

**Análisis y gestión de requerimientos para un sistema de gestión de riesgos en
seguridad informática**

autor

NILSA NEREIDA SATOVA ARIAS

Director

LUZ MARINA SANTOS JAIMES

Ph.D. Ciencias de la computación y matemáticas computacional

**INGENIERÍA DE SISTEMAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA,
SISTEMAS Y TELECOMUNICACIONES
FACULTAD INGENIERÍAS Y ARQUITECTURA**



**UNIVERSIDAD DE PAMPLONA
PAMPLONA, COLOMBIA**

2022

Tabla de contenido

Resumen	9
Capítulo 1. Planteamiento y formulación del problema	11
1.1 Planteamiento	11
1.2 Justificación	11
1.3 Objetivos	11
1.3.1 General	11
1.3.2 Específicos	11
1.4 Metodología	12
1.5 Antecedentes del problema (estado del arte)	12
1.5.1 Trabajo 1:	12
1.5.2 Trabajo 2:	13
1.5.3 Trabajo 3:	13
1.5.4 Trabajo 4:	13
1.5.5 Trabajo 5:	14
1.5.6 Trabajo 6:	14
1.5.7 Trabajo 7:	15
1.5.8 Trabajo 8:	15
1.5.9 Trabajo 9:	15
1.5.10 Trabajo 10:	16

1.6. Formulación	16
1.7. Resultados o alcances esperados	16
Capítulo 2. Marco referencial	16
2.1 Marco Contextual	17
2.2 Marco Normativo	20
2.2.1 Ley 1273 del 2009	20
2.2.2 Ley 87 de 1993	21
2.3 Marco teórico	22
2.3.1 Gestión de los riesgos de TI	22
2.3.2 Seguridad informática	25
2.3.3 Estándares de seguridad	27
Capítulo 3. Comparación de herramientas y metodologías existentes de soporte para la gestión de riesgos en seguridad informática.	29
3.1 Comparación de herramientas para la gestión de riesgos	29
3.2 Comparación entre la metodología Margerit y Octave	33
Capítulo 4. Requerimientos para la elaboración y soporte para el desarrollo de software	37
4.1 Especificación de requerimientos	37
4.1.1 Lista de requerimientos	37
4.2 Clasificaciones a tener en cuenta	40

4.3 Criterios Básicos	43
4.3.1 Criterios de evaluación del riesgo	43
4.3.2 Criterios de impacto	43
4.3.3 Criterios de aceptación del riesgo	44
4.4 Alcance y límites para la gestión de riesgos en seguridad de la información.	45
4.4.1 Identificación de riesgos.	45
4.4.2 Análisis de riesgos	45
4.5 Etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO27005.	46
4.6 Identificación de controles existentes	50
4.7 Identificación de las vulnerabilidades	51
4.8 Identificación de las consecuencias	57
4.9 Evaluación de riesgo	58
4.10 Valoración de controles para el tratamiento de riesgos	62
4.11 Mapa de riesgos	69
4.12 Plantilla de controles genéricos para la gestión de riesgos informáticos	70
Capítulo 5. Requisitos y casos de uso	80
5.1 Requisitos no funcionales	80
5.2 Requisitos funcionales	81
5.3 Estándar de análisis y modelado	81

5.3.1 Identificación de casos de uso	81
5.3.2 Casos de uso para rol administrador	82
5.3.3 Casos de uso para rol operador	101
5.3.4 Casos de uso para rol viewer (espectador)	109
Conclusiones	¡Error! Marcador no definido.
Referencias bibliográficas	113

Índice de tablas

Tabla 1 Normas ISO gestión de seguridad de la información.....	18
Tabla 2. Comparativa de herramientas para la gestión de riesgos	29
Tabla 3. Comparativa de metodologías del análisis del riesgo	33
Tabla 4. Criterios de Clasificación	40
Tabla 5. Niveles de Clasificación	41
Tabla 7. Amenazas comunes	46
Tabla 8. Fuentes de amenazas humanas	48
Tabla 9 Vulnerabilidades conocidas y métodos para la valoración de la misma.	51
Tabla 10. Matriz de calificación, evaluación y respuesta a los riesgos	58
Tabla 11. Especificaciones de probabilidad	59
Tabla 12. Especificación del nivel de impacto	59
Tabla 13. Ejemplo de Análisis de Riesgo.....	61
Tabla 14. Evaluación de la zona de riesgo	61
Tabla 15. Calificación de criterios de controles	63
Tabla 16. Valoración de controles.....	65
Tabla 17. Calificación del riesgo residual, después de aplicar controles	65
Tabla 18. Disminución de cuadrantes, después de aplicar un control.....	66
Tabla 19. Escala de valoración de cuadrantes	66
Tabla 20. Ejemplo de valoración del riesgo, para aplicar un control	67
Tabla 21. Matriz de riesgos, posteriormente de aplicar un control	68
Tabla 22. Nueva valoración de acuerdo a los controles identificados.....	68
Tabla 23. Proceso en el mapa de riesgos para la evaluación de un control.....	69
Tabla 24. Plantilla de controles genéricos	70
Tabla 25. Caso de uso Ingresar al sistema de gestión de riesgos de rol administrador	82
Tabla 26. Caso de uso creación de riesgos con rol administrador.....	83
Tabla 27. Caso de uso modificación de riesgos con rol administrador	85
Tabla 28. Caso de uso eliminación de riesgos con rol administrador	86
Tabla 29. Caso de uso evaluación de riesgos con rol administrador.....	87

Tabla 30. Caso de uso creación de controles con rol administrador	89
Tabla 31. Caso de uso selección de controles predefinidos con rol administrador	91
Tabla 32. Caso de uso creación de grupos de trabajo con rol administrador	92
Tabla 33. Caso de uso modificación de la matriz de riesgo con rol administrador.....	93
Tabla 34. Caso de uso reportación de incidentes con rol administrador	95
Tabla 35. Caso de uso creación del plan de acción con rol administrador.....	96
Tabla 36. Caso de uso observar reportes con rol administrador.....	97
Tabla 37. Caso de uso creación de activos con rol administrador.....	99
Tabla 38. Caso de uso creación de vulnerabilidades y amenazas con rol administrador ...	100
Tabla 39. Caso de uso creación de controles con rol operador	101
Tabla 40. Caso de uso evaluación de controles con rol operador.....	103
Tabla 41. Caso de uso reportación de incidentes con rol operador	106
Tabla 42. Caso de uso observar reportes con rol operador.....	107
Tabla 43. Caso de uso creación de planes de acción con rol operador.....	108
Tabla 44. Caso de uso consultar riesgos con rol viewer.....	109

Índice de ilustraciones

Ilustración 1. Encuesta referida a tipos de incidentes en el año 2021	26
Ilustración 2. Estadística sobre estándares y buenas prácticas de seguridad en el año 2021	27
Ilustración 3. Interfaz Pirani	31
Ilustración 4. Interfaz Asana.....	32
Ilustración 5. Interfaz Aptien.....	32
Ilustración 6. Interfaz Kawak	33
Ilustración 7. Proceso para la administración del riesgo en seguridad de la información....	42
Ilustración 8. Grafica de solidez de controles.....	60
Ilustración 9. Diagrama de casos de uso de las funcionalidades según el sistema de gestión de riesgos	82

Resumen

En el amplio análisis de los datos digitales de una organización, constantemente se ha mantenido la incógnita de ¿cómo identificar, monitorear y controlar riesgos informáticos?, por ello, se buscan tomar medidas que permitan el aseguramiento de la confidencialidad, disponibilidad e integridad de datos y eviten las amenazas como malware, denegación de servicios, entre otras intrusiones. Por tal razón, el tener el conocimiento del manejo de sistema de gestión de riesgos basado en apropiar los estándares ISO 27001, ISO 27002 y mejores prácticas, resulta beneficioso para la seguridad informática de las empresas.

El objetivo de esta propuesta es recolectar información de un sistema de gestión de riesgos en seguridad informática, ya que, al tener una adecuada inquisición de riesgos evitará los fallos de un sistema que puedan perjudicar o permitir la entrada a los intrusos, además servirá como guía para mitigar el impacto de distintos riesgos. Se pretende tener las bases para un futuro desarrollo de un software libre que permita el registro y monitoreo de los riesgos que se puedan presentar en pequeñas y medianas empresas.

Palabras clave: Gestión de riesgo, gestión de riesgo de TI, seguridad informática, estándares de seguridad informática.

Abstract

In the extensive analysis of an organization's digital data, the question of how to identify, monitor and control computer risks has constantly remained, for this reason, measures are sought to ensure the confidentiality, availability and integrity of data. and avoid threats such as malware, denial of service, and other intrusions. For this reason, having knowledge of the management of the risk management system based on appropriating the ISO 27001, ISO 27002 standards and best practices, is beneficial for the information security of companies.

The objective of this proposal is to collect information from a risk management system in computer security, since, by having an adequate investigation of risks, it will avoid failures of a system that can harm or allow intruders to enter, it will also serve as a guide. to mitigate the impact of different risks. It is intended to have the bases for a future development of free software that allows the registration and monitoring of risks that may arise in small and medium-sized companies.

Keywords: Risk management, IT risk management, computer security, computer security standards.

Capítulo 1. Planteamiento y formulación del problema

1.1 Planteamiento

Las empresas regularmente tienen que lidiar con pérdidas o daños de datos e información, debido a que constantemente aparecen nuevas vulnerabilidades y formas de intrusión a los sistemas, por lo tanto, obliga a buscar medidas que permitan el aseguramiento de la confidencialidad, disponibilidad e integridad de los datos. Lo anterior lleva a la necesidad de contar con un sistema de información como apoyo a la identificación, monitoreo y control de riesgos informáticos, y a la vez que sea asequible a pequeñas y medianas empresas que no cuentan con recursos para adquirir software costoso ni contratar personal experto en seguridad, pero deben demostrar que cumplen al menos con las condiciones mínimas de seguridad informática.

1.2 Justificación

Desarrollar un sistema de gestión de riesgos parte de tener un buen modelo y estudio, que consiga identificar los elementos a proteger, detectar y clasificar las vulnerabilidades, identificar amenazas, registrar las medidas de control, hacer monitoreo y seguimiento de los mismos; además el tema de gestión de riesgos se hace cada vez más complejo, puesto que la incorporación de nuevas tecnologías como la computación en la nube, internet de las cosas, entre otros, hace que aparezcan nuevas amenazas y se deban tomar nuevas medidas de seguridad. Este proyecto permitirá una guía para pequeñas y medianas empresas donde adquieran un conocimiento y cultura de seguridad informática donde permanentemente se debe advertir que los intrusos tengan acceso a los datos y sistemas de las empresas, y de esta manera disminuir las pérdidas por delitos informáticos.

1.3 Objetivos

1.3.1 General

Definir los requerimientos para un software de gestión de riesgos en seguridad informática para pequeña y mediana empresa.

1.3.2 Específicos

Indagar sobre los estándares y mejores prácticas de seguridad de la información para determinar los requerimientos para la elaboración de un sistema de gestión de riesgos.

Comparar herramientas y metodologías existentes de soporte para la gestión de riesgos en seguridad informática.

Establecer los requerimientos soporte para el desarrollo de un software de gestión de riesgos en seguridad informática.

1.4 Metodología

En esta monografía se basará en una investigación tipo descriptivo y cualitativo tomando como técnicas y herramientas la revisión de documentos y bibliografías acerca de las problemáticas que se puedan generar en las pymes, analizando y relatando las consecuencias que se produzcan por falta de la gestión de riesgos informáticos, en paralelo se realizará una comparación en las herramientas y metodologías existentes para la gestión de riesgos.

Se recogió información los cuales incluyen: artículos de tesis, metodologías, guías, encuestas, acerca de la seguridad de la información, los controles de entidades públicas, las gestiones de riesgos, la seguridad y privacidad de la información, comparación de modelos tradicionales de la información, donde las principales fuentes de recolección de información fueron guías realizadas por los gobiernos. Adicional a esto, fue necesario estudiar y analizar los requisitos de la norma 27001, para formar, realizar, mantener y poseer un excelente sistema de gestión de seguridad de la información que se desea plantear, es por ello que después de analizar todos los requerimientos de la norma, se procedió a acotarlos, para tener lo estrictamente necesario.

1.5 Antecedentes del problema (estado del arte)

Se relacionan proyectos de la gestión de riesgos para el mejoramiento de sus prácticas, adicionales guías y metodologías.

1.5.1 Trabajo 1:

Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá (Royer David Estrada-Esponda, José Luis Unás-Gómez, Oleskyenio Enrique Flórez-Rincón, 2021). Los autores identificaron las prácticas de seguridad de la información en una comunidad universitaria determinando el nivel de preparación de los miembros de una comunidad académica en relación con la seguridad de la información en

tiempos de pandemia. Los investigadores consideraron una muestra representativa donde los encuestados, fueron 335 estudiantes de pregrado, 37 docentes y 9 de estudios de posgrado, evidenciando que se aplicaron encuestas previstas según el diseño estadístico. Aplicando una encuesta hacia las prácticas de seguridad donde se logró evidenciar a profesores y estudiantes utilizando un alto porcentaje (76.6% en promedio) alguna herramienta de seguridad tipo antivirus. Adicionalmente se probó que, en cuanto al ámbito académico en la Universidad del Valle, los estudiantes y profesores estuvieron altamente afectados a nivel de seguridad de la información en cuanto al uso de las herramientas que solicitaban los profesores a los estudiantes, debido a que había más riesgo al utilizar plataformas como zoom, y en esta Universidad la videoconferencia para dar clases virtuales fue meet.

1.5.2 Trabajo 2:

Primeros pasos NIST Marco de ciberseguridad. (Amy Mahn, Jeffrey Marron, Stephen Quinn, Daniel Topper, 2021) Es una guía la cual consigue apoyar a una organización a iniciar o perfeccionar su plan de ciberseguridad.

Formado de prácticas que son efectivas. Promoviendo el contacto de las partes interesadas internas y externas, El marco está constituido en 5 funciones principales: identificar, proteger, detectar, responder, recuperar.

1.5.3 Trabajo 3:

Encuesta latinoamericana de seguridad de la información. (Jeimy J. Cano M, Gabriela María Saucedo Meza, 2021). Es una presentación detallada de los resultados de la Encuesta Latinoamericana de Seguridad de la Información 2021 realizada en el marco de las XXI Jornadas Internacionales de Seguridad de la Información realizadas por la Asociación Colombiana de Ingenieros de Sistemas ACIS donde presentaron las estadísticas acerca de los incidentes y mecanismos más presentes en las empresas.

