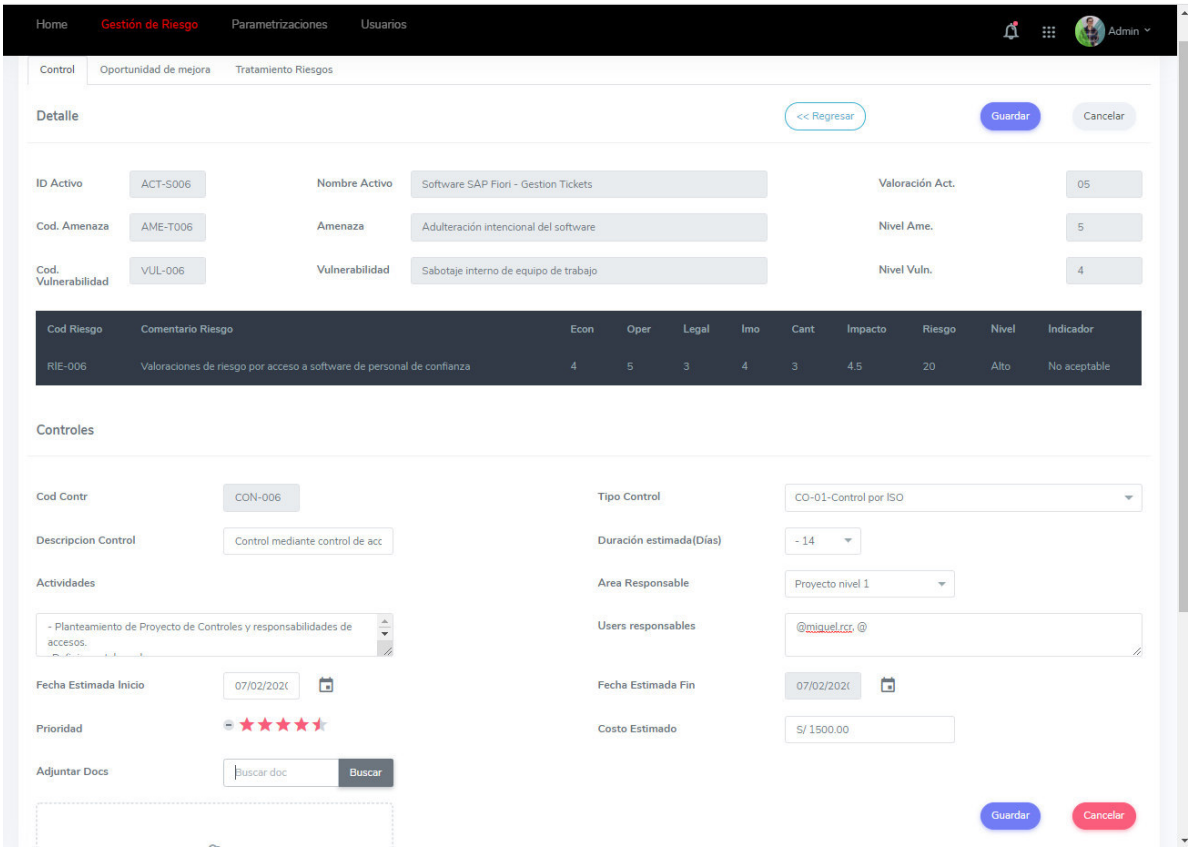

Figura 4.34. Pantalla de Creación de Controles. Elaboración propia

Para las oportunidades de mejora, las pantallas son similares a las del registro de controles, una tabla con los riesgos de los cuales se puede tomar como oportunidad de mejora. Al hacer clic en Registrar Oportunidad se muestra la siguiente pantalla en la cual permite completar un formulario con información básica a la propuesta asignada.

b. Móvil

Las funcionalidades de tratamiento de riesgos que se han detallado en la aplicación web, también se tendrá en cuenta para la ampliación móvil. Aunque de una manera más limitada en cuanto formularios por pantalla, Así también podremos registrar controles y oportunidades de mejora mediante la aplicación web. En la figura 4.35 se visualiza un listado de riesgos con su tasación e indicador, lo cual se toma en cuenta para tener que registrar un control o una mejora; y en casos ya tenga registrado se mostrara solo el detalle. En la figura 4.36 muestra el registro de controles que se grabara por cada riesgo elevado.

Figura 4.35. Pantalla móvil de Listado de Riesgos. Elaboración propia

Figura 4.36. Pantalla móvil de Registro de Controles. Elaboración propia

4.7.7 Sprint n° 7

La pila del séptimo sprint se detalla en la tabla 4.9. En este sprint se desarrolla una funcionalidad ligada bastante a los controles o tratamiento de riesgos, debido a que muchos de los controles implementados se materializan como un proyecto nuevo a desarrollar, es necesario también que el sistema mantenga un control básico de estos

proyectos que engloban las actividades a realizar. Adicional a esto se añade las funcionalidades de reportes y visualización limitadas dependiendo del tipo de usuario. Para las funcionalidades de reportes se ha configurado con una herramienta que nos brinda una interfaz con amplia variedad de tipos de reportes.

Tabla 4.9 Sprint 7: Sprint Backlog. Elaboración Propia.

ID	Historia Usuario	Tarea	Tiempo estimado (Días)	Tiempo Real (Días)	Proceso
H15. T01	Como usuario gestor de proyectos/ usuario líder quiero poder gestionar los proyectos relacionados a los controles implementados	Diseñar interfaces grafica para las funcionalidades de gestor de proyectos	1	1	Web
H15. T02		Desarrollar funcionalidad y lógicas para asignar proyectos a controles existentes, así como creación, editar, seguimiento (Gant y Kanban) y eliminar.	2	2.5	
H15. T03		Testear funcionalidades de creación de proyectos, seguimiento mediante Gant y Kanban	1	1	
H16. T01	Como usuario gestor de proyecto o gerencia quiero poder visualizar los reportes de la gestión de riesgos	Diseñar interfaz gráfica para descarga de proyectos mediante filtros de selección	0.5	0.5	Web Y móvil
H16. T02		Diseñar formato y modelo de reportes de gestión de riesgos	2	1	
H16. T03		Desarrollar e implementar y configurar sistema para exportación de reportes (3 tipos de reportes) en formato Excel y PDF.	3	3.5	
H16. T04		Desarrollar actividad para visualización de reportes	1	1	
H16. T05		Testear formatos e información en reportes.	1	0.5	
H17. T01	Como usuario custodio quiero poder visualizar mis activos asignados y su evaluación de riesgo	Habilitar sistema solo para visualización de activos a usuarios custodio	1.5	2	Web
H17. T02		Testear filtro de validaciones a usuarios custodio.	1	0.5	

Resultados del Sprint

a. **Web**

En la figura 4.37 se visualiza la interfaz de gestión de proyectos que tienen relación con los controles a implementar, en la primera pantalla de este submódulo se visualiza mediante cards el avance de los últimos proyectos en desarrollo. Así también tiene la opción de realizar el seguimiento de cada uno mediante la técnica Gant (por tiempos) y Kanban (por actividades).

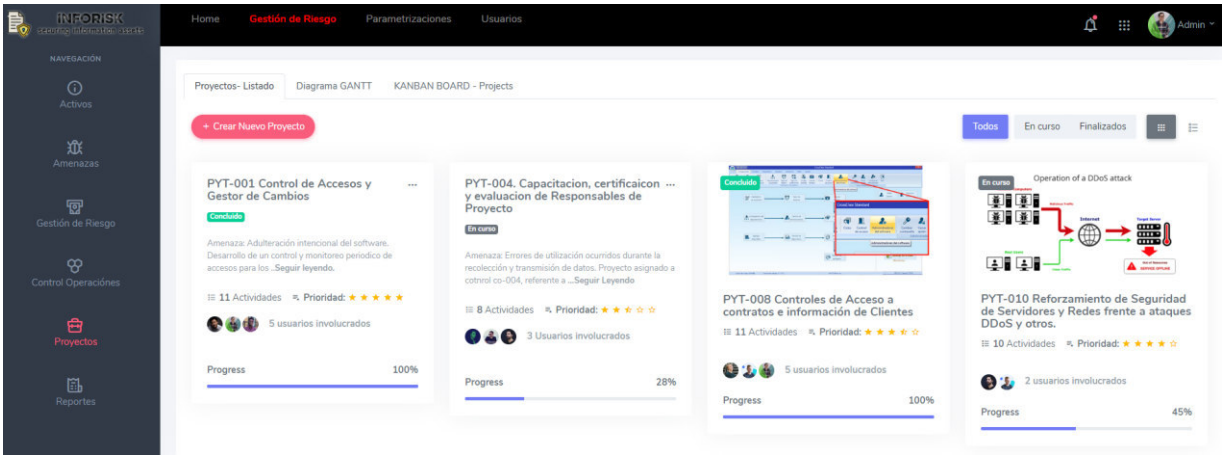

Figura 4.37. Resumen de Estado de Proyectos de Controles. Elaboración propia

En la figura 4.38 se muestra los charts de selecciones del reporte generado, los mismos con opciones de exportación a PDF o XLS. Para esta sección se tendrá los siguientes tipos de reporte.

- Reporte de Matriz de Riesgos
- Reporte de Cantidad de Activos con Riesgo Alto
- Reporte de Parametrizaciones de objetos
- Reporte Consolidado de Gestión de Activos de la Información
- Reporte de Controles y Oportunidad de Mejora

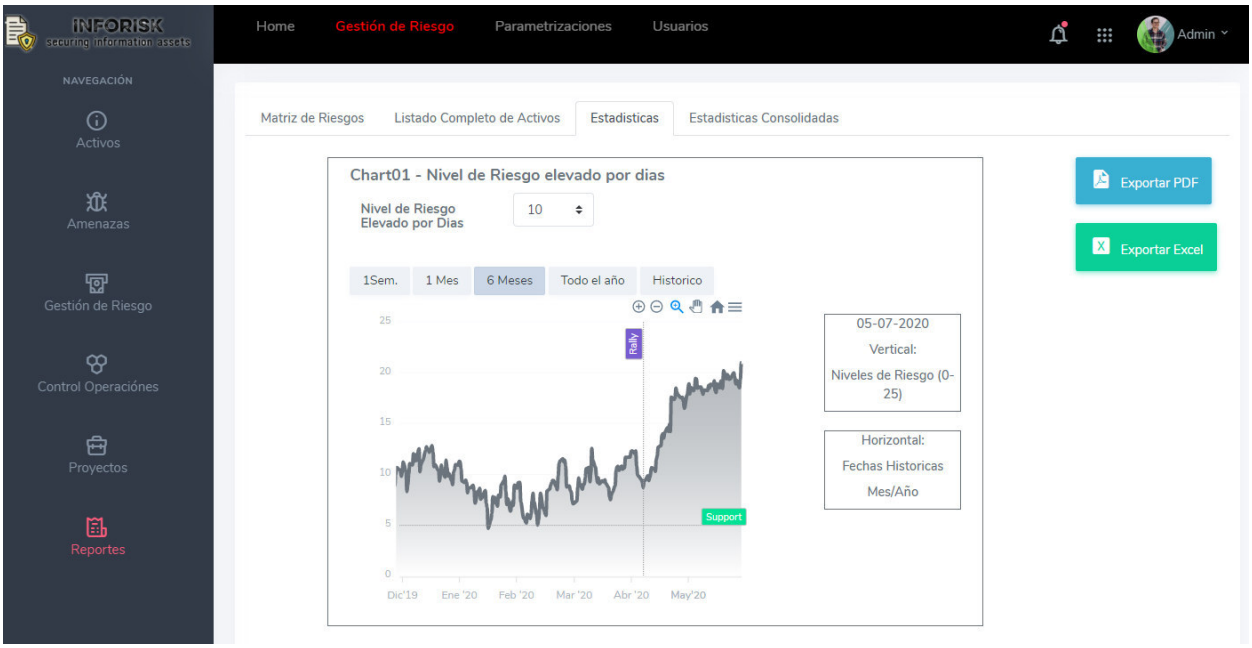

Figura 4.38. Reporte Estadístico por Secciones. Elaboración propia

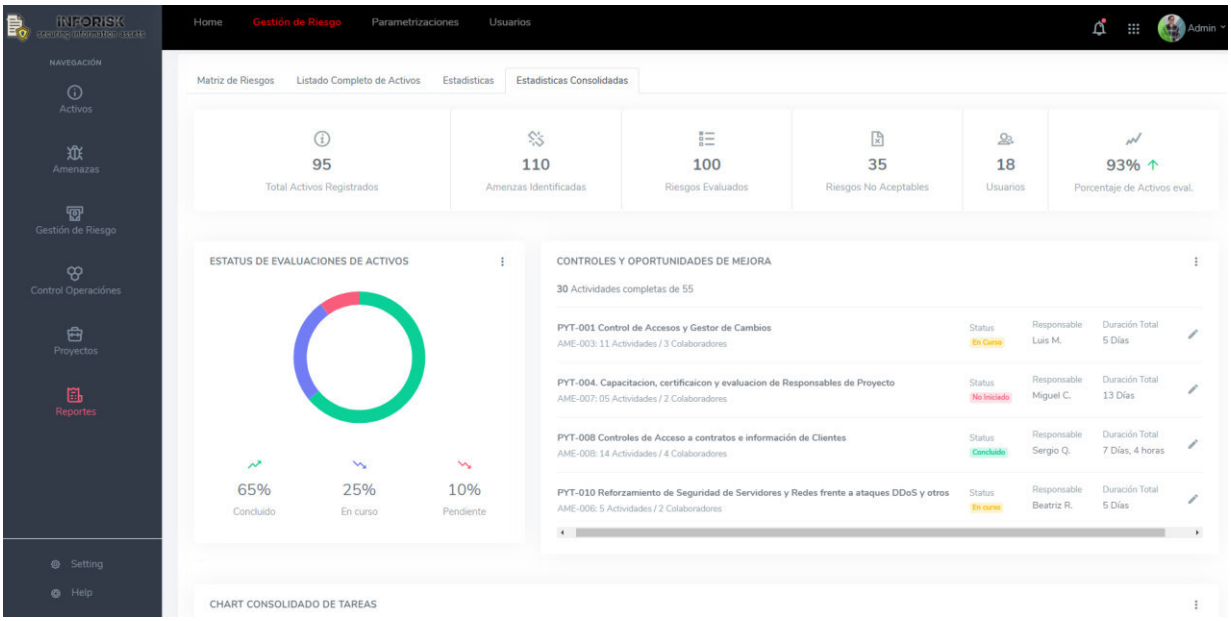

Figura 4.39. Reporte Estadístico Consolidado. Elaboración propia

b. Móvil

Las funcionalidades de reportes se han añadido también a la aplicación móvil, pudiendo visualizar en la aplicación y descargar en PDF los reportes mencionados

anteriormente. En la siguiente figura se muestra los campos de filtros y el mensaje de descarga del archivo generado.

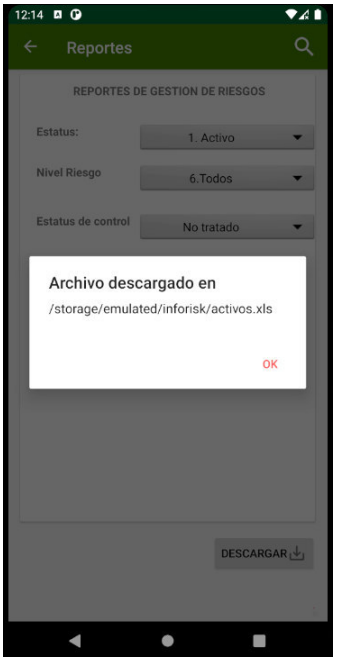

Figura 4.40. Pantalla móvil de Descarga de Reportes. Elaboración propia

4.7.8 Sprint n° 8

La pila del octavo sprint se detalla en la tabla 4.10. En este sprint se desarrolla funcionalidades complementarias al sistema en cuestión. La funcionalidad de permitir búsqueda rápida por palabras clave se implementa y desarrolla en todas las listas y tablas del sistema.

Se desarrolla la funcionalidad para editar y pre configurar el cuerpo genérico de los mails a enviar, esto es como complemento al envío de emails de notificación para las funcionalidades que lo requieran.

Tabla 4.10 Sprint 8: Sprint Backlog. Elaboración Propia.

ID	Historia Usuario	Tarea	Tiempo estimado (Días)	Tiempo Real (Días)	Proceso
H18. T01	Como usuario gestor proyectos, administrador, custodio, Gerencia, quiero poder buscar por palabras clave sobre los activos,	Diseñar en interfaces opciones de filtros de búsqueda en cada sección correspondiente	1	1	Web Y móvil
H18. T02		Desarrollar lógica de filtros de búsqueda para cada fase y sección del sistema	3	4	

	amenazas y riesgos registrados en la BD.				
H19.01	Como usuario Administrador, Gestor de Proyecto quiero poder editar el envío de emails genéricos a los usuarios y evaluadores	Diseñar mockups e interfaz gráfica para la configuración de emails genéricos.	0.5	0.5	Web
H19.02		Desarrollar la funcionalidad para guardar y setear cuerpo de emails de acuerdo al requerimiento	1	1.5	

Resultados del Sprint

a. Web

En la figura 4.41 se visualiza la interfaz gráfica para redactar el cuerpo de un email genérico que se notifica en las funcionalidades de evaluación.

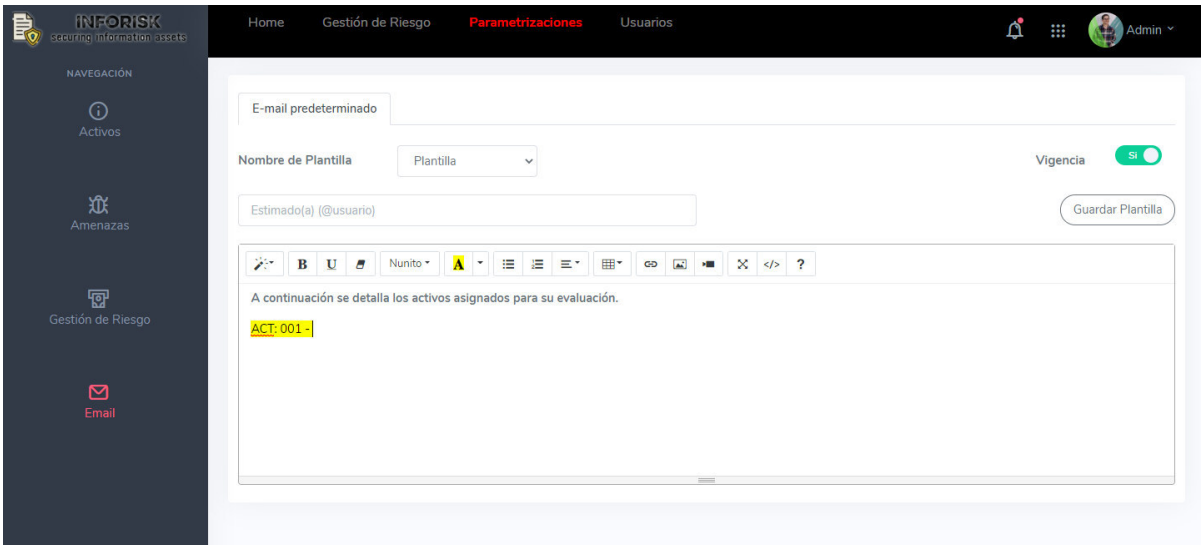

Figura 4.41. Pantalla de Parametrizaciones email. Elaboración propia

CAPÍTULO V

VALIDACIÓN

En este capítulo se desarrolla la validación del aplicativo web y móvil. Se inició con el desarrollo del proyecto Gestión de Riesgos de Seguridad de la Información, autorizado por el área de seguridad informática para la consultora de Sistemas al cual se aplicaría; Para este proyecto se apoyará en la versión beta de los aplicativos webs y móvil propuestos, así como también de la metodología de gestión de riesgos a utilizar. En el apartado de **anexos A, B y C** se listan los activos de información identificados, las amenazas, vulnerabilidades y riesgos calculados identificados de la empresa.