1.5.4 Trabajo 4:

Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5. (Gobierno de Colombia-Dirección de Gestión y Desempeño Institucional, 2020). Los autores muestran elementos metodológicos renovados para un progreso al momento de identificar y valor del riesgo. Donde la implementación de la gestión del riesgo es indispensable que cada entidad realice un análisis de estrategias, la formulación de objetivos

y la consumación de estos en la toma de decisiones frecuentes, permitiendo una identificación del riesgo correcta a las obligaciones de cada planificación, dando un enfoque preventivo admitiendo la protección de los recursos, logrando las metas de alcanzar buenos resultados y perfeccionar la prestación de servicios a los consumidores. Entablando una distribución metodológica con los siguientes pasos, el primero, es la política de dirección del riesgo, donde se mantienen sus lineamientos, como segundo, la identificación del riesgo donde se propone una estructura para la redacción adecuada del riesgo, tercero, valoración del riesgo, se establecen los criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de severidad.

1.5.5 Trabajo 5:

Diseño de manual de diagnóstico y prevención de vulnerabilidades en redes de datos para PYMES. (Julian Hernan Barreto Cuitiva, 2018). Se presenta un manual básico de seguridad informática para pequeñas y medianas empresas, buscando el aseguramiento de los sistemas de información y poniendo en conocimiento los controles que se deben implementar sin necesidad de invertir altos costos de asesoramiento de un especialista en la materia, como primera medida tomaron documentos enmarcados en el tema de seguridad con el fin de recopilar información relevante que aporta en la creación de dicho manual, posteriormente se tomó la experiencia profesional, recurso importante para llevar cabo cada uno de las indicaciones y sugerencias que deben optar de acuerdo a las necesidades que tengan en el momento la pymes.

1.5.6 Trabajo 6:

Comparación de modelos tradicionales de seguridad de la información para centros de educación. (Lara, E., & Corella, F, 2018). El estudio desarrollado se basó en un análisis del estado del arte sobre esta temática y a partir de ello se determinaron las características principales de cuatro modelos de seguridad informática que dominan el mercado en la actualidad, como son: OSSTMM3, ISO 27001, NIST y COBIT 5, para luego hacer un cuadro comparativo de dichas características, con la finalidad de encontrar la mejor opción que pueda ser utilizada en los centros de educación. El estudio demostró que un modelo de seguridad es la presentación formal de una estrategia de seguridad y que debe identificar el conjunto de reglas y prácticas que regulan como un sistema maneja, protege y distribuye la información delicada.

1.5.7 Trabajo 7:

Seguridad y privacidad de la información. (MINTIC, 2016). Este documento tiene la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL. El modelo pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

1.5.8 Trabajo 8:

Gestión de seguridad de información: Revisión bibliográfica (Cárdenas Solano Leidy Johanna, Ardila Hugo Martínez y Becerra Ardila Luis-Eduardo, 2016). El objetivo de este trabajo fue consolidar el estado del arte sobre el tema seguridad de la información para la ventana de tiempo 2001-2015. La revisión bibliográfica que se realizaron fue en tres etapas: a) Revisión de información no estructurada, b) Análisis bibliométrico y c) Análisis, organización y síntesis del contenido. Como resultado se extrajeron un amplio marco de trabajo multidimensional en el que se relaciona gestión del conocimiento, gestión de riesgos, incidentes de seguridad, sistemas de información y redes, recursos humanos, aspectos económicos, gobernanza, políticas, y buenas prácticas.

1.5.9 Trabajo 9:

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (Gobierno de España, 2012). Es la metodología de análisis y gestión de riesgos elaborada en su día por el antiguo Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) con la colaboración del Centro. También es una metodología de carácter público que puede ser utilizada libremente y no requiere autorización previa. Interesa principalmente a las entidades en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) para satisfacer el principio de la gestión de la seguridad basada en riesgos, así como el requisito de análisis y gestión de riesgos,

considerando la dependencia de las tecnologías de la información para cumplir misiones, prestar servicios y alcanzar los objetivos de la organización.

1.5.10 Trabajo 10:

Metodología de Análisis de Riesgos OCTAVE. (Universidad Carnegie Mellon). La metodología OCTAVE significa Evolución de la vulnerabilidad ante amenazas desde el punto de vista operativo crítico, activo. Es un método de análisis de riesgos orientado a activos y a la gestión de los riesgos para garantizar la seguridad de sistemas informativos desarrollado por el CERT. Realiza una evaluación de riesgos en la seguridad de información considerando los temas organizacionales y técnicos, examina cómo la gente emplea la infraestructura en forma diaria. Su objetivo principal es desarrollar una perspectiva de seguridad dentro de una organización, teniendo en cuenta perspectiva de todos los niveles para asegurarse que las soluciones puedan implementarse con facilidad

1.6. Formulación

¿Cómo nivelar, monitorear e intervenir riesgos informáticos llevando a cabo las normas 27001 y 27002 para evitar fallos en un sistema obteniendo como ente de beneficio a PYMES?

1.7. Resultados o alcances esperados

Al finalizar este proyecto como principal producto se espera aportar los requerimientos para un software de gestión de riesgos informáticos base para futuros proyectos. El impacto que se busca con este proyecto a partir del diseño, es proporcionar un modelo inicial de gestión de riesgos que apoyará a futuros a pequeña y mediana empresa, puesto que, no cuentan con un fondo elevado. En el sector académico se beneficiarán estudiantes de cursos de seguridad informática, en el sector productivo pequeñas y medianas empresas que no tienen los recursos para adquirir softwares costosos de gestión de riesgos informáticos.

Capítulo 2. Marco referencial

Primeramente, se tomarán aportes de las siguientes investigaciones: proyecto de grado (DISEÑO DE MANUAL DE DIAGNÓSTICO Y PREVENCIÓN DE VULNERABILIDADES EN REDES DE DATOS PARA PYMES) de Julian Hernan Barreto

Cuitiva, artículo (XXI Encuesta Nacional de Seguridad Informática. Resiliencia un aspecto clave en la ciberseguridad) de Andres Almanza, para tomar contribuciones y así construir un entregable concretando como manual básico acorde con los objetivos planteados.

2.1 Marco Contextual

Según el gobierno de España define a la familia de Normas ISO 2700 como:

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

En concreto la familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporciona un marco para la gestión de la seguridad.

Dentro de este conjunto están:

Las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La seguridad de la información, según la ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento.

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

Dentro de este conjunto están:

Tabla 1 Normas ISO gestión de seguridad de la información

NORMA	DESCRIPCIÓN
ISO/IEC 27000	Vocabulario estándar para el SGSI y para todas las normas de la familia. Se encuentra en desarrollo actualmente.
ISO/IEC 27001	Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
ISO/IEC 27002	Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
ISO/IEC 27003	Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.
ISO/IEC 27004	Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.

ISO/IEC 27005	Normativa dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standar BS 7799 parte 3. Publicada en junio de 2008.
ISO/IEC 27006	Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
ISO/IEC 27007	Guía para auditar al SGSI. Se encuentra en preparación.
ISO/IEC 27799:2008	Guía para implementar ISO/IEC 27002 en la industria de la salud.

Nota. Tomado de “Normas ISO sobre gestión de seguridad de la información”. Gobierno de España. CC BY-SA 3.0 ES

Una vez ya mencionada la normas ISO, se aclara que solo se enfatizan las normas 27001 y 27002 para la realización de este trabajo.

De acuerdo a la ley 590 del 10 de julio del 2000 artículo 2 se define como pyme:

Artículo 2°. Modificado por el art. 2, Ley 905 de 2004, Modificado por el art. 75, Ley 1151 de 2007, Modificado por el art. 43, Ley 1450 de 2011. Definiciones. Para todos los efectos, se entiende por micro, pequeña y mediana empresa, toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuarias, industriales, comerciales o de servicios, rural o urbana, que responda a los siguientes parámetros:

1. Mediana Empresa:

a) Planta de personal entre cincuenta y uno (51) y doscientos (200) trabajadores;

b) Activos totales por valor entre cinco mil unos (5.001) y quince mil (15.000) salarios mínimos mensuales legales vigentes.

2. Pequeña Empresa:

a) Planta de personal entre once (11) y cincuenta (50) trabajadores;

b) Activos totales por valor entre quinientos uno (501) y menos de cinco mil (5.001) salarios mínimos mensuales legales vigentes.

3. Microempresa:

a) Planta de personal no superior a los diez (10) trabajadores;

b) Activos totales por valor inferior a quinientos uno (501) salarios mínimos mensuales legales vigentes.

Según las definiciones previas se puede apreciar que las normas 27001 y 27002 al ser aplicadas a las pymes ayudan a que éstas no sufran grandes pérdidas para sus empresas independientemente si un área es atacada o no. Según el artículo de Julian Barreto el tipo de incidentes más constante en una empresa es por errores humanos, por otro lado, los estándares más utilizados *en las empresas es ISO 27001*.

2.2 Marco Normativo

2.2.1 Ley 1273 del 2009

De acuerdo a la ley 1273 de 2009 en la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

EL CONGRESO DE COLOMBIA

DECRETA:

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPÍTULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A: Acceso abusivo a un sistema informático.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

Artículo 269E: Uso de software malicioso.

Artículo 269F: Violación de datos personales.

Artículo 269G: Suplantación de sitios web para capturar datos personales.

Artículo 269H: Circunstancias de agravación punitiva

CAPÍTULO. II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión correspondiente.

2.2.2 Ley 87 de 1993

"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"

ARTÍCULO 2. Objetivos del sistema de Control Interno.

a. Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que lo afecten;

f. Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.

2.3 Marco teórico

2.3.1 Gestión de los riesgos de TI

Según (RED HAT uno de los proveedores a nivel mundial de soluciones empresariales) los riesgos provienen de la posibilidad de pérdidas o daños si una amenaza aprovecha un punto vulnerable de seguridad en sus sistemas de hardware o software. Los puntos vulnerables y las exposiciones comunes (CVE), una lista de fallas de seguridad que se encuentra disponible para todo el público, permite que los especialistas en TI coordinen sus iniciativas para priorizar y solucionar estos inconvenientes, con el fin de mejorar la seguridad de los sistemas informáticos. Es por esto, que la seguridad de la TI debe formar parte de la infraestructura y del ciclo de vida del producto desde el comienzo, y debe incorporarse a la estrategia de gestión de riesgos para que su empresa pueda adelantarse a los sucesos y responder a ellos. Adicional a esto, una forma para mitigar los riesgos es utilizando herramientas, como el análisis predictivo y la automatización, para supervisar su infraestructura.

Se resalta la importancia de empezar con la seguridad TI en una empresa, puesto que está constantemente en peligro a ser vulnerable por medio de todos los riesgos existentes en una empresa, ya que no se puede afirmar que una empresa pueda estar cien por ciento libre de toda amenaza existente.

A continuación, se mostrarán los pasos que son esenciales para aplicar una correcta gestión de riesgos. Según Julia Martins muestra una guía de buenas prácticas con seis pasos la cual se enfoca hacia la gestión de proyecto, pero independientemente hacia donde se enfatice los pasos seguirán siendo los mismos.

1. Identificación

El primer paso para crear el proceso de gestión de riesgos es reunir una lista de todos los casos en los que se podrían presentar, potencialmente, los riesgos que afectan. Un caso de riesgo es cualquier causa que pudiese afectar negativamente al presupuesto o, en definitiva, al éxito en sí.

Para el registro de riesgos se debe responder a varias preguntas acerca de los riesgos que se han identificado para una mejor selección, los interrogantes son:

¿Qué probabilidad hay de que se produzca este caso de riesgo?

¿Cuál sería el impacto y la gravedad que tendría si se produjese?

¿Cuál es nuestro plan de respuesta a este riesgo?

Dados la probabilidad de ocurrencia y el impacto que podría tener, ¿qué nivel de prioridad le asignarías?

¿Quién es el responsable en caso de que este riesgo se haga realidad?

Se puede incluir que la autora quiere dar a conocer en este primer paso es que se tenga en cuenta el escenario en el que se encuentran los riesgos de mayor amenaza realizando una lista de estos, resaltando las formas fundamentales para la identificación de riesgos, adicional a esto, evidenciar y reafirmar cada una de las hipótesis que se generen de un riesgo independientemente si este no tiene la certeza de que es concreto y por último rectificar que el equipo de trabajo ha logrado tener el registro de riesgos frecuentes de lo contrario realizar un informe de estos.

2. Análisis de riesgos

Por cada riesgo identificado, se analiza la probabilidad de que se produzca, la gravedad y el plan de respuesta. Dependiendo de la complejidad de los riesgos, considerando llevar a cabo un análisis del riesgo con el equipo o con algunos participantes clave. Para decidir acerca de la gravedad, es vital pensar el impacto que tendría el caso en los objetivos. ¿Retrasa lo programado con el cronograma, afectará al presupuesto o reducirá el impacto que tendrán los entregables del proyecto?

Después, por cada riesgo, elaborar un plan de respuesta. El plan de respuesta no debe ser necesariamente una acción pendiente a realizar ahora mismo; más bien, es lo que realizará el equipo para revertir rápidamente el riesgo y abordarlo en caso de que surja.

En otras palabras, este paso hace énfasis al proceso de controlar un riesgo, puesto que, para dominarlo, se necesita identificar qué tan grave puede ser el impacto que alcanza a generar y estimar si trae consecuencias para lo que se esté realizando, a causa de esto es necesario gestar un plan de respuesta.

3. Priorización

Para establecer las prioridades de los riesgos, es necesario cuestionar lo siguiente: basado en el registro y análisis de los riesgos, ¿cuáles tienen mayor probabilidad de producirse que sean, potencialmente, los que afectan con mayor intensidad al éxito?

Lo más importante es detectar los riesgos que tengan mayor probabilidad de ocurrencia y cuya gravedad tenga un mayor impacto. Probablemente es lo que se quiere controlar y responder a todos los riesgos potenciales, pero son estos a los que se deben prestar más atención y controlar con mayor frecuencia.

Resulta lógico que después de realizar los controles se organicen los riesgos en orden de procedencia logrando así detectar a tiempo los riesgos que tienen mayor porcentaje de peligro y en efecto disminuir la probabilidad de ocurrencia.

4. Asignación

Este paso es opcional, pero recomendado. A pesar de que todavía no se hayan producido los casos de riesgo, es muy útil asignar un responsable lo antes posible, para que los miembros del equipo estén preparados. La persona asignada no solo debe controlar si se produce o no el caso, sino que además será el contacto para la toma de decisiones y desarrollar el plan de mitigación de ese riesgo; independientemente de que el riesgo, valga la redundancia, corra el riesgo de producirse o no.

Suena coherente decir que cada miembro del equipo de trabajo tenga uno o más peligros a cargo dependiendo de la dificultad a resolver, debido a que, una vez asignado los riesgos, el personal encargado se dedicará al riesgo asignado y así poder tener un excelente control para mitigar la producción o reproducción de cada uno de los conflictos presentes.

5. Supervisión

A estas alturas, se daría inicio. Si todo sale según lo esperado, orientado para cumplir con los objetivos fundamentales. Pero se debe seguir controlando activamente los riesgos para evitar impresiones desafortunadas. Enviando actualizaciones de estado con regularidad para que el equipo y los demás participantes estén alineados permitiendo al sistema de gestión de riesgos ser proactivo.

Consultando con frecuencia a los gerentes responsables de cada riesgo. Cada “encargado” de un riesgo deberá supervisar y estar atento a la probabilidad de que se produzca el caso de riesgo, como gerente o líder del equipo, dialogar con ellos constantemente para asegurarse de que todo esté funcionando correctamente.

Si se llega a cambiar la probabilidad de que un riesgo se produzca o si se actualiza un plan de mitigación de riesgos, ese cambio debería reflejarse en el registro de riesgos.

Al igual que con el resto de los elementos de la gestión, el plan para gestión del riesgo debe ser un documento activo que el equipo use para mantenerse bien orientado. La colaboración es muy importante en esta etapa.

En caso de que el proyecto ya se esté ejecutando, es necesario estar actualizando constantemente al equipo para el desarrollo de estrategias y mantener la comunicación con los gerentes responsables de cada riesgo para verificar que todo esté funcionando correctamente y que este cambio se vea reflejado en el registro de riesgos.

6. Respuesta

Si en algún momento un riesgo se convierte en realidad, será hora de responder. Si todo resulta como es de esperar, como se cuenta con un registro de riesgos y un plan para gestionar los riesgos, ya se tendrá un excelente plan de contingencia para afrontarlo.

Es necesario tener en cuenta que: la gestión de riesgos no consiste en evitarlos, aunque sí puede colaborar con la prevención. Más bien, la gestión de riesgos es la práctica de prepararse para los casos de riesgo y contar con un excelente plan listo de antemano para que nunca estemos desprevenidos.

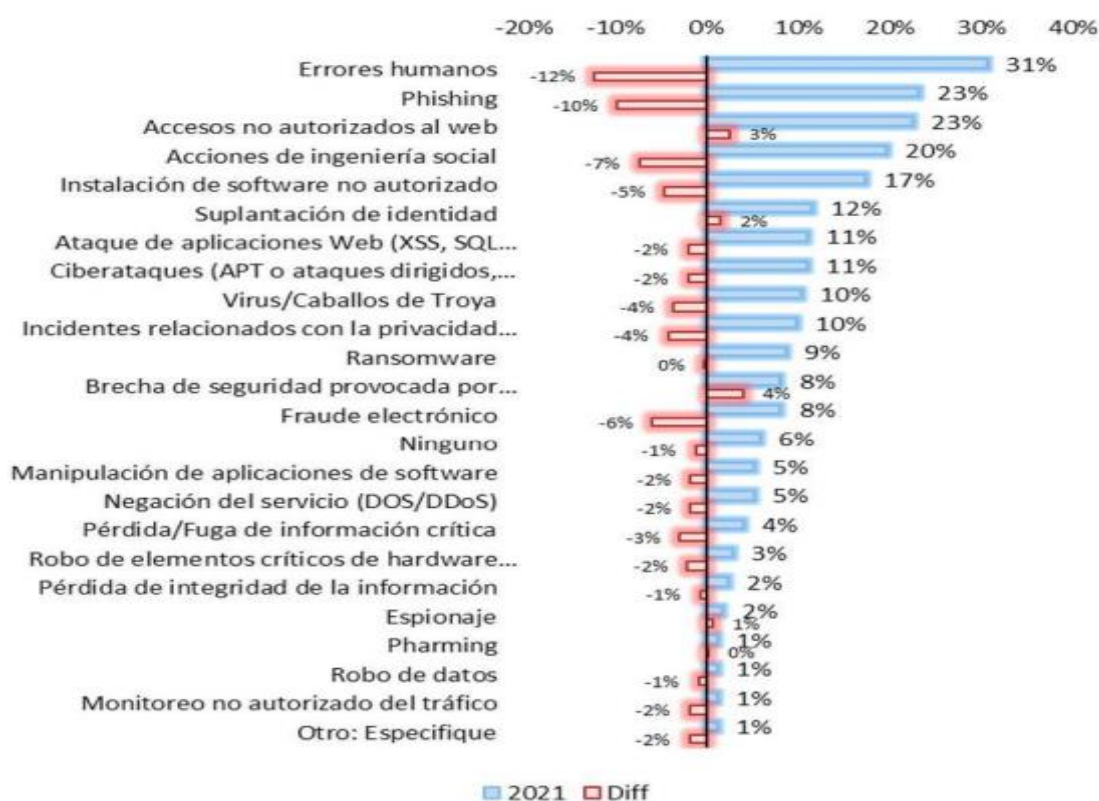
Como su nombre lo indica es necesario que siempre se tenga la forma en cómo se va a actuar frente a diferentes riesgos que se pueda evitar reproducirse y así afectar grandemente etapas e información importante del proyecto que se esté efectuando.

2.3.2 Seguridad informática

De acuerdo con (Julián Pérez Porto y María Merino) la seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático pero como hay un inconveniente que no existe ninguna técnica que permita el total aseguramiento de un sistema, este puede ser predilecto a nivel lógico o físico, por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas). Hay tres tipos principales de seguridad, el primero es la seguridad de hardware que es la encargada de escudar a los dispositivos que se usan para acoger sistemas, redes, apps y programas exteriores frente a diversos riesgos, el segundo es la seguridad de software utilizado para salvaguardar los sistemas cuando se presenten

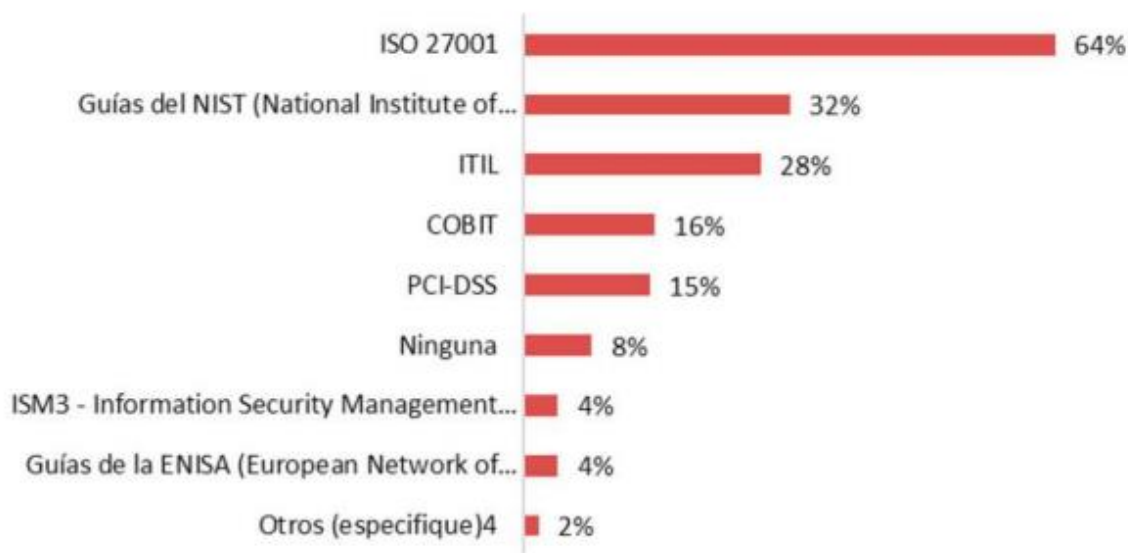
ataques por hackers, por ultimo esta la seguridad de red que está relacionada con el diseño de actividades para proteger los datos que sean accesibles por medio de la red y que existe la posibilidad de que sean modificados, robados o mal usados. Las principales amenazas en esta área son: virus, troyanos, phishing, programas espía, robo de datos y suplantación de identidad. A continuación, en la ilustración 1, se observa como estas amenazas están presentes en las empresas, siendo de las más comunes los errores humanos, y phishing, que se presentan cuando el personal no está suficientemente capacitado para evitar errores sencillos, y acerca de que el cliente cuide más sus acciones al momento de entregar datos personales.

Ilustración 1. Encuesta referida a tipos de incidentes en el año 2021



Nota. Tomado de “XXI Encuesta Nacional de Seguridad Informática. Resiliencia un aspecto clave en la ciberseguridad” por Andres Almanza, 2021, p. 15. © 2020 ACIS.

Ilustración 2. Estadística sobre estándares y buenas prácticas de seguridad en el año 2021



Nota. Tomado de “XXI Encuesta Nacional de seguridad Informática. Resiliencia un aspecto clave en la ciberseguridad” por Andres Almanza, 2021, p. 29. © 2020 ACIS

De acuerdo con la ilustración 2, lo que se quiere resaltar, es que en gran medida en las pymes y grandes empresas aplican las prácticas de la norma ISO 27001, que en este trabajo es esencial, donde se puede afirmar que está es de vital importancia a la hora de evaluar la seguridad de cualquier empresa.

En síntesis, la seguridad informática es aquella que permite tener la completa certeza de que los datos que una persona almacene ya sean en la nube o en una empresa, van a quedar protegidos puesto que se busca que la integridad y privacidad de los clientes sea una de las principales en ser protegida.

2.3.3 Estándares de seguridad

En este caso, solo se centrará en los estándares ISO 27001 y ISO 27002. Conforme a (nqa organismo de certificación global) ISO 27001 es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal. La implantación de la ISO 27001 es la respuesta

ideal a los requisitos legislativos y de los clientes, incluyendo el RGPD y otras amenazas potenciales, incluyendo: crimen cibernético, violación de los datos personales, vandalismo, terrorismo, daños, uso malintencionado, robo y ataque de virus.

Con arreglo a (ISOTools Excellence) ISO 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

Según (OSTEC) Algunas de las ventajas proporcionadas por la certificación ISO 27002 son representativas para las empresas, sobre todo porque son reconocidas mundialmente.

- Mejor concienciación sobre la seguridad de la información.
- Mayor control de activos e información sensible.
- Ofrece un enfoque para la implementación de políticas de control.
- Oportunidad de identificar y corregir puntos débiles.
- Reducción del riesgo de responsabilidad por la no implementación de un SGSI o determinación de políticas y procedimientos.
- Promueve reducción de costos con la prevención de incidentes de seguridad de la información.
- Conformidad con la legislación y otras reglamentaciones.

Capítulo 3. Comparación de herramientas y metodologías existentes de soporte para la gestión de riesgos en seguridad informática.

3.1 Comparación de herramientas para la gestión de riesgos

En la búsqueda de herramientas, son muy pocas las que permiten probar un mes de prueba gratis, los precios son compensados a lo que brinda cada herramienta, en este estudio se comprobó que hay muy pocas herramientas que son netamente encaminadas hacia la gestión de riesgos en el área de seguridad informática, puesto que en la mayoría de herramientas dan solución a gestionar riesgos a nivel general más no en un área específica

Tabla 2. Comparativa de herramientas para la gestión de riesgos

Herramientas	Pirani	Asana	Aptien	Kawak
Características	- Identifica, mide, controla y monitorea fácilmente los riesgos operativos de tu organización. - Ayudar a las empresas a controlar y optimizar los procesos de riesgo relacionados con la gobernanza corporativa.	- Es una plataforma web y móvil de gestión del trabajo. - Crea procesos automatizados para coordinar los equipos - Ayudar a los equipos a organizar, realizar un seguimiento y gestionar su trabajo. - Es una herramienta que permite gestionar el flujo de trabajo (tareas y proyectos) ofreciendo el detalle de inicio y culminación de cada una de estas. - Conecta a todo el equipo de trabajo permitiendo la comunicación,	- Organizar el trabajo, las tareas y otros recursos de la empresa. - Software de colaboración y gestión de equipos que es sencillo y agradable. - Permite gestionar tareas, administrar proyectos, usar contraseñas, activos y equipos. - Permite a las empresas mantener la mayor parte de su información en una sola plataforma.	- Permite a toda tu empresa vivir su sistema de gestión de forma digital, cuidando el medio ambiente. - Tiene varios módulos que permiten simplificar en una empresa la gestión y a digitalizar sus procesos - Permite dar un seguimiento de las tareas

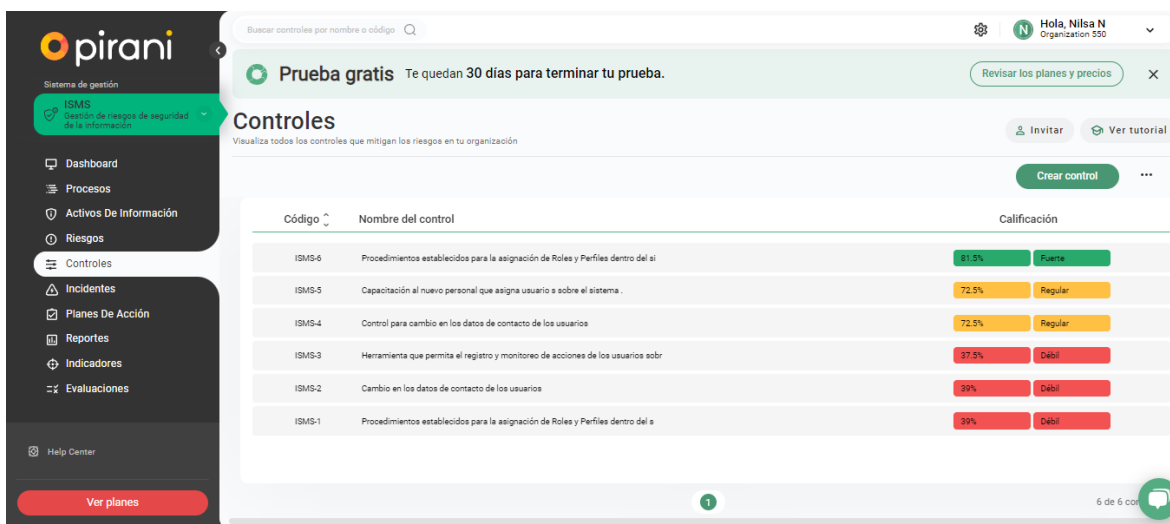
		organización y planificación para llevar a feliz término los proyectos en cuestión.		
Ventajas	● Brinda un mes de prueba gratis ● Cumple con estándares internacionales como ISO 31000, ISO 27000, COSO ERM, AS / NZS 4360, Basilea. ● Respalda el cumplimiento de regulaciones locales. ● Interfaz interactiva y fácil de comprender ● Ofrece varios módulos como Pirani Risk ORM, Pirani Event View, Pirani Reporting, Pirani Planning, Pirani Metrics y más. ● Implementación es basada en la nube ● Permite editar la matriz de riesgo. ● Cada semana muestran mejoras en el software y cada mes, nuevas funcionalidades. ● Tiene 3 sistemas de gestión de riesgos normativos (seguridad de la información, operacionales, lavado de activos)	● Brinda un mes de prueba gratis ● Implementación es basada en la nube y entorno local	● Brinda un mes de prueba gratis ● Implementación es basada en la nube y entorno local ● Las empresas pueden organizar clientes, relaciones, personas, activos, riesgos, descripciones de trabajos, proyectos y más. ● Es altamente configurable y de fácil manejo. ● Implementación es basada en la nube ● Implementación es basada en entorno local ● Se integra con las siguientes aplicaciones: Dropbox Business, Google Drive, Mailchimp, Microsoft 365, Microsoft Azure, Microsoft Outlook, Microsoft Power BI, Microsoft SharePoint, OneDrive, SAP Business One, Slack	● Implementación es basada en la nube. ● Soporta sistemas de gestión de Calidad – ISO 9001, NTC 6001, Ambiental – ISO 14001, de Responsabilidad Social – ISO 26000, de Seguridad de la Información – ISO 27001, de Gestión de Riesgos – ISO 31000, de Seguridad y Salud en el Trabajo – ISO 45001. ● Interfaz interactiva y fácil de comprender ● Ofrecen subsidios para micros, pequeñas y medianas empresas, siempre y cuando cumplan con los requisitos acordados. ● Se puede adquirir un módulo según lo necesite la empresa (289.000 para empresas medianas y pequeñas).