Para el proceso de validación y medición de resultados del sistema propuesto se realiza mediante la técnica de encuesta a grupo objetivo, la cual se aplica a un grupo de usuarios clave para evaluar su satisfacción con respecto a las expectativas del sistema y metodología propuestas.

6.1 Determinación de Datos Cualitativos.

De acuerdo al análisis del objetivo de la metodología de gestión de riesgos y a las aplicaciones informáticas (web y móvil) desarrolladas, se identificó los siguientes datos cualitativos a tomar en cuenta para la evaluación.
(Cada datos o indicadores tendrán 1-4 preguntas en el cuestionario)

Tabla 5.1 Datos cualitativos de calificación al sistema. Elaboración Propia.

Calificación	Descripción
C1	Nivel de entendimiento de la metodología de gestión de riesgos planteada
C2	Nivel de satisfacción de usabilidad de la aplicación web (intuitivo)
C3	Nivel de satisfacción de usabilidad de la aplicación móvil
C4	Comprensión de las funcionalidades del sistema.
C5	Facilidad de aprendizaje del sistema.
C6	Capacidad de respuesta acorde a lo requerido

C7	Rapidez en operaciones rutinarias del sistema
C8	Utilidad para las tareas requeridas.

Para determinación de las encuestas se calificarán lo datos listados anteriores en escala de 1 a 10. Los valores de la escala se encuentran la siguiente tabla.

Tabla 5.2 Escala de evaluación para calificaciones. Elaboración Propia.

Puntaje (Intervalo)	**Descripción**
[9-10]	Muy entendible Muy Satisfecho con el sistema Fácil de entender e intuitivo Muy útil y de acuerdo a los objetivos Capacidad de respuesta alta
[7-8]	Entendible Satisfecho Fácil de usar el sistema Útil en los objetivos propuestos. Buena capacidad de respuesta
[4-6]	Medianamente comprensible Regular Se toma poco de tiempo comprender el sistema Útil solo en algunos aspectos Capacidad de respuesta regular
[2-3]	Incomprensible en algunos aspectos Poco satisfecho con el sistema Complicado Sistema poco útil Capacidad de respuesta baja
1	Totalmente incomprensible Totalmente insatisfecho con el sistema Muy difícil de entender Totalmente inútil para el objetivo Capacidad de respuesta muy mala

El grupo objetivo de la encuesta fue encuestar a distintos tipos de usuarios que interactuaron con las aplicaciones web y móvil dependiendo su respectivo alcance. Se tuvo un total de 20 participantes, entre tipos de usuario Gestor de proyecto, Gerentes, Custodios y Evaluadores (juicio de expertos).

Tabla 5.3 Tabla de Actividades a Evaluar. Elaboración Propia.

Actividades	Descripción
A1	Parametrizaciones del Sistema (Solo usuario administrador)
A2	Registrar, eliminar, editar y/o evaluar Activos de Información
A3	Registrar, eliminar, editar Amenazas y/o vulnerabilidades
A4	Estimación de vulnerabilidades
A5	Evaluación de Impacto y riesgos
A6	Gestión de Controles, tratamiento de riesgos y Oportunidades de mejora
A7	Revisión de reportes analíticos.

6.2 Ejecución de la Prueba

Las encuestas se realizaron a un grupo de 20 usuarios de distintos tipos. Los cuales respondieron de acuerdo a las actividades del sistema competentes para su rol y sobre unas cualidades de calificación especificada en la tabla 6.1.

En la tabla 6.4 se muestra las evaluaciones separadas por el tipo de usuario, las actividades referentes, los aspectos evaluados y la puntuación desde el 1 hasta el 10. Se agrupa mediante promedio simple la evaluación por actividad y por cualidad del sistema.

Tabla 5.4 Tabla de Calificaciones de Usuarios al Sistema InfoRisk. Elaboración Propia.

Tipo usuario / Rol	Usuario	Actividad	C1	C2	C3	C4	C5	C6	C7	C8	Promedio
Administrador	U1	A1	5	6	6	6	8	8	4	9	6.5
	U2	A1	8	4	6	5	8	8	5	9	6.625
Gestor de Proyecto	U3	A2	7	6	7	7	7	8	5	8	6.875
	U3	A3	8	7	7	8	8	8	5	8	7.375
	U3	A4	7	6	7	7	3	9	5	9	6.625
	U3	A5	6	7	7	7	2	8	5	9	6.375
	U3	A6	6	8	7	7	4	9	4	8	6.625
	U3	A7	6	8	6	6	5	8	5	9	6.625
	U4	A2	5	8	7	6	7	9	5	9	7
	U4	A3	8	9	6	6	2	7	7	9	6.75
	U4	A4	5	9	7	7	3	8	5	9	6.625
	U4	A5	6	9	8	5	4	9	8	9	7.25
	U4	A6	6	10	8	7	5	8	5	9	7.25
	U5	A2	7	7	6	4	7	7	5	10	6.625
	U5	A3	8	8	9	5	5	8	6	10	7.375
	U5	A4	7	6	8	6	9	9	3	9	7.125
	U5	A5	8	7	7	7	5	8	6	9	7.125
	U6	A2	6	8	7	6	4	9	5	9	6.75
	U6	A4	4	9	5	7	7	8	4	9	6.625
	U6	A5	8	4	6	8	5	8	2	9	6.25
	U6	A6	8	5	7	5	6	8	1	8	6
	U7	A2	9	6	7	7	5	8	5	9	7
	U7	A3	7	7	7	5	7	7	2	9	6.375
	U7	A4	8	8	7	6	5	8	5	8	6.875
	U7	A6	5	9	8	7	5	9	4	9	7

	U8	A4	7	8	8	6	8	8	2	9	7
	U8	A5	7	7	8	7	8	7	3	8	6.875
	U8	A6	9	7	8	6	8	7	3	10	7.25
	U8	A7	7	7	8	8	9	7	4	10	7.5
	U9	A2	8	7	8	6	6	8	5	10	7.25
	U9	A3	7	7	8	7	6	9	2	8	6.75
	U9	A4	8	8	7	6	7	8	2	9	6.875
	U9	A6	7	8	6	5	8	7	7	9	7.125
	U9	A7	7	8	6	8	9	8	5	9	7.5
Custodio	U10	A2	7	9	9	5	7	9	5	9	7.5
	U10	a3	6	6	9	7	9	8	7	8	7.5
	U10	A4	9	7	5	6	7	7	7	7	6.875
	U11	A2	9	8	8	6	9	7	7	9	7.875
	U11	A3	8	8	8	6	7	8	7	9	7.625
	U11	A4	7	9	8	6	9	8	8	9	8
	U12	A2	8	8	8	6	7	8	5	9	7.375
	U12	A3	7	7	8	6	9	8	7	8	7.5
	U12	A4	9	9	8	5	8	8	5	7	7.375
	U13	A2	6	8	9	5	9	8	4	9	7.25
	U13	A3	9	7	7	6	8	7	5	9	7.25
	U13	A4	7	8	8	7	8	7	4	9	7.25
	U13	A5	8	9	6	8	7	8	5	6	7.125
Experto/ Evaluador	U14	A4	6	8	3	6	6	9	6	9	6.625
	U14	A5	6	9	7	7	8	9	5	9	7.5
	U15	A4	5	8	7	6	6	8	6	9	6.875
	U15	A5	5	9	8	4	7	7	5	10	6.875
	U16	A2	8	8	9	6	8	8	6	9	7.75

	U16	A4	6	9	8	5	6	9	3	9	6.875
	U16	A5	9	8	7	7	8	8	5	9	7.625
	U17	A2	9	8	8	6	6	7	4	10	7.25
	U17	A4	8	8	7	7	8	7	8	9	7.75
	U17	A5	8	8	6	5	9	6	2	9	6.625
	U18	A2	7	7	8	6	5	8	5	9	6.875
	U18	A4	7	9	7	7	7	6	4	9	7
	U18	A5	8	9	6	8	8	8	7	9	7.875
Gerencia	U19	A3	7	9	8	6	7	6	2	9	6.75
	U19	A4	9	9	6	5	8	6	2	9	6.75
	U19	A5	5	7	8	7	6	8	3	8	6.5
	U19	A6	6	7	6	6	6	9	6	8	6.75
	U19	A7	8	8	8	5	6	9	2	8	6.75
	U20	A6	4	9	6	7	6	9	3	7	6.375
	U20	A7	7	6	8	5	6	8	4	7	6.375
	U21	A4	8	8	6	6	6	7	5	9	6.875
	U21	A5	4	8	8	7	7	8	2	9	6.625
	U21	A6	6	7	6	8	8	9	2	6	6.5
	U21	A7	7	8	8	5	7	9	3	9	7
	TOTALES		7.014084507	7.67605634	7.18309859	6.22535211	6.67605634	7.91549296	4.57746479	8.73239437	7

6.3 Resultados

Los resultados se basan en la tabla 5.4, que concierne las calificaciones de los usuarios participantes en la encuesta. A continuación, se muestra el resultado por capacidades evaluadas.