Desventajas		- No tiene sistemas de gestión de riesgos conforme a la norma 27001 - Se centraliza en el manejo de la gestión de proyecto, más no en la gestión de riesgos	- El idioma es admitido en inglés. - No está disponible para Colombia	No brinda mes de prueba gratis
Precio (COP)	\$ 199,553	\$ 54,827	\$ 164,631	\$768,279,82 (289,000 solo un módulo) (Puede variar según el módulo que requiera la empresa)

Nota. Tomada de: getApp.

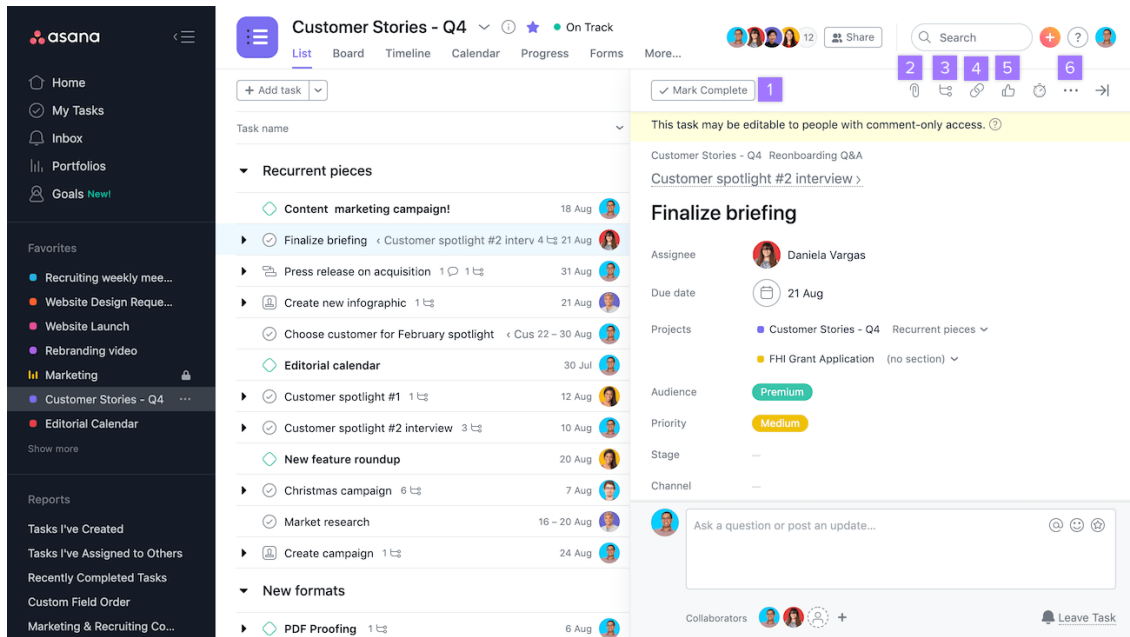
4.1.1 Comparación de interfaces de las herramientas

Ilustración 3. Interfaz Pirani



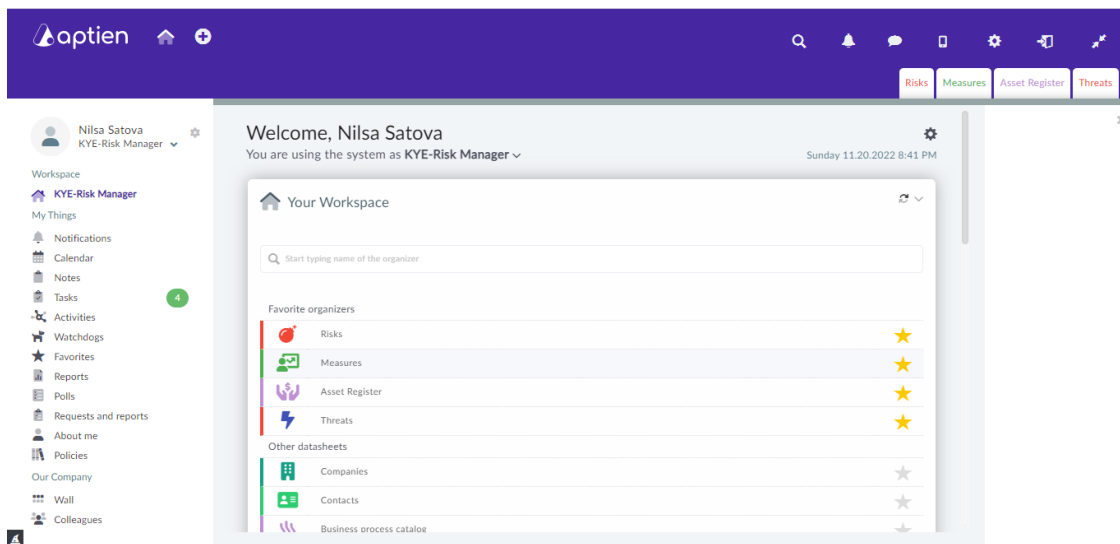
Nota: Tomado de Pirani.

Ilustración 4. Interfaz Asana



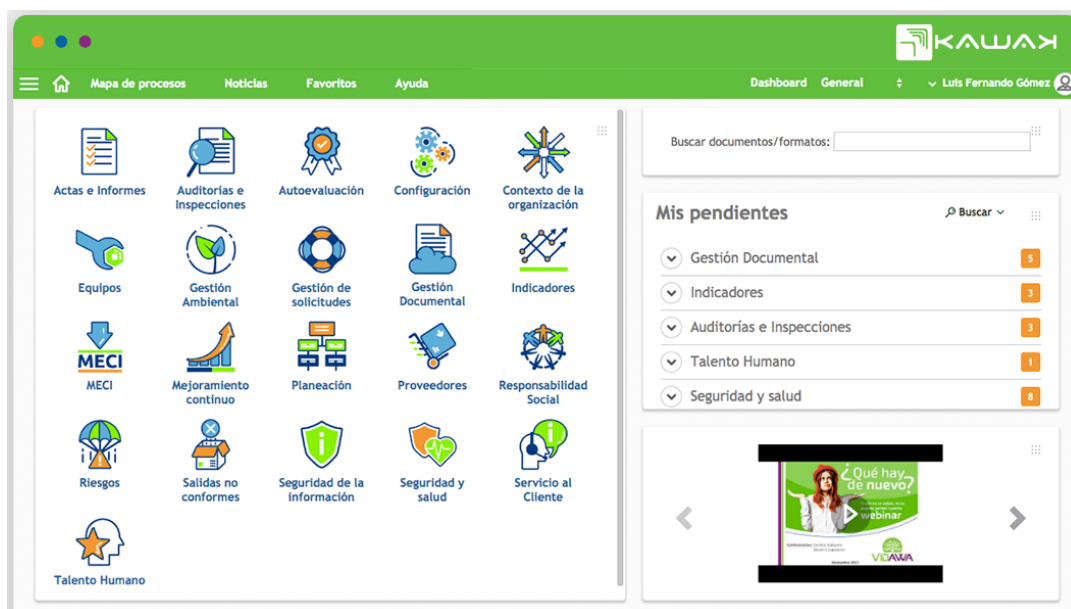
Nota: Tomado de asana.

Ilustración 5. Interfaz Aptien



Nota: Tomado de aptien.

Ilustración 6. Interfaz Kawak



Nota: Tomado de Kawak

3.2 Comparación entre la metodología Margerit y Octave

Tabla 3. Comparativa de metodologías del análisis del riesgo

Metodologías	Magerit	Octave
Características	● Creado por el Consejo Superior de la Administración Electrónica. ● Promueve la sensibilización a los responsables de la existencia de riesgos en los sistemas de información y asimismo en la necesidad de identificarlos a tiempo.	● Creado por un centro de investigación en EE. UU ● Está dirigido a diferentes grupos de trabajo desde los más pequeños hasta los más grandes. ● Plantea una gestión de riesgo basada en la operatividad de la organización, y considera la seguridad

	● Considera que los riesgos están inmersos dentro de los sistemas de seguridad de la información. ● Focaliza su objetivo en el análisis de los riesgos en los sistemas de Seguridad Informática para descubrirlos de manera oportuna ● Está relacionado con el uso de medios electrónicos, informativos y tecnológicos con el objetivo de reducir la desconfianza por parte de los usuarios al uso de estos medios.	informática no un tema únicamente técnico ● Metodología autodirigida, donde permite que las personas de una organización puedan ser parte del establecimiento y de las estrategias para la protección de la seguridad, esto con el uso de métodos y herramientas ● Metodología flexible que puede ser personalizada a cada una de las organizaciones. ● Maneja talleres, hojas de trabajo y procedimientos para el análisis de los riesgos y la priorización de los mismos en pro del planteamiento de estrategias.
Fases	● El análisis de riesgo. ● La gestión del riesgo	● La creación de amenazas. ● La identificación de vulnerabilidades.

		● El planteamiento de estrategias pro a la mitigación de los riesgos.
Implementación	● Inicia su método con el análisis de riesgos a los activos de la organización, su incidencia en ellos y las amenazas a los que están expuestos.	● Establece 4 procesos que sugieren puntos de vista a los activos críticos, las áreas de operatividad importantes, requerimientos de seguridad, las vulnerabilidades y la estrategia a implementar.
Enfoque	● Dividir los activos de la organización en diversos grupos para determinar una gran cantidad de riesgos	● Trabaja en la planificación con antelación de los sistemas de información basados en los riesgos.
Métodos	● Basada en un lineamiento sistemático ● Trabaja en pro de las tecnologías de la información y en brindar confianza en el uso de las mismas	● Plantea la auto dirección y flexibilidad ● Enfoca todo en el riesgo interno u organizacional de la empresa. ● Establece los riesgos en cuanto al tipo de activo

	● Lleva a cabo un proceso de concientización al personal de la organización, con la idea de enseñarles que existen diferentes tipos de riesgos en los sistemas de información y en la importancia de ubicarlos a tiempo ● Se enfoca en atender las solicitudes del Gobierno, Organismos, Pymes y compañías comerciales	software, hardware, usuario y red. ● Se enfoca para trabajar con empresas pequeñas y medianas
--	---	--

Nota. Tomada de “Gestión de riesgo metodologías octave y magerit”, por Martha, Hurtado, Universidad Piloto de Colombia, p. 10. © 2014 // SMPC®.

De acuerdo a la tabla 23, la metodología a trabajar será MARGERIT, puesto que tiene guías que permiten una mejor calificación de riesgos y controles, tanto como en activos, lo cual permite a las pymes tener una excelente gestión de riesgos, generando una confianza, adicional a esto resalta su importancia en tener sistemas que estén manejando correctamente para evitar la mayor parte de amenazas posibles.

Capítulo 4. Requerimientos para la elaboración y soporte para el desarrollo de software

4.1 Especificación de requerimientos

Para la especificación de requerimientos primero se realizó un análisis de todos los requisitos contemplados en la norma ISO (27001), luego se contemplaron cuáles de ellos son estrictamente necesarios para las pymes, de acuerdo a estos parámetros se realizó una acotación obteniendo como resultado una lista de 30 ítems que se deben implementar para una correcta gestión de riesgos en la seguridad informática.

A continuación, se muestra el inventario de requerimientos que se implementará en la futura herramienta. Según la norma anteriormente mencionada, especifica los siguientes requisitos para establecer, implementar y mejorar continuamente un sistema de gestión de la seguridad de la información:

4.1.1 Lista de requerimientos

En el ámbito estructura se debe:

1. Determinar las partes interesadas que son pertinentes al SGSI, y los requisitos de estas partes pertinentes a seguridad de la información, como requisitos legales, reglamentarios y obligaciones contractuales.
2. Determinar los límites y la aplicabilidad del SGSI para establecer su alcance.

Para una correcta planificación es indispensable

3. Planificar las acciones para tratar estos riesgos y oportunidades.
4. Planificar la manera de integrar e implementar estas acciones en sus procesos del sistema de gestión de la seguridad de la información, y evaluar la eficacia de estas acciones.

Valoración de riesgos de la seguridad de la información

5. Definir y aplicar un proceso de valoración de riesgos de la seguridad de la información que establezcan y mantengan criterios de aceptación de riesgos y para realizar valoraciones de riesgos de la seguridad de la información.
6. Asegurar que las valoraciones repetidas produzcan resultados consistentes válidos y comparables.
7. **Identificar los riesgos de la seguridad de la información:** Aplicando el proceso de valoración de riesgos para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de información dentro del alcance del SGSI e identificar a los dueños de los riesgos.
8. **Analizar los riesgos de la seguridad de la información:** Valorando las consecuencias potenciales que resultaran si se materializaran los riesgos identificados en el numeral anterior, junto con la probabilidad que ocurran estos riesgos, determinando el nivel de cada uno de los riesgos.
9. **Evaluar los riesgos de seguridad de la información:** Comparando los resultados del análisis de riesgos con los criterios de riesgo y priorizar los riesgos analizados para el tratamiento de riesgos.
10. Conservar información documentada acerca del proceso de valoración de riesgos de la seguridad de la información.

Tratamiento de riesgos de la seguridad de la información

11. Definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información.
12. Seleccionar las opciones apropiadas de tratamiento de riesgos de la seguridad de la información, teniendo en cuenta los resultados de la valoración de riesgos
13. Determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la seguridad de la información.
14. Comparar los controles determinados en el número 16 con los del Anexo A, y verificar que no se han omitido controles necesarios.
15. Producir una declaración de aplicabilidad que contenga los controles necesarios y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A.

- 16.** Formular un plan de tratamiento de riesgos de la seguridad de la información
- 17.** Obtener de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información.
- 18.** Conservar información documentada acerca del proceso de tratamiento de riesgos de la seguridad de la información.

Objetivos de seguridad de la información y planes para lograrlos.

- 19.** Establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Valoración de riesgos de la seguridad de la información

- 20.** Llevar a cabo valoraciones de riesgos de la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos.
- 21.** Conservar información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información.

Tratamiento de riesgos de la seguridad de la información

- 22.** Implementar el plan de tratamiento de riesgos de la seguridad de la información.
- 23.** Conservar información documentada de los resultados del tratamiento de riesgos de la seguridad de la información.

Seguimiento, medición, análisis y evaluación

- 24.** Determinar a qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información.
- 25.** Determinar los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos.
- 26.** Determinar cuándo se deben llevar a cabo el seguimiento y la medición.
- 27.** Determinar quién debe llevar a cabo el seguimiento y la medición.

28. Determinar cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición y quién debe analizar y evaluar estos resultados.
29. Conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.

Se debe considerar que la alta dirección debe:

30. Incluir consideraciones sobre resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y las oportunidades de mejora continua.

4.2 Clasificaciones a tener en cuenta

Se tendrá en cuenta la siguiente tabla para la calificación de criterio de confidencialidad, integridad y disponibilidad.

Tabla 4. Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 7.

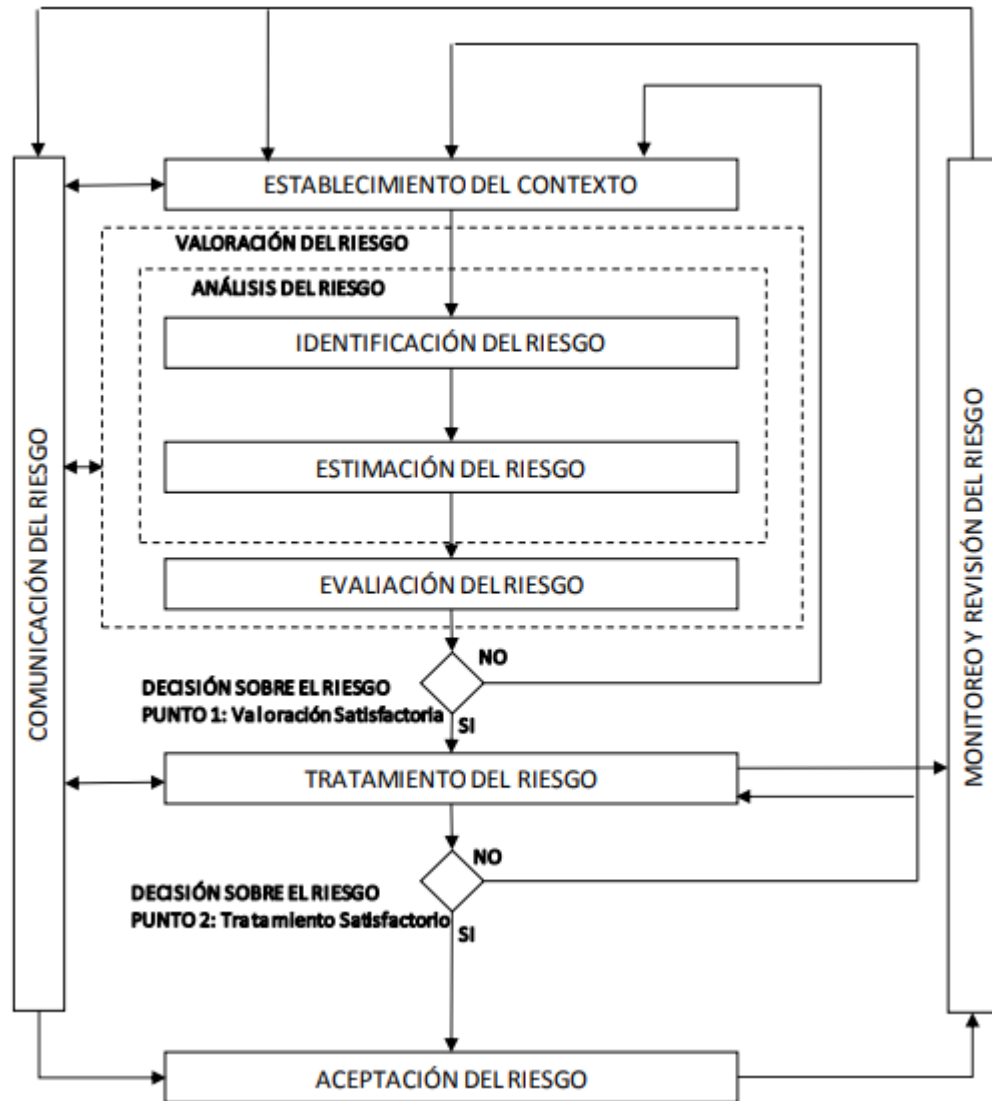
Se consideran los siguientes niveles de clasificación en la siguiente tabla:

Tabla 5. Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 7.

Ilustración 7. Proceso para la administración del riesgo en seguridad de la información



Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 11.

Se puede observar en la Ilustración 3, el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o de tratamiento del riesgo.

Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo suministra un buen

equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos altos se valoren de manera correcta.

Seguidamente se muestran las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI en la siguiente tabla:

4.3 Criterios Básicos

Dependiendo del alcance y los objetivos de la gestión del riesgo se pueden aplicar diferentes enfoques, que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo.

4.3.1 Criterios de evaluación del riesgo

Desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización teniendo en cuenta:

- El valor estratégico del proceso de información para la entidad.
- La criticidad de los activos de información involucrados en el proceso.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

4.3.2 Criterios de impacto

Desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información de procesos
- Brechas en la seguridad de la información (ejemplo: pérdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas.
- Pérdida del negocio y del valor financiero.
- Alteración de planes y fechas límites.
- Daños para la reputación.
- Incumplimiento de los requisitos legales.

4.3.3 Criterios de aceptación del riesgo

Desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas.

La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo, se deberían considerar los siguientes aspectos:

- Incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas.
- Se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado.
- Pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual.
- Pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

4.4 Alcance y límites para la gestión de riesgos en seguridad de la información.

La entidad debe definir el alcance y los límites y el alcance para de esta manera garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo.

4.4.1 Identificación de riesgos.

Establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos.

Se listan los términos que son necesarios dentro del empleo de esta metodología:

- Proceso.
- Objetivo del Proceso.
- Identificación de Activos.
- Riesgo.
- Causas (Amenazas y Vulnerabilidades).
- Descripción del Riesgo.
- Efectos de la materialización del Riesgo.

4.4.2 Análisis de riesgos

Documentar y especificar cada una de las etapas surtidas para el proceso de Gestión de Riesgos para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria.

Acciones fundamentales para valorar el riesgo:

- Identificar controles existentes.
- Verificar efectividad de los controles.
- Establecer prioridades de tratamiento

4.5 Etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO27005.

- **Identificación del riesgo:** Determinar que podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir esta pérdida.
- **Identificación de los activos:** Se debería llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. ***Para realizar esta identificación es necesario revisar la guía de gestión de activos adjunta al MSPI.***
- **Identificación de las amenazas:** Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas)

Se muestra la Serie de amenazas en la siguiente tabla:

D= Deliberadas, A= Accidentales, E= Ambientales

Tabla 6. Amenazas comunes

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E

Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Pérdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
Compromiso de información	Interceptación de señales de interferencia comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	
	Recuperación de medios reciclados o desechados	
	Divulgación	
	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
	Fallas del equipo	
	Mal funcionamiento del equipo	
	Saturación del sistema de información	
	Mal funcionamiento del software	

Fallas técnicas	Incumplimiento en el mantenimiento del sistema de información.	
Acciones no autorizadas	Uso no autorizado del equipo	
	Copia fraudulenta del software	
	Uso de software falso o copiado	
	Corrupción de los datos	
	Procesamiento ilegal de datos	
Compromiso funciones	Error en el uso	
	Abuso de derechos	
	Falsificación de derechos	
	Negación de acciones	
	Incumplimiento en la disponibilidad del personal	

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 20-21.

Tabla 7. Fuentes de amenazas humanas

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	● Piratería. ● Ingeniería Social. ● Intrusión, accesos forzados al sistema. ● Acceso no autorizado.

Criminal de computación la	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	● Crimen por computador Acto fraudulento ● Soborno de la información ● Suplantación de identidad ● Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	● Bomba/Terrorismo ● Guerra de la información ● Ataques contra el sistema DDoS. ● Penetración en el sistema ● Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos	Ventaja competitiva Espionaje económico	● Ventaja de defensa ● Ventaja política ● Explotación económica
extranjeros, otros intereses)		● Hurto de información ● Intrusión en privacidad personal ● Ingeniería social ● Penetración en el sistema ● Acceso no autorizado al sistema

Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.
--	---	---

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 21-22

4.6 Identificación de controles existentes

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

Un control existente planificado se podría calificar como ineficaz, insuficiente o injustificado, si es injustificado o insuficiente.

Actividades para revisar controles existentes o planificados:

- Revisando los documentos que contengan información sobre los controles.
- Verificación con las personas responsables de la seguridad de la información y los usuarios.

- Efectuar revisiones en sitio comparando los controles implementados contra la lista de controles que deberían estar.
- Cuáles están implementados correctamente y si son o no eficaces.
- Revisión de los resultados de las auditorías internas.

4.7 Identificación de las vulnerabilidades

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes.

Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal
- Ambiente físico
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas

Tabla 8 Vulnerabilidades conocidas y métodos para la valoración de la misma.

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento

HARDWARE	Sensibilidad a la radiación Electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación.	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso

SOFTWARE	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Mal funcionamiento del software
	Ausencia de copias de respaldo	Mal funcionamiento del software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta

RED	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autenticación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
LUGAR	Uso inadecuado o descuidado del control	

	de acceso físico a las edificaciones y los recintos	
	Ubicación en área susceptible de inundación	
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	
ORGANIZACIÓN	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información.	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del

		sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo

	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 24-30.

4.8 Identificación de las consecuencias

Es necesario tener:

- Lista de activos de información y su relación con cada proceso de la entidad.
- Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia

En esta actividad se deben identificar los daños o las consecuencias para entidad que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades relacionadas a un activo.

Las entidades deberían identificar las consecuencias operativas de los escenarios de incidentes en términos de:

- Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Pérdida de oportunidad
- Salud y seguridad
- Costo financiero
- Imagen, reputación y buen nombre.

4.9 Evaluación de riesgo

Se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”, y presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en lo siguiente:

Tabla 9. Matriz de calificación, evaluación y respuesta a los riesgos

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)		B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi seguro (5)	A	A	E	E	E
B: Zona de riesgo Baja: Asumir el riesgo M: Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir E: Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir					

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 32.

Teniendo en cuenta las siguientes tablas y de impacto son las siguientes:

Tabla 10. Especificaciones de probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA	CALIFICACIÓN
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.	20%
2	Improbable	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 5 años.	40%
3	Posible	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años.	60%
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año.	80%
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año	100%

Nota: Tomada de “Guía para la administración del riesgo”, DAFP, 2011, p. 28.

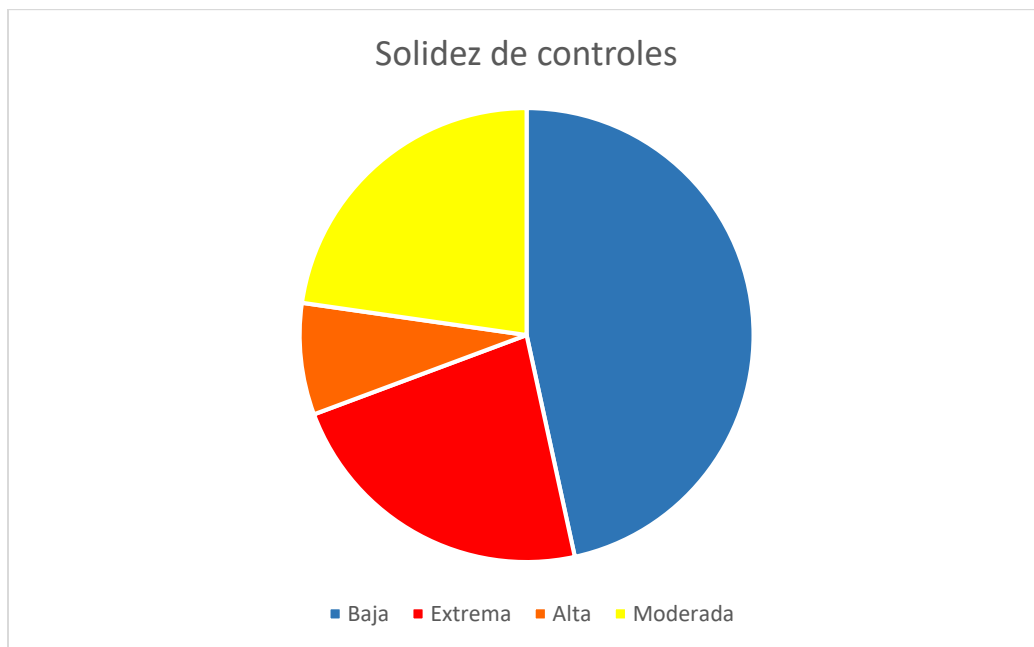
Tabla 11. Especificación del nivel de impacto

NIVEL	DESCRIPTOR	DESCRIPCIÓN	CALIFICACIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.	20%
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.	40%
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.	60%
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad	80%
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.	100%

Nota: Tomada de “Guía para la administración del riesgo”, por DAFP, 2011, p. 28.

Teniendo en cuenta la evaluación para cada uno de los controles de la tabla 10, se calculará la solidez de los controles, en este caso la variable solidez hará énfasis a las zonas de riesgo donde se califique el riesgo. Es por esto que se realiza la ilustración 8.

Ilustración 8. Grafica de solidez de controles



Fuente: Autor

Se muestra un ejemplo del análisis de uno de los riesgos de Seguridad de la Información seguidamente de la evaluación en la zona de riesgos identificados anteriormente:

Tabla 12. Ejemplo de Análisis de Riesgo

ANÁLISIS DEL RIESGO					
PROCESO: ATENCIÓN AL USUARIO					
OBJETIVO: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.					
RIESGO	CALIFICACIÓN		Tipo Impacto	Evaluación	Medidas de Respuesta
	Probabilidad	Impacto		Zona de Riesgo	
Cambio en los datos de contacto de los usuarios	3	4	CONFIDENCIALIDAD DE LA INFORMACIÓN	Extrema	Reducir el Riesgo Evitar Compartir o Transferir

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 24-30.