6.3.1 Nivel de entendimiento de la metodología de Gestión de riesgos utilizada.

En la figura 5.1 se visualiza que más del 80% ha referido que la metodología de gestión de riesgos de seguridad de la información es de un nivel de entendimiento aceptable.

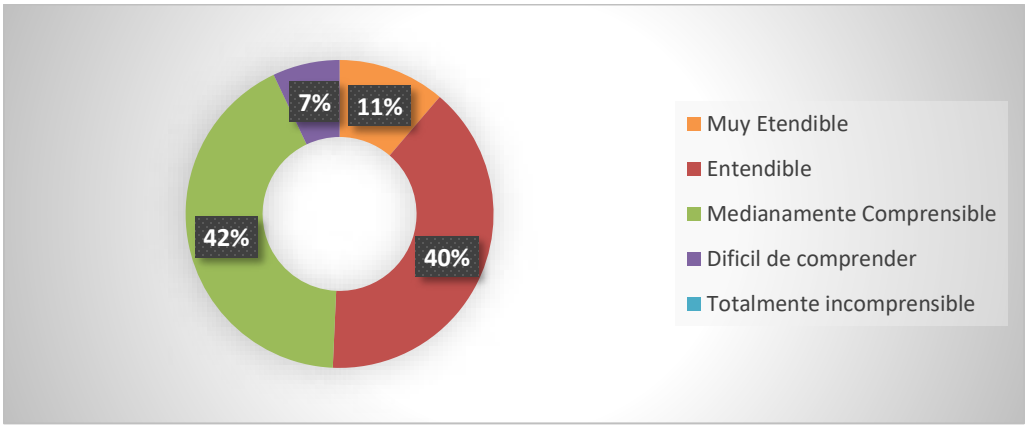

Figura 5.1. Calificaciones de nivel de entendimiento de metodología. Elaboración propia

6.3.2 Nivel de satisfacción de usabilidad de la aplicación web

En la figura 5.2 muestra el nivel de satisfacción de la aplicación web desarrollada, el cual es 60% de satisfacción en todas sus funcionalidades.

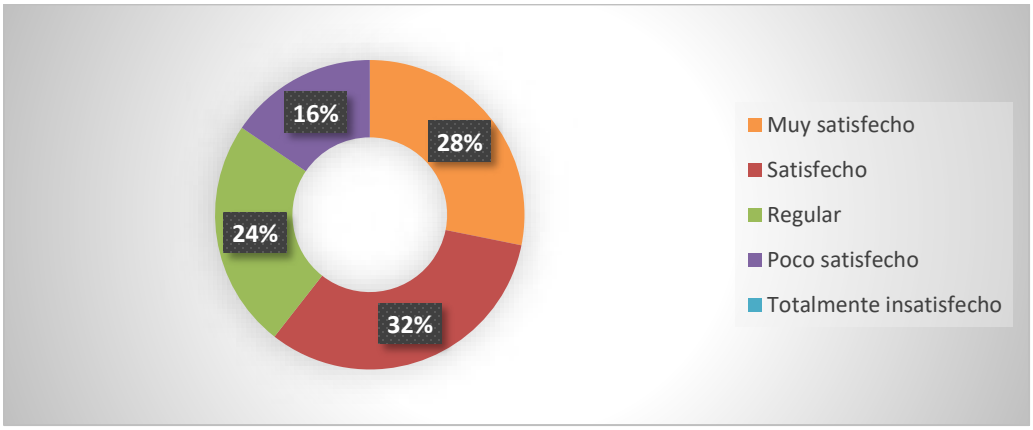

Figura 5.2. Calificaciones de nivel de usabilidad web. Elaboración propia

6.3.3 Nivel de satisfacción de usabilidad de la aplicación móvil

En la figura 5.3 se muestra un nivel de satisfacción alto de la aplicación móvil, y comparándola con la aplicación web, tiene mayor grado de preferencia.

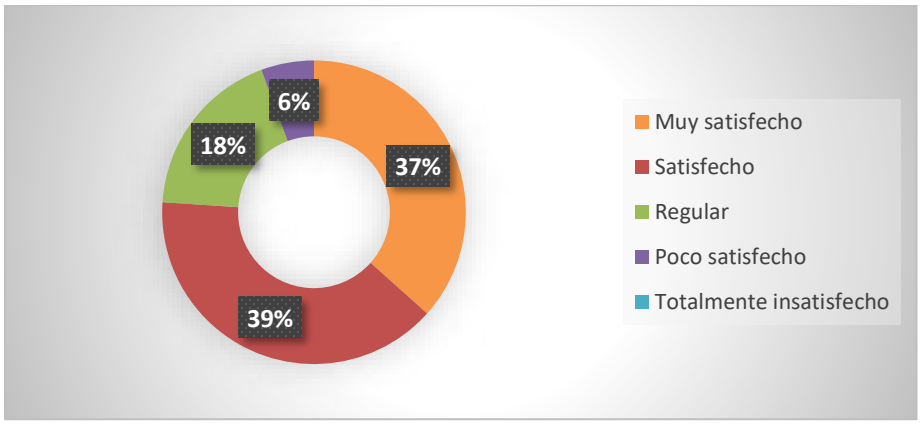

Figura 5.3. Calificaciones de nivel de usabilidad móvil. Elaboración propia

6.3.4 Rapidez en operaciones rutinarias del sistema

En la figura 5.4 se visualiza un nivel de rapidez del sistema, en mayor medida, regular.

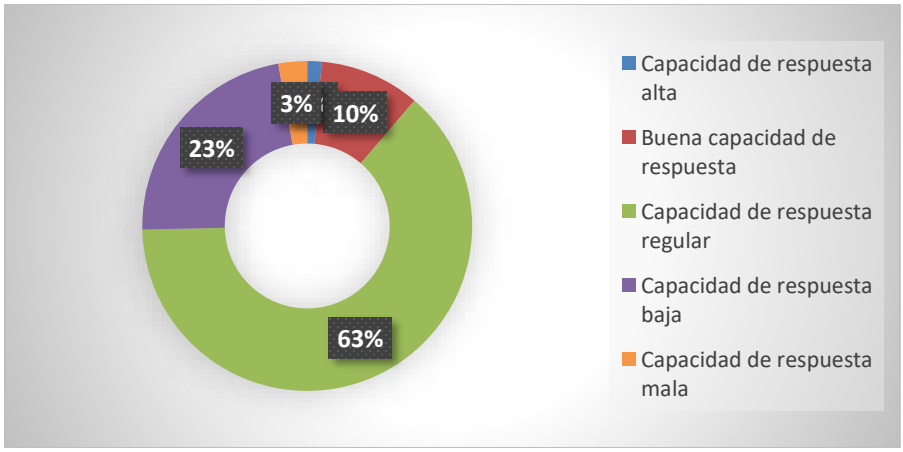

Figura 5.4. Calificaciones nivel de rapidez del sistema. Elaboración propia

6.3.5 Utilidad para las tareas requeridas.

En la figura 5.5 se muestra un nivel muy satisfactorio del nivel de utilidad de las aplicaciones con respecto a las aplicaciones desarrolladas.

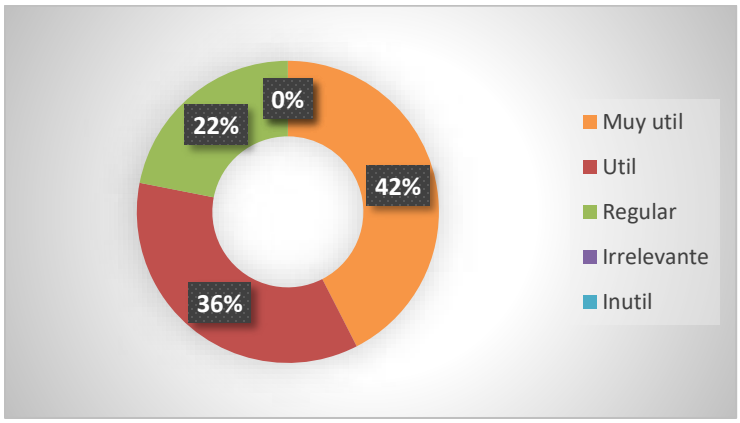

Figura 5.5. Calificaciones nivel de utilidad. Elaboración propia

CONCLUSIONES Y TRABAJOS FUTUROS

Conclusiones

En la presente investigación se detalló la importancia de salvaguardar la información de las empresas y sus activos de información. Para lo cual se presentó el desarrollo de un sistema web y móvil, ejecutándolo en una prueba piloto en una consultora de sistemas, de lo cual se llegó a las siguientes conclusiones:

- Luego de analizar y comparar las distintas metodologías existentes de gestión de seguridad de la información y estudiar su aplicación en una empresa del sector de consultoría de sistemas, se seleccionó y tomó como referencia a la metodología MAGERIT.
- Se logró modelar el uso de la metodología seleccionada, adaptando la metodología MAGERIT en el proceso de Gestión de Riesgos de Seguridad de la Información desarrollado en esta tesis y aplicado en la empresa consultora de software. Para lo cual se realizaron pruebas piloto, las cuales fueron favorables y con buena aceptación en su metodología.
- Se logró desarrollar una propuesta técnica de una aplicación web y móvil que sea el soporte de los procesos de Gestión de Riesgos de Seguridad de la Información definido anteriormente. Para lo cual se estudió, analizó, definió y explicó la arquitectura del software propuesta, definiendo las distintas tecnologías a utilizar y módulos funcionales a implementar para el desarrollo de las aplicaciones propuestas.
- Se logró planificar el desarrollo, implementación y despliegue de la propuesta tecnológica en la empresa seleccionada, para lo cual se desarrolló las aplicaciones web y móvil de acuerdo a los aspectos técnicos y funcionales detallados también en la presente investigación.
- Se establecieron las políticas y actividades de evaluación de riesgos de la información, para lo cual se tomó como prueba piloto la implementación de un sistema de seguridad de la información para la consultora, utilizando las aplicaciones web y móvil desarrolladas. Se evaluó el sistema INFORISK

mediante encuestas a los usuarios y obtuvo unas calificaciones aceptables que lo respaldan.

- La aplicación desarrollada INFORISK fue implementada de manera exitosa y se mantiene para ser utilizada de manera periódica por la empresa consultora, la cual a su vez validó el cumplimiento de las expectativas propuestas para la evaluación de riesgos de seguridad de la información.

Recomendaciones y trabajos futuros

- Tener en cuenta que la presente investigación está orientada a una consultora de sistema donde se puso énfasis en aplicar una metodología ágil que no demande muchos recursos para su implementación.
- Si bien los tiempos de respuesta de las aplicaciones se encuentran dentro del margen aceptado por los usuarios, esto se podría mejorar en futuras versiones. De acuerdo a las pruebas unitarias aplicadas, se verifica que el mayor tiempo de respuesta es debido al consumo de web services, debido a esto se tiene como trabajo futuro desarrollar optimizaciones en cuanto a tiempos de respuestas y de consumos de servicios web.
- Ampliar el alcance del Sistema de Gestión de Riesgos de Seguridad de la Información considerando la parametrización de entidades a fin de ser utilizado como un producto en distintas empresas.
- Desarrollar las funcionalidades al Sistema de Gestión de Riesgos aplicable también a mediciones de proyectos.

BIBLIOGRAFÍA

Adelmeyer Michael (2018). A Risk Management Tool for Cloud Computing Environments, Osnabrück University, Alemania. Recuperado de: https://aisel.aisnet.org/amcis2018/Security/Presentations/11

Alireza Shameli (2016). Taxonomy of Information Security Risk Assessment (ISRA). University of Quebec, Canadá. Recuperado de: https://doi.org/10.1016/j.cose.2015.11.001

AON (2019) Cyber Security Risk Report. AON Corporation.

Aubert Jocelyn, Mayer Nicolas (2017). An integrated conceptual model for information system security risk management. Software & Systems Modeling, vol 18, pp 2285 -2312. Recuperado de: doi.org/10.1007/s10270-018-0661-x

Beltran C (2019). Web Service & API Difference. Recuperado de: https://medium.com/beltranc/diferencia-entre-api-y-servicio-web-5f204af3aedb

EY (2019). Encuesta Global de Seguridad de la Información. Ernst & Young. Recuperado de: https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf

Chanchala Joshi, Umesh Kumar (2017). Information Security risks management framework. Journal of Information Security and Applications, vol 35, pp128-137. Recuperado de: doi.org/10.1016/j.jisa.2017.06.006

CISCO (2018). Reporte Anual de Ciberseguridad de CISCO 2018.

Crespo M. Paul (2016). Metodología de seguridad de la información para la gestión de riesgo informático aplicable a pymes. Universidad de Cuenca. Recuperado de: http://dspace.ucuenca.edu.ec/handle/123456789/26105

Cuentas Luciana (2018). ¿Cuáles son los delitos informáticos en Perú? Diario Correo, publicado el 17.06.2018.

Deloitte (2016). Artículo de Ley de Protección de Datos Personales, Enterprise Risk Services. Recuperado de: https://www2.deloitte.com/content/Deloitte/pe/Documents/risk/ley_n29733_la_experiencia_implementacion.pdf

Dávila Wendy (2017). Delitos Informáticos Perú. Resultado Legal. Recuperado de: http://resultadolegal.com/delitos-informaticos-peru

García Porras Johari, Huamani Pastor Sarita (2018). Information Security Risk Management model of Peruvian PYMES. Revista Peruana de Computación y Sistemas,1(1), 47,56. Recuperado de: doi.org/10.15381/rpcs.v1i1.14856

Huerta Antonio (2012). Introducción al análisis de riesgos – Metodologías. Security at Work. Recuperado de: https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i

IBM (2019). X-Force Threat Intelligence Index. IBM Security.

INCIBE (2017). Gestión de Riesgos, Una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad, Gobierno de España.

International Organization for Standardization (2009). ISO/IEC 31000:2009. Gestión del riesgo. Principios y Directrices. Suiza.

International Organization for Standardization (2014). ISO/IEC 27001:2013 Tecnologías de Información. Técnicas de Seguridad. Requerimientos. Suiza.

ISO.ORG (2018). Risk Management – Guidelines ISO 31000:2018

ISM3 Consortium (2009). Information Security Management Maturity Model.

IsoWin (2018). Los Activos de la Información en la norma ISO 27001 2017. Recuperado el 22.09.2019 de: https://isowin.org/blog/activos-ISO-27001

Llontop Diaz C. (2018). Gestión de riesgos de tecnologías de información de las empresas de Nephila Networks. UCV. Recuperado de: http://repositorio.ucv.edu.pe/handle/UCV/17596.

Markus Erb (2016). Gestión de Riesgo en la Seguridad Informática. Recuperado el 20.08.2019, de: https://protejete.wordpress.com/gdr_principal

Mataracioglu Tolga (2017). Proposal for next version of the ISO/IEC 27001. ISACA Journal, Vol 4, 2017.

Najar Pacheco (2015). La seguridad de la información: un activo valioso de la organización. Revista Vínculos. Recuperado de: doi.org/10.14483/2322939X.10518

Salesio M. Kiura.(2017). Information systems security risk management model in kenyan private chartered universities. European Journal of Computer Science and Information Technology, vol 5, 1-15. Recuperado de: http://www.eajournals.org/wp-content/uploads/Information-Systems-Security-Risk-Management-ISSRM-Model-in-Kenyan-Private-Chartered-Universities.pdf

Samuel E. Diego (2015). Los Beneficios y la importancia de gestionar la seguridad de la información. Recuperado el 15.08.2019, de: https://reportedigital.com/seguridad/la-seguridad-de-la-informacion

Santos Llanos D. (2016). Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en ISO 27001:2013, para una empresa de consultoría de software. PUCP. Recuperado de: http://hdl.handle.net/20.500.12404/7616.

Serban (2018). La importancia de la Seguridad de la información en la empresa. Recuperado el 20.08.2019, de: https://www.serban.es/la-importancia-de-la-seguridad-de-la-informacion-en-la-empresa

Stucchi Pierino (2017). El ABC de la protección de datos personales. Diario Gestión. Recuperado de: https://gestion.pe/blog/reglasdejuego/2017/06/el-abc-de-la-proteccion-de-datos-personales-data-privacy.html

Valencia Duque Francisco, Orozo Alzate Mauricio (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Revista Ibérica de Sistemas y Tecnologías de la Información n°22. Recuperado de: doi.org/10.17013/risti.22.73-88

Zúñiga Cortez Juan (2015). La información como activo estratégico en la administración de la Pyme. Red Internacional de Investigadores en Competitividad, Vol 9, Num. 1.

ANEXOS

ANEXO A: ENCUESTA DE EVALUACIÓN DE SATISFACCION DE APLICACIONES INFORISK

Encuesta de Evaluación de nivel de Satisfacción de aplicaciones INFORISK

I. Datos

1. Puesto Laboral: _____

2. Tipo de Usuario Representado (Selección única)
a) Usuario Administrador
b) Usuario Gestor de Proyecto
c) Usuario Custodio
d) Usuario experto/Evaluador
e) Usuario Gerencia

3. Actividad Realizada (Una o varias opciones)
☐ A1. Parametrizaciones del Sistema
☐ A2. Registrar, eliminar, editar y/o evaluar Activos de Información
☐ A3. Registrar, eliminar, editar amenazas y/o vulnerabilidades
☐ A4. Estimación de vulnerabilidades
☐ A5. Evaluación de Impacto y riesgos
☐ A6. Gestión de Controles: Tratamientos de riesgos mediante salvaguardas y oportunidades de mejora.
☐ A7. Revisión de Reportes analíticos.

II. Evaluaciones

Las siguientes preguntas tendrán una escala de evaluación del 1 al 10, donde 1 represente poca intensidad, y 10 mucha intensidad respecto a la pregunta planteada.

1. ¿Cuál es el nivel de entendimiento de la metodología de gestión de riesgos que se planteó en las aplicaciones?

Inentendible	1	2	3	4	5	6	7	8	9	10	Muy entendible

2. ¿Cuál es el nivel de satisfacción de la aplicación web en cuanto a usabilidad?