Tabla 13. Evaluación de la zona de riesgo

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi seguro (5)	A	A	E	E	E
B: Zona de riesgo Baja: Asumir el riesgo M: Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir E: Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir					

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 32.

4.10 Valoración de controles para el tratamiento de riesgos

Se debe tener en cuenta la evaluación realizada, inicia con la evaluación de los controles existentes en la Entidad estableciendo su descripción, su formalidad (¿se aplican?, ¿están documentados?) y su efectividad (calificación en la matriz de riesgos) para luego ser comparados con los criterios definidos en las etapas de identificación y análisis de riesgos.

Para la clasificación y valoración de los controles, se va a tener en cuenta que la clasificación entre tres tipos de Controles, Preventivos y Correctivos definidos como se indica en la siguiente ilustración:

Para realizar la valoración de los controles existentes es necesario recordar que estos se clasifican en según la guía de lineamientos para la administración del riesgo son:

Preventivos: Aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.

Correctivos: Aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

Detectivos: Aquellos que registran un evento después de presentado; sirven para descubrir resultados no previstos y alertar sobre la presencia de un riesgo

Tabla 14. Calificación de criterios de controles

Criterios	Nombres	Descripción de la calificación	Calificación
Diseño del control			
Tipo de control	Correctivo	Debilitan el impacto del evento y permite el perfeccionamiento del desempeño futuro aprendiendo de faltas pasadas.	10
	Detectivo	Ajustan procesos en curso, este tipo de control monitorean movimientos en el presente para impedir que se infrinjan los resultados esperados	50
	Preventivo	Se adelanta a situaciones e informa sobre problemas	100
Tipo de ejecución	Manual	Existe la presencia e intervención de una persona en la acción de controlar	50
	Automático	La acción de control es realizada por un programa o sistema	100
¿Se ejecuta con alguna frecuencia?	Si	Tiene ejecución asignada	100
	No	No se conoce ejecución	0
¿Está documentado?	Documentado	Esta registrado	100
	No documentado	No existe registro	0
¿Tiene evidencia?	Si	No da soporte	100
	No	Deja soporte	0
¿Tiene responsables asociados?	Si	Conoce el responsable	100
	No	No se conoce	0
Calificación final (promedio)			80
Ejecución del control			

¿Se han presentado eventos?	Si	Existen eventos relacionados a falla del control	0
	No	No existen eventos que afecte al control	100
¿El diseño del control es efectivo?	Si	Una o varias variables del control no son efectivas para el control	0
	No	La calificación de variables fue acorde al diseño	100
¿La evidencia es efectiva?	Si	La evidencia no es clara y suficiente	0
	No	La evidencia cumple como soporte de auditoria	100
Calificación final (promedio)		Con base en las variables seleccionadas se multiplica el peso de la misma por el peso de la opción, y finalmente se realiza la sumatoria de los resultados de la multiplicación hecha previamente.	20

Nota. Tomado de pirani

Las herramientas con las cuales se va a lograr una cuantificación del análisis de los controles elegidos son las siguientes:

Tabla 15. Valoración de controles

PARÁMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.			15
	Existen manuales, instructivos o procedimientos para el manejo de la herramienta			15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.			30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.			15
	La frecuencia de ejecución del control y seguimiento es adecuada.			25
	TOTAL			100

Nota: Tomada de “Guía para la administración del riesgo”, por el Departamento Administrativo de la Función Pública (DAFP), 2011, p. 35.

Tabla 16. Calificación del riesgo residual, después de aplicar controles

CONTROL	Escala de Afectación	Probabilidad	Impacto
Control 1	Probabilidad	X1	0
Control 2	Impacto		Y1
...			
Control N	Ambos	XN	XY
Total, promedio		X Promedio	Y Promedio

Nota. Tomada de “Lineamientos para la administración del riesgo” por la presidencia de la república, 2017, p. 26.

Tabla 17. Disminución de cuadrantes, después de aplicar un control

Rangos de calificación de los controles	Dependiendo si el control afecta probabilidad o impacto desplaza en la matriz de calificación, evaluación y respuesta a los riesgos	
	Cuadrantes a disminuir en la probabilidad	Cuadrantes a disminuir en el impacto
Entre 0-50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

Nota: Tomada de “Guía para la administración del riesgo”, por el Departamento Administrativo de la Función Pública (DAFP), 2011, p. 35.

Tabla 18. Escala de valoración de cuadrantes

ESCALA DE VALORACIÓN	DEFINICIÓN DE RANGOS
0	Menor al 51% no se disminuirá cuadrantes
1	Entre el 51% y el 76% se disminuirá un cuadrante
2	Mayor al 76% se disminuirá dos cuadrantes

Nota: Tomada de “Guía para la administración del riesgo”, por el Departamento Administrativo de la Función Pública (DAFP), 2011, p. 35.

5.10 Plan de implementación

Define qué tratamiento se dará a los riesgos de acuerdo con las opciones entregadas, qué acciones se implementarán, quienes serán los responsables de esta implementación. Este plan debe plantear claramente cada acción, etapa y procedimientos que se ejecutarán para poder ser monitoreado y lograr el seguimiento a la ejecución del mismo.

A continuación, se muestra la valoración del riesgo y como se disminuye la probabilidad en la matriz de riesgos.

Tabla 19. Ejemplo de valoración del riesgo, para aplicar un control

VALORACIÓN DEL RIESGO							
PROCESO: ATENCIÓN AL USUARIO							
OBJETIVO: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.							
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN			
	Probabilidad	Impacto		Tipo Controles Prob. o Impacto	PUNTAJE Herramientas para ejercer el control	PUNTAJE Seguimiento al control	Puntaje Final
Cambio en los datos de contacto de los usuarios	3	4	Procedimientos establecidos para la asignación de Roles y Perfiles dentro del sistema	PROBABILIDAD	35	20	55
			Herramienta que permita el registro y monitoreo de acciones de los usuarios sobre sistema, generando alarmas ante anomalías	PROBABILIDAD	30	25	55

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 36.

Tabla 20. Matriz de riesgos, posteriormente de aplicar un control

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi seguro (5)	A	A	E	E	E
B: Zona de riesgo Baja: Asumir el riesgo M: Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir E: Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir					

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 37.

Tabla 21. Nueva valoración de acuerdo a los controles identificados

ANÁLISIS DEL RIESGO					
PROCESO: ATENCIÓN AL USUARIO					
OBJETIVO: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.					
RIESGO	CALIFICACIÓN		Tipo Impacto	Evaluación	Medidas de Respuesta
	Probabilidad	Impacto		Zona de Riesgo	
Cambio en los datos de contacto de los usuarios	1	4	CONFIDENCIALIDAD DE LA INFORMACIÓN	ALTA	Reducir el Riesgo Evitar Compartir o Transferir

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 37-38.

4.11 Mapa de riesgos

Presenta un resumen de las acciones empleadas para la identificación, análisis y evaluación de riesgos, así como de la evaluación y elección de los controles.

Ejemplo

Para un correcto entendimiento primero debe entender las tablas 17, 18, 19, 20, 21, 22. Puesto que se visualizan mejor las variables y la calificación de estas.

Tabla 22. Proceso en el mapa de riesgos para la evaluación de un control

MAPA DE RIESGOS											
PROCESO: ATENCIÓN AL USUARIO											
OBJETIVO: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio de acuerdo a las disposiciones legales vigentes.											
RIESGO	CALIFICACIÓN		EVALUACIÓN RIESGO	CONTROLES	NUEVA CALIFICACIÓN		NUEVA EVALUACIÓN	OPCIONES MANEJO	ACCIONES	RESPUESTA	INDICADOR
	Probabilidad	Impacto			Probabilidad	Impacto					
Incumplimiento en la generación de respuestas a los usuarios (términos establecidos por la ley).	4	3	ZONA RIESGO ALTA	Aplicativo que permite mediante alarmas controlar las fechas límite para las respuestas a los usuarios sobre las comunicaciones escritas recibidas.	2	3	ZONA RIESGO MODERADA	ASUMIR O REDUCIR EL RIESGO	Asignación de identificaciones para uso del software por parte de los servidores del área. Elaboración de cronograma de capacitación por grupos	Líder Proceso Tecnología Líder Proceso Atención al usuario	Número de solicitudes contestadas en términos/ Total de Solicitudes Reporte por funcionario entregado.
				Plan de capacitaciones a los servidores, sobre la normatividad vigente y el manejo adecuado del sistema de información implementado.					Elaboración de cronograma de capacitación por grupos. Ejecutar evaluaciones finales programadas sobre temas normativos. Establecer resultados de las evaluaciones por funcionario	Líder Proceso Gestión Humana	Reporte quejas antes de la capacitación con evaluación posterior a 6 meses

Nota: Tomada de “Guía Gestión de riesgos”, por el Ministerio de Tecnologías de la Información y las Comunicaciones, 2016, p. 38.

4.12 Plantilla de controles genéricos para la gestión de riesgos informáticos

En un principio lo que quiere esta plantilla es que las empresas que no tienen bastante conocimiento en el área de gestión de riesgos informáticos, puedan ejercer los controles básicos que se encuentran en la norma 27001 en el Anexo A, en la cual se enfatizar un riesgo, una amenaza o varias, y controles cual o cuales serían los controles a realizar para evitar que algún amago logre afectar a las empresas.

Para la realización de la 24, se consideró para la columna 4 (AMENAZA) las amenazas que se encuentran en la tabla 7 (Amenazas comunes) junto con la tabla 8, y tabla 9, para una mejor orientación para analizar la presencia de cada una de ellas y sus causas más frecuentes.

Tabla 23. Plantilla de controles genéricos

Núm.	RIESGO	AMENAZA	CONTROL
A.6.2.1	Filtración de información.	Espionaje remoto, hurto de equipo, divulgación, datos provenientes de fuentes no confiables.	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Hurto de equipos con información confidencial.	Manipulación con software, uso no autorizado del equipo.	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7.2.3	Funcionario vendió datos de usuarios importantes	Abuso de derechos, corrupción de los datos, procesamiento ilegal de datos.	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.8.1.1	Pérdida de implementos de seguridad laboral	Hurto de medios o documentos, Hurto de equipo	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2	Pérdida de la caja menor	Falsificación de derechos, Abuso de derechos, Incumplimiento en la disponibilidad del personal	Los activos mantenidos en el inventario deben tener un propietario.

A.8.1.3	Daño de enrutadores debido al mal manejo del personal	Interceptación de señales de interferencia comprometida, Espionaje remoto, Mal funcionamiento del equipo	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Hurto o pérdida de equipos o herramientas que contienen información confidencial	Uso no autorizado del equipo, Abuso de derechos, Negación de acciones, Hurto de equipo.	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2.1	Falsificación de firmas	Abuso de los derechos, Error en el uso, Falsificación de derechos, Procesamiento ilegal de datos	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Inadecuado contrato	Error en el uso	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Ingreso de intrusos	Abuso de los derechos, Incumplimiento en el mantenimiento del sistema de información, Falsificación de derechos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.2	Daño de un equipo que no tenía copia de respaldo.	Destrucción de equipos o medios, Polvo, corrosión y congelamiento, Hurtos medios o documentos.	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Ingreso de un intruso al software de administración	Abuso de los derechos, Falsificación de derechos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9.1.1	Adquirir un acceso erróneo	Abuso de los derechos	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Extracción de las contraseñas	Falsificación de derechos, Espionaje remoto	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente
A.9.2.1	Caída constante del software	Mal funcionamiento del software	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

A.9.2.2	Acceso de un usuario a la interfaz de administrador	Error en el uso, Mal funcionamiento del software	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Cambio de roles	Abuso de los derechos, Corrupción de datos, Falsificación de derechos	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Filtración de información de la empresa en redes sociales	Datos provenientes de fuentes no confiables, Error en el uso	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A.9.3.1, A.12.4.2	Ingreso al software de usuarios no autorizados	Error en el uso, Abuso de los derechos	- Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta. - Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.9.4.1, A.9.4.2	Permitir el acceso a sistemas y aplicaciones sin verificar al personal que quiere ingresar	Falsificación de derechos, Abuso de los derechos	- El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. - Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A.9.4.3	Fácil ingreso de un intruso al sistema	Falsificación de derechos	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A.9.4.4	Sanciones o multas por parte de entidades	Espionaje remoto, Manipulación con software, Escucha encubierta	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Mal rendimiento en el software	Mal funcionamiento del software	Se debe restringir el acceso a los códigos fuente de los programas
A.10.1.1	Destrucción de información	Corrupción de datos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Suplantación de identidad	Espionaje remoto, Escucha encubierta	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.

A.11.1.1, A.11.1.2, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.2, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8, A.12.2.1	Ingreso de un código malicioso medio de un empleado	Incumplimiento en la disponibilidad del personal, Entrenamiento insuficiente en seguridad	● Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. ● Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. ● Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras. ● Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. ● Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. ● Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. ● Los equipos, información o software no se deben retirar de su sitio sin autorización previa. ● Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. ● Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso. ● usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada. ● Se deben implementar controles de detección, de prevención y de recuperación, combinados con la
---	--	---	--

			toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.11.1.3, A.11.2.3, A.14.2.6	Incendio eléctrico	Fuego, agua, accidente importante, destrucción del equipo o medios.	• Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. • El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño • Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.11.2.4	Impedimento a algunas funcionalidades por falta de actualización en equipos o software	Mal funcionamiento del software	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.12.1.1	Mal ejecución de un proceso	Procesamiento ilegal de datos, Incumplimiento en la disponibilidad del personal	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A.12.1.2, A.12.1.3	Proyectos inconclusos	Error en el uso, Abuso de los derechos	• Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. • Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
A.12.1.4	Fácil acceso a áreas de desarrollo, prueba y operación de un criminal de la computación	Intrusión, accesos forzados al sistema.	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

A.12.3.1	Pérdidas en la base de datos	Datos provenientes de fuentes no confiables, inconsistencia de datos, Corrupción de datos	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas
A.12.4.1	Inconsistencia en los registros del cliente.	Incumplimiento en la disponibilidad del personal	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.3	Abstrusa recuperación de datos	Ausencia de documentación, mal funcionamiento del software	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A.12.4.4	Rehúso de funcionalidades del sistema	Error en el uso	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.12.5.1, A.12.6.2	Sabotaje al sistema	Mal funcionamiento del software, Escucha encubierta	● Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. ● Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.6.1, A.12.7	Pérdida en tiempo de investigación	Uso no autorizado de equipo	● Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. ● Los requisitos y actividades de auditoría que involucren la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13.1.1, A.13.1.2	Ataques contra el sistema y aplicaciones	Escucha encubierta, Saturación del sistema de información	● Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. ● Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios

			se presten internamente o se contraten externamente.
A.13.1.3	Fallas en el acceso de tipo de usuarios	Saturación del sistema de información, Mal funcionamiento del software	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2.1, A.13.2.2	Caída de un nuevo servicio (sistema contable)	Procesamiento ilegal de los datos, Saturación del sistema de información, Negación de acciones	• Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. • Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Amenazas y soborno a clientes, empresa	Corrupción de datos, Falsificación de derechos, Procesamiento ilegal de datos	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Multas significativas de usuarios hacia la empresa	Error en el uso, Procesamiento ilegal de los datos	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14.1.1	Daño integral a la empresa	Mal funcionamiento del software, Saturación del sistema de información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Alteración no autorizada de los datos	Escucha encubierta, Espionaje remoto, Uso no autorizado del equipo	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Accesos forzados al sistema	Hurto de medios o documentos, Divulgación, Manipulación con software	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2.1	Problemas de compatibilidad con las herramientas existentes en las	Espionaje remoto, Interceptación de señales de interferencia comprometida	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.