Insatisfecho	1	2	3	4	5	6	7	8	9	10	Satisfecho

3. ¿Cuál es el nivel de satisfacción de la aplicación móvil b en cuanto a usabilidad?

Insatisfecho	1	2	3	4	5	6	7	8	9	10	Muy insatisfecho

4. En cuanto a las funcionalidades de las aplicaciones ¿Qué tan simple de comprender son?

Incomprensible	1	2	3	4	5	6	7	8	9	10	Sencillo de comprender

5. ¿Qué tan fácil es de aprender el funcionamiento del sistema?

Complicado	1	2	3	4	5	6	7	8	9	10	Muy fácil

6. ¿Cuál es la capacidad de respuesta de las aplicaciones acorde a los requerimientos?

No cumple	1	2	3	4	5	6	7	8	9	10	Cumple los requisitos

7. Para las aplicaciones web y móvil. Califique la rapidez de las operaciones y consultas del sistema.

Muy lento	1	2	3	4	5	6	7	8	9	10	Rápido

8. Para UD. ¿Qué tan útil considera que son las aplicaciones para las tareas y actividades de gestión de riesgos de la información?

Poco útil	1	2	3	4	5	6	7	8	9	10	Muy útil

9. En general, ¿Considera que las aplicaciones testeadas ayudaran a salvaguardar de manera eficiente los activos de información frente a riesgos?

SI	NO

III. Respuestas Libres

1. Recomendaciones y/o sugerencias respecto a la aplicación web

_____

_____

2. Recomendaciones y/o sugerencias respecto a la aplicación móvil

_____

_____

INFORISK
securing information assets

REPORTE LISTADO Y EVALUACION DE ACTIVOS DE INFORMACIÓN

Fecha: 02.04.2020 **Proyecto:** Info-2020

PROCESO	CUSTODIO	Dueño Activo	VIGENCIA	Valoración Promedio del Activo					
				Confidencialidad	Integridad	Disponibilidad	Trazabilidad	Autenticidad	Valor Activo
Soporte Complementario	Manuel - 45789625	OTI	X	1	2	3	4	3	2.6
Proyectos nivel 3	Omar L - 35426879	Gerencia TI	X	5	5	5	3	5	4.6
Proyectos nivel 2	Carlos M - 41589477	Propios		3	4	5	2	3	3.4
Proyectos nivel 2	Miguel C - 47230158	Propios	X	3	4	5	2	3	3.4
Soporte Complementario	Manuel - 45789625	OTI	X	2	5	5	3	5	4
Proyectos nivel 1	Omar L - 35426879	Gerencia Comercial	X	5	5	5	4	5	4.8
Proyectos nivel 1	Omar L - 35426879	Gerencia Comercial	X	4	5	4	5	5	4.6
Proyectos nivel 2	Omar L - 35426879	Gerencia General	X	5	5	5	3	5	4.6
Procesos Internos	Rita V - 04455778	RRHH	X	4	5	3	3	5	4
Proyectos nivel 3	Manuel - 45789625	Cliente	X	5	4	4	3	4	4
Seguridad Técnica	Victor M- 36584752	OTI	X	3	3	5	2	3	3.2
Soporte Complementario	Rita V - 04455778	RRHH	X	2	3	3	3	3	2.8
Soporte Complementario	Rita V - 04455778	RRHH	X	2	2	3	3	3	2.6
Soporte Complementario	Manuel - 45789625	OTI	X	1	2	2	1	3	1.8
Soporte Complementario	Manuel - 45789625	OTI	X	1	2	1	1	2	1.4
Soporte Complementario	Manuel - 45789625	OTI	X	3	3	4	3	4	3.4
Proyectos nivel 2	Sofia C - 41587896	Operaciones	X	5	4	4	2	4	3.8
Proyectos nivel 3	Sofia C - 41587896	Operaciones	X	3	3	4	2	3	3
Soporte Complementario	Manuel - 45789625	OTI	X	2	2	5	2	3	2.8
Proyectos nivel 2	Rita V - 04455778	RRHH	X	4	4	4	3	3	3.6
Soporte Complementario	Manuel - 45789625	OTI	X	3	3	5	2	3	3.2
Proyectos nivel 1	Sofia C - 41587896	Operaciones	X	5	4	4	3	4	4
Proyectos nivel 1	Sofia C - 41587896	Operaciones	X	4	4	4	3	4	3.8
Formativo	Rita V - 04455778	RRHH	X	3	3	4	3	3	3.2
Proyectos nivel 1	Sofia C - 41587896	Operaciones	X	4	5	4	4	3	4
Proyectos nivel 1	Omar L - 35426879	Comercial	X	5	4	4	2	4	3.8
Administrativo	Ani R. - 04966557	Logística	X	4	4	3	2	4	3.4
Proyectos nivel 3	Ani R. - 04966557	logística	X	4	4	4	5	4	4.2
Proyectos	Omar L - 35426879	Comercial	X	5	5	5	4	5	4.8

Sección B

INFORISK
securing information assets

REPORTE LISTADO Y EVALUACION DE ACTIVOS DE INFORMACIÓN

Fecha: 02.04.2020 **Proyecto:** Info-2020

ID	DESCRIPCION ACTIVO	CATEGORIA	TIPO	CLASIFICACION	DEPENDENCIA	SERVICIO
ACT-F001	Servidor de BK - HP Proliant DL380	Físico	Equipo de Procesamiento	Uso Interno	OTI-Oficina de TI	Infraestructura
ACT-F002	Servidor Clientes SAP - DELL ProwerEdge T310 Intel Xeon	Físico	Equipo de Procesamiento	Uso Interno	OTI-Oficina de TI	Hosting
ACT-F003	Laptop Lenovo Ideapad 530s - CRKF52	Físico	Equipo de Computo	Uso laboral diario	OTI-Oficina de TI	Consultoría
ACT-F004	Laptop Lenovo Ideapad 530s - CFK030	Físico	Equipo de Computo	Uso laboral diario	OTI-Oficina de TI	Consultoría
ACT-F005	Router Cisco ISR 4221	Físico	Equipo de Comunicaciones	Uso Interno	OTI-Oficina de TI	Infraestructura
ACT-S006	Software Firmas Electrónicas - Proveedor SUNAT V 2.5	Software	Software/ soluciones para ventas	Uso Clientes	Gerencia Comercial	Consultoría
ACT-S007	Software SAP Fiori - Gestion Tickets	Software	Software/ soluciones para ventas	Uso Clientes	Gerencia Comercial	Consultoría
ACT-I008	Contratos con Clientes	Información	Información electrónica	Uso Interno	Gerencia Comercial	Consultoría
ACT-I009	Datos de Planillas de pagos a trabajadores	Información	Información electrónica	Uso Interno	RRHH	Complementario Interno
ACT-I010	Alojamiento/ Hosting BD de clientes	Servicio	Procesamiento	Uso Clientes	OTI-Oficina de TI	Hosting
ACT-F011	Antirvirus Eset Nod32 x25 lic Premium	Software	Licencias de soporte	Uso Interno	OTI-Oficina de TI	Soporte
ACT-F012	Equipo de control biométrico ZK-S900	Físico	Mobiliario y equipamiento	Uso laboral soporte	RRHH	Infraestructura
ACT-I013	B.D Control de Asistencia Ctrl Bio.	Información	Información electrónica	Uso Interno	RRHH	Complementario Interno
ACT-S014	Licencias Microsoft Office 2016 x25	Software	Licencias de soporte	Uso laboral soporte	OTI-Oficina de TI	Soporte
ACT-S015	Licencias Microsoft Windows 10 Home x 30	Software	Licencias de soporte	Uso laboral soporte	OTI-Oficina de TI	Soporte
ACT-S016	Licencias Windows Server 2016	Software	Licencias de soporte	Uso Proyectos	OTI-Oficina de TI	Soporte
ACT-S017	Licencias SAP R3/ Partner	Software	Licencias de proyectos	Uso laboral	Gerencia Operaciones	Consultoría
ACT-S018	Licencias Jira Enterprise x10	Software	Licencias de soporte	Uso laboral soporte	Gerencia Operaciones	Complementario Interno
ACT-F019	Sensores de temperatura para enfriamiento DataCenter	Físico	Otros Equipos	Uso laboral soporte	OTI-Oficina de TI	Infraestructura
ACT-F020	Smartphones Huawei P20 x10	Físico	Equipo de Comunicaciones	Uso laboral diario	RRHH	Complementario Interno
ACT-F021	UPS Sistema de alimentación ininterrumpida	Físico	Otros Equipos	Uso laboral soporte	OTI-Oficina de TI	Seguridad y redundancia
ACT-P022	Consultores Funcionales SAP	Personal	Empleados	Fuerza laboral	Gerencia Operaciones	Consultoría
ACT-P023	Consultores Técnicos ABAP, Java, PHP	Personal	Empleados	Fuerza laboral	Gerencia Operaciones	Consultoría
ACT-P024	Practicantes	Personal	Empleados	Fuerza laboral	RRHH	Varios
ACT-P025	Personal Certificado DBA	Personal	Empleados	Fuerza laboral	Gerencia Operaciones	Soporte
ACT-P026	Equipo de Ventas y Marketing	Personal	Empleados	Fuerza laboral	Gerencia Comercial	Ventas
ACT-P027	Personal administrativo y de RRHH	Personal	Empleados	Fuerza laboral	Logística	Administrativos
ACT-F028	Oficina de Fabrica de Software	Físico	Infraestructura física	Uso laboral diario	Logística	Infraestructura
ACT-C029	Claves de Firma electrónica / Proveedor SUNAT	Claves criptográficas	Clave firma electrónica	Uso Clientes	Gerencia Comercial	Consultoría

INFORISK
securing information assets

REPORTE ANÁLISIS DE AMENAZAS Y VULNERABILIDADES

Fecha: 02.04.2020 **Proyecto:** Info-2020

AMENAZA			VULNERABILIDAD					
TIPO	CATEGORIA	NIVEL AME.PROM	VULNERABILIDAD	CAP PREV.	CAP DETEC.	CAP CORREC.	NIVEL VUL.	PROB. OCCUR
Amen. Hardware	ELEC	4	Corte de fluido eléctrico no programado	4	4	2	2.667	3.333
Amen. Hardware	ELEC	4	Falla en caja fusibles	5	4	5	1.333	2.667
Amen. Hardware	PER	5	No transportar de manera adecuada los equipos, generando daños físicos	3	4	4	2.500	3.750
Amen. Hardware	SEG	3	Permitir llevarse equipos de trabajo a locales del cliente	3	5	2	2.667	2.833
Amen. Hardware	SEG	2	Manipulación de personal no calificado	2	5	3	2.667	2.333
Amen. Software	PER	2	Analistas no calificados, sin certificación / experiencia	3	2	2	3.667	2.833
Amen. Software	PRO	1	Sabotaje interno de equipo de trabajo	1	3	4	3.500	2.250
Amen. Información	SEG	2	Falta de revisión de control de accesos a niveles de información confidencial	2	4	4	2.667	2.333
Amen. Información	SEG	1	Falta de control de alertas y notificaciones en modificación de archivos susceptibles	2	3	4	3.000	2.000
Amen. Servicios	SEG	1	Ataques externos/ internos frente a tráfico de datos por servicios de hosting empresarial	1	1	1	5.000	3.000
Amen. Seguridad	SW	2.5	No mantener control de vencimiento licencias/licencia expirada	2	2	4	3.333	2.917
Amen. Seguridad	ELEC	2.2	Falta de mantenimiento continuo	2	3	4	3.000	2.600
Amen. Información	SEG	3.1	No existe respaldo y BKs de Asistencias y controles de acceso	3	2	3	3.333	3.217
Amen. Software	SW	4	Licencia desfasada	3	2	3	3.333	3.667
Amen. Software	SW	3	Licencia cancelada/clonada	2	2	3	3.667	3.333
Amen. Software	SW	4.1	Licencia desfasada	3	3	3	3.000	3.550
Amen. Operaciones	SW	3.6	No se realiza actualizaciones de licencia de manera periódica	3	3	2	3.333	3.467
Amen. Operaciones	SW	2.9	Irregularidades en la custodia y distribución de licencias	3	2	3	3.333	3.117
Amen. Soporte	SP	2.7	Falta de mantenimiento equipo	2	2	2	4.000	3.350
Amen. Información	INF	1.3	No se cuenta con antivirus para móvil	3	4	2	3.000	2.150
Amen. Información	INF	1.5	No se restringe el uso personal	2	1	2	4.333	2.917
Amen. Soporte	SP	1.9	Personal no preparado para instalaciones y configuraciones	2	2	2	4.000	2.950
Amen. Continuidad	Co	3.7	Personal pide licencia por distintos motivos	2	3	3	3.333	3.517
Amen. Operaciones	OP	3.5	Personal no preparado para exigencias del cliente	3	2	3	3.333	3.417
Amen. Software	SW	4.2	No contar con protocolo formal gestión de versiones	3	2	1	4.000	4.100
Amen. Operaciones	OP	2.8	No contar con protocolo de inducción y formación continua al personal	4	3	2	3.000	2.900
Amen. Operaciones	OP	4.3	No contar con protocolo de teletrabajo y conexiones	3	2	2	3.667	3.983
Amen. Personal	PER	3.9	Permitir desplazamiento de personal sin transporte privado	3	3	2.5	3.167	3.533
Amen. Seguridad	SEG	2.1	Acceso sin verificación	3	1	2	4.000	3.050

INFORISK
securing information assets

REPORTE ANÁLISIS DE AMENAZAS Y VULNERABILIDADES

Fecha: 02.04.2020 **Proyecto:** Info-2020

ACTIVOS				AMENAZA	
ID-ACTIVO	DESCRIPCION ACTIVO	CATEGORIA	TIPO	ID_AME	DESC AMENAZA
ACT-F001	Servidor de BK - HP Proliant DL380	Físico	Equipo de Procesamiento	AME-0001	Fallo Sistema Aire acondicionado/ Refrigeración
ACT-F002	Servidor Clientes SAP - DELL ProwerEdge T310 Intel Xeon	Físico	Equipo de Procesamiento	AME-0002	Interrupción de servicios de Disponibilidad 24/7
ACT-F003	Laptop Lenovo Ideapad 530s - CRKF52	Físico	Equipo de Computo	AME-0003	Uso inadecuado de equipos
ACT-F004	Laptop Lenovo Ideapad 530s - CFK030	Físico	Equipo de Computo	AME-0004	Robo equipo o componentes
ACT-F005	Router Cisco ISR 4221	Físico	Equipo de Comunicaciones	AME-0005	Desconfiguración de equipo
ACT-S006	Software Firmas Electrónicas - Proveedor SUNAT V 2.5	Software	Software/ soluciones para ventas	AME-0006	Errores de utilización ocurridos durante la recolección y transmisión de datos
ACT-S007	Software SAP Fiori - Gestion Tickets	Software	Software/ soluciones para ventas	AME-0007	Adulteración intencional del software
ACT-I008	Contratos con Clientes	Información	Información electrónica	AME-0008	Acceso no autorizado a información
ACT-I009	Datos de Planillas de pagos a trabajadores	Información	Información electrónica	AME-0009	Modificación no autorizada a información
ACT-I010	Alojamiento/ Hosting BD de clientes	Servicio	Procesamiento	AME-0010	Errores de monitorización, trazabilidad o registros del tráfico de información
ACT-F011	Antivirus Eset Nod32 x25 lic Premium	Software	Licencias de soporte	AME-0011	Infectar con virus
ACT-F012	Equipo de control Acceso biométrico ZK-S900	Físico	Mobiliario y equipamiento	AME-0012	Falla Provisión eléctrica
ACT-I013	B.D Control de Asistencia Ctrl Bio.	Información	Información electrónica	AME-0013	Adulteración de datos de asistencia y controles
ACT-S014	Licencias Microsoft Office 2016 x25	Software	Licencias de soporte	AME-0014	No poder editar archivos de office
ACT-S015	Liicencias Microsoft Windows 10 Home x 30	Software	Licencias de soporte	AME-0015	Ocasionar baja de problemas de conexión de trabajadores
ACT-S016	Licencias Windows Server 2016	Software	Licencias de soporte	AME-0016	Ocasionar caída de soporte y servicio
ACT-S017	Licencias SAP R3/ Partner	Software	Licencias de proyectos	AME-0017	Disminución de rendimiento del sw frente a competidores
ACT-S018	Licencias Jira Enterprise x10	Software	Licencias de soporte	AME-0018	Acceso de personas no autorizadas a avances de proyectos restringidos
ACT-F019	Sensores de temperatura para enfriamiento DataCenter	Físico	Otros Equipos	AME-0019	Ocasionar falla en advertencia o regulaciones
ACT-F020	Smartphones Huawei P20 x10	Físico	Equipo de Comunicaciones	AME-0020	Infectar con virus y vulnerar información confidencial de empresa
ACT-F020	Smartphones Huawei P20 x10	Físico	Equipo de Comunicaciones	AME-0021	Robo de equipo
ACT-F021	UPS Sistema de alimentación ininterrumpida	Físico	Otros Equipos	AME-0022	Uso inadecuado de equipos
ACT-P022	Consultores Funcionales SAP	Personal	Empleados	AME-0023	Ausencia de servicios del consultor
ACT-P022	Consultores Funcionales SAP	Personal	Empleados	AME-0024	Bajo rendimiento en servicios a clientes
ACT-P023	Consultores Técnicos ABAP, Java, PHP	Personal	Empleados	AME-0025	Realizar modificaciones no autorizadas en el código de programas
ACT-P024	Practicantes	Personal	Empleados	AME-0026	Ocasionar fallas en equipos o aplicativos
ACT-P025	Personal Certificado DBA	Personal	Empleados	AME-0027	Dificultad en el desplazamiento hacia el centro de trabajo
ACT-P026	Equipo de Ventas y Marketing	Personal	Empleados	AME-0028	Asaltos cuando se dirigen a reuniones de ventas
ACT-P027	Personal administrativo y de RRHH	Personal	Empleados	AME-0029	Uso de credenciales falsificadas