	que confían los usuarios		
A.14.2.3, A.14.2.5	No tener tiempo para lograr reaccionar ante un ataque	Mal funcionamiento del software, Abuso de los derechos	• Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización. • Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.4	Dificultad al usar un paquete por actualización del software	Mal funcionamiento del software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.8, A.14.2.9, A.14.3.1	No encontrar mal funcionamientos del sistema para corregir	Intrusión, accesos forzados al sistema, Intrusión en el sistema	• Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad. • Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados. • Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.15.1.1	Falta de suministros de seguridad	Mala reputación	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.
A.15.1.2, A.15.1.3	Manipulación en el sistema por un criminal de la computación.	Manipulación en el sistema, Abuso de derechos, Procesamiento ilegal de datos	• Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. • Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro

			de productos y servicios de tecnología de información y comunicación.
A.15.2.1	Disminución en la gestión del desempeño por parte de los proveedores	Incumplimiento en la disponibilidad del personal, Uso inadecuado del computador, Incumplimiento en el mantenimiento del sistema de información	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Clientes insatisfechos por falta de mejoras en los sistemas	Incumplimiento en el mantenimiento del sistema de información	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.
A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5	No tener disponible los sitios web de la empresa	Ataques contra el sistema DDoS.	● Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. ● Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. ● Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. ● Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. ● Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. ● El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

A.16.1.7	Falta de evidencia al comprobar la identidad de un intruso	Intrusión en privacidad personal, Penetración en el sistema	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17.1.1	Alteración del contenido de los circuitos de memoria de computadoras y servidores	Radiación electromagnética	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2, A.17.1.3	Destrucción de la información que se clasifica como nivel mayor de confidencialidad	Incumplimiento en el mantenimiento del sistema de información	• La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. • La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.18.1.3, A.18.1.4	Hurto de información	Soborno de la información, Acceso no autorizado al sistema	• Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. • Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.
A.18.1.5	Hurto de claves del equipo de administración	Hurto de medios o documentos, Procesamiento ilegal de datos, Soborno de la información	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2.1, A.18.2.2, A.18.2.3	Incumplimiento del procesamiento y procedimientos de	Recuperación de medios reciclados o desechados, Datos provenientes de	• El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las

la información con respecto a las políticas de la empresa	fuentes no confiables, Manipulación con software y hardware	políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. • Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad. • Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información
---	---	---

Fuente: Norma ISO 27001, Adecuación autor

Capítulo 5. Requisitos y casos de uso

5.1 Requisitos no funcionales

Se describen aspectos del sistema visible por el usuario que no se relacionan en forma directa con el comportamiento funcional del sistema (Bruegge & H. Dutoit, 2002)

El software deberá manejar tres roles: administrador, operador y viewer (espectador), se mostrará una ventana al usuario para que pueda elegir el rol y posteriormente ingresar, dependiendo del rol, se mostrarán diferentes funcionalidades.

- **Rol administrador:** Tendrá acceso a todas las funcionalidades, las cuales le permitirán crear, editar, eliminar y actualizar tanto riesgos como controles, de igual forma creará los grupos de trabajo por cada riesgo y editar la matriz de riesgos.
- **Rol operador:** Tendrá acceso a la tabla de riesgos junto con sus controles predefinidos, también tendrá acceso a evaluaciones de los controles.
- **Rol viewer:** El acceso va a ser limitado, obtendrá acceso a las funciones de consultar riesgos y controles.

5.2 Requisitos funcionales

Se describen interacciones entre el sistema y su ambiente, en forma independiente a su implementación. El ambiente incluye al usuario y cualquier otro sistema con el cual interactúe (Bruegge & H. Dutoit, 2002).

El sistema debe permitir únicamente al administrador actualizar correo y contraseña.

Este software permitirá al administrador ingresar los datos de la empresa y acceder al sistema para proceder con la gestión de riesgos en seguridad informática, una vez ingrese el software le activará las funcionalidades como la de crear riesgos donde el sistema pide los datos necesarios para crear el riesgo, adicional es el encargado de crear los grupos de trabajo y asignar el responsable de cada riesgo, también puede enlazar un control al riesgo establecido, si no se valida la creación del riesgo, el sistema no permitirá la creación de controles, así mismo, puede editar la matriz de riesgo, ver las estadísticas conforme se estén desarrollando los riesgos, controles y evaluaciones, y en dado caso que llegase a presentarse un evento, el administrador es el encargado de reportarlos.

El operador puede ingresar al sistema, pero sus funciones son más limitadas, este se encargará de llevar el seguimiento al riesgo que le fue asignado, aparte de eso, se encargará de inventar los controles para dicho riesgo, junto con las evaluaciones de este mismo. De modo similar comparte actividades como reportar eventos, ver reportes estadísticos y gestionar planes de acción, al igual que el administrador.

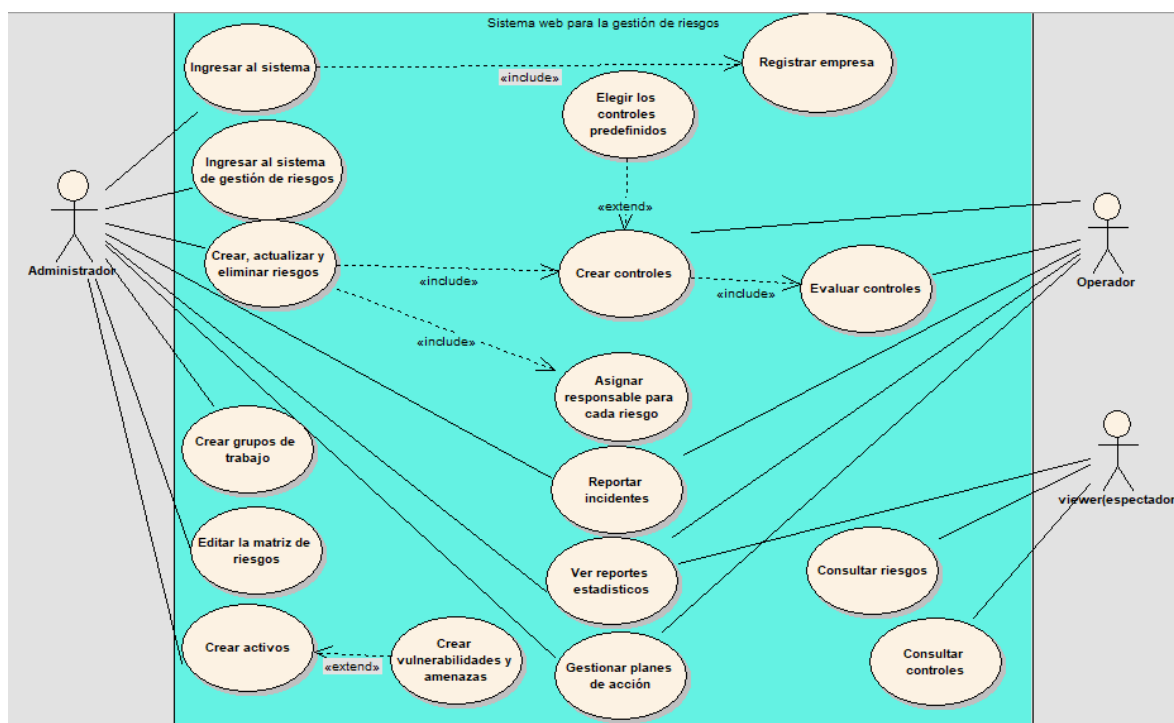
Por último, para el viewer el sistema limitará la mayoría de acciones que tratan acerca de editar o crear, puesto que, solo va a tener el rol de observador, cuyas funciones son: ver reportes estadísticos, consultar riesgos y controles.

5.3 Estándar de análisis y modelado

5.3.1 Identificación de casos de uso

En la siguiente ilustración se muestra el diagrama de casos de uso general para el sistema de gestión de riesgos en seguridad informática.

Ilustración 9. Diagrama de casos de uso de las funcionalidades según el sistema de gestión de riesgos



5.3.2 Casos de uso para rol administrador

Tabla 24. Caso de uso Ingresar al sistema de gestión de riesgos de rol administrador

Nombre del caso de uso	Ingresar usuario
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema

Flujo de eventos	El sistema presenta una ventana con los campos para ingresar la empresa y datos personales del encargado, adicional el ingreso de la contraseña
	El administrador ingresa los datos.
Condición de salida	Si los datos son correctos el sistema presentará una nueva ventana con las funcionalidades para la gestión de riesgo
	Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Fuente: Autor

Tabla 25. Caso de uso creación de riesgos con rol administrador

Nombre del caso de uso	Crear riesgos
Especificación ID	Se creará con las iniciales RGO-autonumérico (RGO -01)
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	El administrador inicia el sistema

Flujo de eventos	2. El sistema presenta una ventana con los campos para ingresar el nombre de riesgo, el impacto (insignificante, menor, moderado, mayor, catastrófico) (Observar Tabla 12), probabilidad del riesgo (raro, improbable, posible, probable, casi seguro) (Observar Tabla 11), descripción del riesgo, el riesgo afecta la continuidad de la empresa (si, no).
	3. El administrador ingresa los datos.
	4. El sistema muestra la calificación del impacto (Ver tabla 12. Columna calificación) y la probabilidad (Ver tabla 11. Columna calificación). Adicional el sistema muestra la zona de riesgo (Baja, Moderada, Alta, Extrema) (Observar Tabla 14)
Condición de salida	5. Si los datos son correctos el sistema agrega el riesgo creado y se muestra la lista de riesgos

	6. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Fuente: Autor

Tabla 26. Caso de uso modificación de riesgos con rol administrador

Nombre del caso de uso	Editar riesgos
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con los campos para editar el nombre de riesgo, el impacto (insignificante, menor, moderado, mayor, catastrófico) (Observar Tabla 12) junto con la calificación (Ver tabla 11, columna calificación), probabilidad del riesgo (raro, improbable, posible, probable, casi seguro) (Observar Tabla 11) junto

	con su calificación (Ver tabla 11, columna calificación), descripción del riesgo, y si el riesgo afecta la continuidad de la empresa. Adicional, muestra la zona del riesgo (Ver tabla 10)
	3. El administrador actualiza los datos.
Condición de salida	4. Si los datos son correctos el sistema modifica el riesgo y se muestra la lista de riesgos
	5. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Fuente: Autor

Tabla 27. Caso de uso eliminación de riesgos con rol administrador

Nombre del caso de uso	Eliminar riesgos
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos

Condición inicial	1. El administrador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con la lista de riesgos, y verifica si esté no tiene ningún control, para habilitar o bloquear la opción de eliminar.
	3. El administrador selecciona el riesgo a eliminar y le da eliminar.
Condición de salida	4. Se actualiza la página, mostrando la lista de riesgos
Requerimiento especial	El sistema consulta a la base de datos para actualizar y mostrar el contenido.

Fuente: Autor

Tabla 28. Caso de uso evaluación de riesgos con rol administrador

Nombre del caso de uso	Evaluar riesgos
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema

Flujo de eventos	2. El sistema presenta una ventana con la lista de riesgos
	3. El administrador selecciona el riesgo a evaluar y elige la opción evaluar riesgos.
	4. El sistema muestra una ventana con 2 columnas, la primera los valores actuales de riesgo (Impacto, Probabilidad) (Ver tabla 11 y 12, columna calificación), y la otra para una nueva calificación (Impacto, Probabilidad) (Ver tabla 11 y 12, columna calificación).
	5. El administrador realiza la nueva calificación y da en guardar.
Condición de salida	6. Se actualiza la página, mostrando la lista de riesgos
Requerimiento especial	El sistema consulta a la base de datos para actualizar y mostrar el contenido.

Fuente: Autor

Tabla 29. Caso de uso creación de controles con rol administrador

Nombre del caso de uso	Crear controles
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con la lista de riesgos para vincular el control a un riesgo.
	3. El administrador elige el riesgo donde quiere añadir el control
	4. El sistema presenta una ventana solicitando el nombre del control, el tipo del control (correctivo, detectivo, preventivo) (Ver 4.10) y para su calificación (Ver tabla 15), tipo de ejecución (manual, automático), si se ejecuta con frecuencia (si, no), si está documentado (documentado, sin documentar), si tiene responsables asociados (si, no).

	5. El sistema muestra una ventana para la ejecución del control, donde pregunta si se han presentado eventos (si o no), si el diseño del control es efectivo (si o no), y, por último, si la evidencia es efectiva (si o no)
	6. El administrador ingresa los datos y el sistema calcula la calificación promedio dependiendo de las respuestas. (Ver tabla 15) para entender como la calificación del sistema
Condición de salida	7. Si los datos son correctos el sistema agrega el control y se muestra la lista de controles
	8. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Tabla 30. Caso de uso selección de controles predefinidos con rol administrador

Nombre del caso de uso	Elegir controles genéricos
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con la lista de riesgos para vincular el control a un riesgo. (Ver tabla 24). En este paso solo se mostrarán la columna 2 llamada riesgo y 4 llamada control.
	3. El administrador elige el riesgo donde quiere añadir el control
	4. El sistema presenta una ventana mostrando los controles predefinidos que el sistema tiene para ese riesgo. (Ver tabla 24)
	5. El administrador elige el control

Condición de salida	6. Si los datos son correctos el sistema agrega el control y se muestra la lista de controles
	7. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para agregarlos y mostrar el contenido.

Fuente: Autor

Tabla 31. Caso de uso creación de grupos de trabajo con rol administrador

Nombre del caso de uso	Crear grupos de trabajo
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con la opción de crear grupos de trabajo
	3. El administrador añade el correo de cada uno de los integrantes del grupo, digita el nombre del grupo y le da aceptar

	6. El sistema muestra los integrantes del grupo, y adicional se le notifica a cada integrante que están como responsables de un riesgo
Condición de salida	7. Si los datos son correctos el sistema agrega el grupo de trabajo, y muestra la lista de grupos creados
	8. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y enviar los correos.