INFORISK
securing information assets

REPORTE DE EVALUACIÓN DE RIESGOS

Fecha: 02.04.2020 **Proyecto:** Info-2020

Activo		Amenaza		VULNERABILIDAD	
ID-ACTIVO	DESCRIPCION ACTIVO	ID_AME	DESC AMENAZA	VULNERABILIDAD	Prob. Ocurr.
ACT-F001	Servidor de BK - HP Proliant DL380	AME-0001	Fallo Sistema Aire acondicionado/ Refrigeración	Corte de fluido eléctrico no programado	3.33
ACT-F002	Servidor Clientes SAP - DELL ProwerEdge T310 Inel Xeon	AME-0002	Interrupción de servicios de Disponibilidad 24/7	Falla en caja fusibles	2.67
ACT-F003	Laptop Lenovo Ideapad 530s - CRKF52	AME-0003	Uso inadecuado de equipos	No transportar de manera adecuada los equipos, generando daños físicos	3.67
ACT-F004	Laptop Lenovo Ideapad 530s - CFK030	AME-0004	Robo equipo o componentes	Permitir llevarse equipos de trabajo a locales del cliente	2.83
ACT-F005	Router Cisco ISR 4221	AME-0005	Desconfiguración de equipo	Manipulación de personal no calificado	2.78
ACT-S006	Software Firmas Electrónicas - Proveedor SUNAT V 2.5	AME-0006	Errores de utilización ocurridos durante la recolección y transmisión de datos	Analistas no calificados, sin certificación / experiencia	4.60
ACT-S007	Software SAP Fiori - Gestión Tickets	AME-0007	Adulteración intencional del software	Sabotaje interno de equipo de trabajo	3.35
ACT-I008	Contratos con Clientes	AME-0008	Acceso no autorizado a información	Falta de revisión de control de accesos a niveles de información confidencial	2.58
ACT-I009	Datos de Planillas de pagos a trabajadores	AME-0009	Modificación no autorizado a información	Falta de control de alertas y notificaciones en modificación de archivos susceptibles	2.50
ACT-I010	Alojamiento/ Hosting BD de clientes	AME-0010	Errores de monitorización, trazabilidad o registros del tráfico de información	Ataques externos/ internos frente a tráfico de datos por servicios de hosting empresarial	4.00
ACT-F011	Antivirus Eset Nod32 x25 Lic. Premium	AME-0011	Infectar con virus	No mantener control de vencimiento licencias/licencia expirada	2.92
ACT-F012	Equipo de control Acceso biométrico ZK-S900	AME-0012	Falla Provisión eléctrica	Falta de mantenimiento continuo	1.80
ACT-I013	B.D Control de Asistencia Ctrl Bio.	AME-0013	Adulteración de datos de asistencia y controles	No existe respaldo y BKs de Asistencias y controles de acceso	3.22
ACT-S014	Licencias Microsoft Office 2016 x25	AME-0014	No poder editar archivos de office	Licencia desfasada	3.67
ACT-S015	Licencias Microsoft Windows 10 Home x 30	AME-0015	Ocasionar baja de problemas de conexión de trabajadores	Licencia cancelada/clonada	3.33
ACT-S016	Licencias Windows Server 2016	AME-0016	Ocasionar caída de soporte y servicio	Licencia desfasada	3.75
ACT-S017	Licencias SAP R3/ Partner	AME-0017	Disminución de rendimiento del sw frente a competidores	No se realiza actualizaciones de licencia de manera periódica	3.47
ACT-S018	Licencias Jira Enterprise x10	AME-0018	Acceso de personas no autorizadas a avances de proyectos restringidos	Irregularidades en la custodia y distribución de licencias	3.12
ACT-F019	Sensores de temperatura para enfriamiento DataCenter	AME-0019	Ocasionar falla en advertencia o regulaciones	Falta de mantenimiento equipo	3.35
ACT-F020	Smartphones Huawei P20 x10	AME-0020	Infectar con virus y vulnerar información confidencial de empresa	No se cuenta con antivirus para móvil	3.25
ACT-F020	Smartphones Huawei P20 x10	AME-0021	Robo de equipo	No se restringe el uso personal	3.42
ACT-F021	UPS Sistema de alimentación ininterrumpida	AME-0022	Uso inadecuado de equipos	Personal no preparado para instalaciones y configuraciones	2.90
ACT-P022	Consultores Funcionales SAP	AME-0023	Ausencia de servicios del consultor	Personal pide licencia por distintos motivos	3.72
ACT-P022	Consultores Funcionales SAP	AME-0024	Bajo rendimiento en servicios a clientes	Personal no preparado para exigencias del cliente	3.57
ACT-P023	Consultores Técnicos ABAP, Java, PHP	AME-0025	Realizar modificaciones no autorizadas en el código de programas	No contar con protocolo formal gestión de versiones	4.10
ACT-P024	Practicantes	AME-0026	Ocasionar fallas en equipos o aplicativos	No contar con protocolo de inducción y formación continua al personal	2.90
ACT-P025	Personal Certificado DBA	AME-0027	Dificultad en el desplazamiento hacia el centro de trabajo	No contar con protocolo de teletrabajo y conexiones	3.98

INFORISK
securing information assets

REPORTE DE EVALUACIÓN DE RIESGOS

Fecha: 02.04.2020

Proyecto: Info-2020

Riesgo		Evaluación del Nivel de Impacto del Riesgo						Nivel de exposición al Riesgo			
ID_RIS	DESC. RIESGO	ASPECTO ECONOMICO	ASPECTO CONTINUIDAD	ASPECTO LEGAL	ASPECTO DE IMAGEN	ASPECTO CONTRACTUAL	IMPACT PROM.	Nivel Riesg	Cant. Evaluador	Tasación	Indicador
RIS-001	Perder registro de backup de transacciones de clientes	4.5	4.2	4.6	5	4.1	4.48	14.93	7/8	Alto	No Aceptable
RIS-002	Perder servicio brindado de Alojamiento de BD a clientes	4.6	4.5	5	4.8	4.6	4.7	12.53	7/7	Alto	No Aceptable
RIS-003	No se puede atender los requerimientos de soporte	3.8	3	3	4	3	3.36	12.32	4/6	Alto	No Aceptable
RIS-004	Divulgación de información confidencial en equipo	3	3	2.5	3	2.2	2.74	7.76	9/9	Medio	No Aceptable
RIS-005	Corte de servicio de internet y red interno para soporte a clientes	4.2	4.5	4	4	3.5	4.04	11.24	6/8	Alto	No Aceptable
RIS-006	Parametrizaciones de software no cumple con requisitos definidos	4.8	4.6	4	5	4.5	4.58	21.07	12/12	Extremo	No Aceptable
RIS-007	Software con mal funcionamiento o malware	5	4.5	5	5	4	4.7	15.75	8/8	Muy Alto	No Aceptable
RIS-008	Divulgar datos referentes a contrataciones y acuerdos	4.8	4	3.5	4.2	3.8	4.06	10.49	7/7	Alto	No Aceptable
RIS-009	Pérdida económica por modificaciones a planilla de pagos	5	3	3	3.5	3.8	3.66	9.15	7/9	Medio	No Aceptable
RIS-010	Corte de servicio de almacenamiento de BD	4.8	4.6	4	5	4.2	4.52	18.08	8/12	Muy Alto	No Aceptable
RIS-011	Pérdida de archivos infectados	3.5	4	3.8	4	3.8	3.82	11.14	8/12	Alto	No Aceptable
RIS-012	No se puede registrar los accesos del personal	3	3.5	1	3	3	2.7	4.86	4/4	Bajo	Aceptable
RIS-013	Falta de control de asistencia de personal por adulteración	3.5	3	3	3	2	2.9	9.33	5/5	Medio	No Aceptable
RIS-014	No se puede atender los requerimientos funcionales	2.5	2.5	2	3.5	2	2.5	9.17	5/5	Medio	No Aceptable
RIS-015	Sin acceso a actualizaciones del S.O	3	3.5	3	4	3	3.3	11.00	5/5	Alto	No Aceptable
RIS-016	Perdida del servicio de soporte y de actualizaciones	3	3.5	3.9	4.2	4	3.72	13.95	5/6	Alto	No Aceptable
RIS-017	No se puede acceder al ERP ocasionando insatisfacción en clientes	3	4.3	4.2	4.2	4	3.94	13.66	4/4	Alto	No Aceptable
RIS-018	Divulgación y/o modificaciones a proyectos gestionados	3.6	4	4	4.5	4	4.02	12.53	6/6	Alto	No Aceptable
RIS-019	Ocasiona sobrecalentamiento en servidores del Datacenter	3.8	3.6	3.9	4.2	4.6	4.02	13.47	6/6	Alto	No Aceptable
RIS-020	Afecta al rendimiento y uso del equipo de la empresa	2	1	1	2	1	1.4	4.55	6/6	Bajo	Aceptable
RIS-021	Divulgar datos personales y propios de la empresa	3	1.8	1.6	4.2	1.2	2.36	8.06	7/7	Medio	No Aceptable
RIS-022	No se esta preparado frente a imprevistos de falla eléctrica	4	3	3	4	2	3.2	9.28	7/7	Medio	No Aceptable
RIS-023	Falla en servicio brindado a cliente e incumplimiento de bolsa de horas	4.6	5	4.8	5	5	4.88	18.14	7/8	Muy Alto	No Aceptable
RIS-024	Incumplimiento de consultoría especializada y de calidad a clientes	4.6	4	4	5	5	4.52	16.12	7/9	Muy Alto	No Aceptable
RIS-025	Falla o alteración de procedimientos funcional en software de clientes	4	4.2	4.5	4.6	4.2	4.3	17.63	10/10	Muy Alto	No Aceptable
RIS-026	Perdida de registros o archivos por alteración sin procedimientos adecuados	3.9	4	4	4.5	4	4.08	11.83	11/11	Alto	No Aceptable
RIS-027	Incumplimiento de soporte brindado a clientes	4.8	4.5	4	5	4.5	4.56	18.16	8/8	Muy Alto	No Aceptable
RIS-028	Ausencia y repercusiones en ventas corporativas	4.6	3.5	3.2	4.5	3.8	3.92	13.85	7/7	Alto	No Aceptable