Fuente: Autor

Tabla 32. Caso de uso modificación de la matriz de riesgo con rol administrador

Nombre del caso de uso	Editar la matriz de riesgos
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema

Flujo de eventos	2. El sistema presenta una ventana con la matriz de riesgos (Ver tabla 10), esta tiene la opción de editar
	3. El administrador elige la opción de editar
	4. El sistema presenta una ventana con el panel de edición mostrando el impacto y la frecuencia por defecto (Como está en la tabla 10) pero con la opción de editarlos.
	5. El administrador ingresa el impacto y la frecuencia, acorde a la empresa y guarda los cambios
Condición de salida	7. Si los datos son correctos el sistema agrega las nuevas variables de impacto y frecuencia
	8. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema actualiza la matriz de riesgos para validarlos y mostrar el contenido.

Fuente: Autor

Tabla 33. Caso de uso reportación de incidentes con rol administrador

Nombre del caso de uso	Reportar incidentes
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con la lista de incidentes, más la opción de agregar un incidente
	3. El administrador elige agregar un incidente
	4. El sistema presenta una ventana solicitando el nombre, descripción, en dado caso que se tenga evidencia se puede adjuntar, la pregunta de si el incidente genera pérdidas (si o no), donde ocurrió el incidente, fecha y hora donde se materializó y se descubrió el incidente.
	5. El administrador ingresa los datos y le da la opción de crear incidentes.

Condición de salida	Si los datos son correctos el sistema agrega el incidente y se muestra la lista de incidentes junto con quien reportó el incidente y el estado (En gestión o finalizado).
	Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Fuente: Autor

Tabla 34. Caso de uso creación del plan de acción con rol administrador

Nombre del caso de uso	Crear plan de acción
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	El administrador inicia el sistema
Flujo de eventos	El sistema presenta una ventana con los campos para ingresar el nombre, descripción, fecha de inicio, responsable del plan, y si hay evidencia adjuntarla, adicionalmente se muestra cuáles actividades se

	quieren llevar a cabo en el plan, y la opción de adjuntar al plan de acción, riesgos, controles, ejecutores o responsables.
	3. El administrador rellena los datos y le da clic en crear
Condición de salida	4. Si los datos son correctos el sistema agrega el plan de acción y se muestra la lista de estos
	5. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Fuente: Autor

Tabla 35. Caso de uso observar reportes con rol administrador

Nombre del caso de uso	Ver reportes estadísticos
Actor participante	Iniciado por: Administrador

	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema
Flujo de eventos	2. El sistema presenta una lista de opciones entre ellas está reportes
	3. El administrador da clic en reportes
	4. El sistema presenta una ventana con el perfil de riesgo organizacional por medio de un diagrama de torta sobre solidez de los controles que se han creado. (Observar Ilustración 8)
Condición de salida	5. Si los datos son correctos el sistema generará las gráfica correspondiente.
	6. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para actualizar y mostrar el contenido.

Fuente: Autor

Tabla 36. Caso de uso creación de activos con rol administrador

Nombre del caso de uso	Crear activo
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	1. El administrador inicia el sistema y selecciona la opción de crear activo
Flujo de eventos	2. El sistema presenta una ventana con los campos para ingresar el nombre, descripción, los tipos de criterios (confidencialidad, integridad y disponibilidad) (Ver definición en 2.1) junto con su correspondiente calificación (Alta, Media, Baja) (Observar niveles de clasificación en tabla 5), los tipos de activos (Hardware, Software, Red, Personal, Lugar, Organización) (Para más detalles dirigirse a la tabla 9)
	3. El administrador rellena los datos y le da clic en crear

Condición de salida	Si los datos son correctos el sistema agrega el activo, seguidamente se observa el listado de los activos
	Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Tabla 37. Caso de uso creación de vulnerabilidades y amenazas con rol administrador

Nombre del caso de uso	Añadir vulnerabilidades y amenazas a un activo
Actor participante	Iniciado por: Administrador
	Consulta a: Base de datos
Condición inicial	El administrador inicia el sistema y selecciona la opción de activos de información
Flujo de eventos	El sistema presenta una ventana con la lista de activos y la opción de agregar vulnerabilidades y amenazas

	3. El administrador elige la opción de agregar vulnerabilidades y amenazas
	4. El sistema muestra una ventana solicitando que ingresen de que tipo es (amenaza o vulnerabilidad). Consecutivamente el nombre y la descripción. (Ver tabla 9)
Condición de salida	5. Si los datos son correctos el sistema agrega la amenaza o vulnerabilidad, inmediatamente se observa el listado de amenazas y vulnerabilidades.
	6. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

5.3.3 Casos de uso para rol operador

Tabla 38. Caso de uso creación de controles con rol operador

Nombre del caso de uso	Crear controles
Especificación ID	Se creará con las iniciales CTRL-autonumérico (CTRL-01)

Actor participante	Iniciado por: Operador
	Consulta a: Base de datos
Condición inicial	1. El operador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con la lista de riesgos para vincular el control a un riesgo.
	3. El operador elige el riesgo donde quiere añadir el control
	4. El sistema presenta una ventana solicitando el nombre del control, el tipo del control (correctivo, detectivo, preventivo), (Ver 4.10) para su calificación (Ver tabla 15), tipo de ejecución (manual, automático), si se ejecuta con alguna frecuencia (si, no), si este documentado (documentado, sin documentar), si tiene responsables asociados (si, no).
	5. . El sistema muestra una ventana para la ejecución del control, donde pregunta si se han presentado eventos (si o no), si el diseño del

	control es efectivo (si o no), y, por último, si la evidencia es efectiva (si o no)
	6. El administrador ingresa los datos y el sistema calcula la calificación promedio dependiendo de las respuestas. (Ver tabla 15) para entender como la calificación del sistema
Condición de salida	7. Si los datos son correctos el sistema agrega el control y se muestra la lista de controles
	8. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Fuente: Autor

Tabla 39. Caso de uso evaluación de controles con rol operador

Nombre del caso de uso	Evaluar controles
Actor participante	Iniciado por: Operador
	Consulta a: Base de datos

Condición inicial	1. El operador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con la lista de riesgos para vincular el control a un riesgo, adicional tiene la opción de vincular una evaluación sobre los controles que ya hayan sido vinculados a un riesgo.
	3. El operador elige el riesgo para añadir la evaluación del control
	4. El sistema presenta una ventana solicitando el nombre del control, el tipo del control (correctivo, detectivo, preventivo) (Ver 4.10), tipo de ejecución (manual, automático), si se ejecuta con alguna frecuencia (si, no), si este documentado (documentado, sin documentar), si tiene responsables asociados (si, no). Adicional a esto, En frente de cada una de las evaluaciones ya realizadas al momento de generar el control, están las casillas para seleccionar la nueva calificación del control, una vez se haya calificado cada evaluación (Recordar que las calificaciones se realizaron conforme a la tabla 15), se

	deberá realizar una justificación, donde se podrá colocar las razones por que fue un buen o mal control.
	5. El operador ingresa las calificaciones y justificaciones correspondientes conforme a las respuestas y da clic en guardar cambios. (Para la justificación se puede guiarse de la tabla 23)
	6. El sistema muestra una lista de los controles evaluados y el estado (En proceso o en evaluación)
Condición de salida	7. Si los datos son correctos el sistema agrega el control y se muestra la lista de controles
	8. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Fuente: Autor

Tabla 40. Caso de uso reportación de incidentes con rol operador

Nombre del caso de uso	Reportar incidentes
Actor participante	Iniciado por: Operador
	Consulta a: Base de datos
Condición inicial	1. El operador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con la lista de incidentes, con la opción agregar incidente
	3. El operador elige agregar un incidente
	4. El sistema presenta una ventana solicitando el nombre, descripción, en dado caso que se tenga evidencia se puede adjuntar, la pregunta de si el incidente genera pérdidas (si o no), donde ocurrió el incidente, fecha y hora donde se materializó y se descubrió el incidente.
	5. El operador ingresa los datos y le da la opción de crear incidentes.

Condición de salida	Si los datos son correctos el sistema agrega el incidente y se muestra la lista de incidentes junto con quien reportó el incidente y el estado (En gestión o finalizado).
	Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Fuente: Autor

Tabla 41. Caso de uso observar reportes con rol operador

Nombre del caso de uso	Ver reportes estadísticos
Actor participante	Iniciado por: Operador
	Consulta a: Base de datos
Condición inicial	El Operador inicia el sistema
Flujo de eventos	El sistema presenta una lista de opciones entre ellas está reportes
	El operador da clic en reportes

	4. El sistema presenta una ventana con el perfil de riesgo organizacional por medio de un diagrama de torta sobre solidez de los controles que se han creado. (Observar Ilustración 8)
Condición de salida	5. Si los datos son correctos el sistema generará la gráfica correspondiente
	6. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para actualizar y mostrar el contenido.

Fuente: Autor

Tabla 42. Caso de uso creación de planes de acción con rol operador

Nombre del caso de uso	Crear plan de acción
Actor participante	Iniciado por: Operador
	Consulta a: Base de datos
Condición inicial	1. El operador inicia el sistema
Flujo de eventos	2. El sistema presenta una ventana con los campos para ingresar el nombre,

	descripción, fecha de inicio, responsable del plan, y si hay evidencia adjuntarla, adicionalmente se muestra cuáles actividades se quieren llevar a cabo en el plan, y la opción de adjuntar al plan de acción, riesgos, controles, ejecutores o responsables.
	3. El operador rellena los datos y le da clic en crear
Condición de salida	4. Si los datos son correctos el sistema agrega el plan de acción y se muestra la lista de estos
	5. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Fuente: Autor

5.3.4 Casos de uso para rol viewer (espectador)

Tabla 43. Caso de uso consultar riesgos con rol viewer

Nombre del caso de uso	Consultar riesgos
-------------------------------	-------------------

Actor participante	Iniciado por: viewer
	Consulta a: Base de datos
Condición inicial	1. El viewer inicia el sistema
Flujo de eventos	2. El sistema presenta únicamente tres opciones
	3. El viewer elige la opción consultar riesgos
Condición de salida	4. El sistema le mostrará la lista de riesgos
	5. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Nombre del caso de uso	Consultar controles
Actor participante	Iniciado por: viewer

	Consulta a: Base de datos
Condición inicial	1. El viewer inicia el sistema
Flujo de eventos	2. El sistema presenta únicamente tres opciones
	3. El viewer elige la opción consultar controles
Condición de salida	4. El sistema le mostrará la lista de controles
	5. Si los datos son incorrectos el sistema informará el error.
Requerimiento especial	El sistema consulta a la base de datos para validarlos y mostrar el contenido.

Conclusiones

Lo expuesto anteriormente puede concluir que para una correcta gestión de riesgos en el área de seguridad informática teniendo como principal beneficiario a las pequeñas y medianas empresas, se puede aplicar en diferentes factores, y es por ello, que al sumergirse en las mejores prácticas para la recolección de requerimientos es vital que las empresas cumplan con una correcta gestión de riesgos informáticos, puesto que si no se realiza el debido soporte, se pueden generar varias pérdidas entre ellas pueden ser tanto económicas como de información.

En cuanto al enfoque de metodologías, se prefiere trabajar con Margerit ya que, es más sistemática que octave, lo que permite llevar una rapidez al organizar la información, por último, se aplican todos los requerimientos que se acotaron tanto de la norma ISO como de la guía número 7 de Ministerio de Tecnologías de la Información y las Comunicaciones, realizando así que se cumplan la clasificación y valorización de estas en la estructura y análisis del software que se requiere implementar a largo plazo.

Referencias bibliográficas

HACKNOID. Importancia de la gestión de riesgos informáticos [blog]. Blog Ciberseguridad. 26 de Agosto de 2019. [Consultado: 30 de agosto de 2022]. Disponible en: <https://www.hacknoid.com/hacknoid/importancia-de-la-gestion-de-riesgos-informaticos/#:~:text=La%20gesti%C3%B3n%20de%20riesgos%20TI%20busca%20garantizar%20la%20integridad%2C%20confidencialidad,vuelven%20cada%20vez%20m%C3%A1s%20indispensables.>

PÉREZ PORTO, Julián y MERINO, María. Seguridad informática [en línea]. (2021). [Consultado: 30 de agosto de 2022]. Disponible en: <https://definicion.de/seguridad-informatica/>

OSTEC. ISO 27002: Buenas prácticas para gestión de la seguridad de la información [blog]. Ostecblog. 30 de diciembre de 2016. [Consultado: 3 de septiembre de 2022]. Disponible en: <https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/>.

NQA. Gestión de seguridad de la información: ISO 27001 [sitio web]. [Consultado: 3 de septiembre de 2022]. Disponible en: <https://www.nqa.com/es-co/certification/standards/iso-27001.>

REDHAT. ¿Qué es la gestión de riesgos? [sitio web]. 11 de octubre de 2019. [Consultado: 4 de septiembre de 2022]. Disponible en: <https://www.redhat.com/es/topics/management/what-is-risk-management.>

MARTINS, Julia. Qué es la gestión de riesgos y cómo aplicarla a tu proyecto en solo 6 pasos [en línea]. Asana. (31 de enero de 2022). [Consultado: 4 de septiembre de 2022]. Disponible en: <https://asana.com/es/resources/project-risk-management-process.>

Gerens: Gestión de riesgos: ¿Qué es? ¿Por qué emplearla? ¿Cómo emplearla?, gestión estratégica y operativa [blog]. 4 de agosto de 2016. [Consultado 4 de septiembre de 2022]. Disponible en: <https://gerens.pe/blog/gestion-de-riesgos/>.

MARTÍN, Eliseo: ¿Qué es la gestión de riesgos en ciberseguridad?, ciberseguridad [blog]. [Consultado 4 de septiembre de 2022]. Disponible en: <https://www.grupocibernos.com/blog/que-es-la-gestion-de-riesgos-en-ciberseguridad#:~:text=La%20gesti%C3%B3n%20de%20riesgos%20en%20ciberseguridad%20es%20un%20proceso%20que,pueden%20encontrarse%20y%20logra%20reducirlas.>

UBIETA ROMERO, Fernando. Gestión de riesgos en proyectos de investigación [en línea]. Trabajo de investigación para la obtención del título de graduado de ingeniería en tecnologías industriales. Escuela técnica superior de ingenieros industriales. Universidad politécnica de Madrid 2021. 87 p. [Consultado 5 de septiembre de 2022]. Disponible en: https://oa.upm.es/68567/1/TFG_FERNANDO_UBIETA_ROMERO.pdf.

SANTOS JAIMES, Luz Marina. Guía para la evaluación de seguridad en un sistema. En: Conference: II Jornada Nacional de Seguridad Informática [en línea]. Rg. Junio 2002, nro. 12. [Consultado de 6 septiembre de 2022]. Disponible en: https://www.researchgate.net/publication/305212963_Guia_para_la_evaluacion_de_seguridad_en_un_sistema.

VEGA BRICEÑO, Edgar. Seguridad de la Información [en línea]. 1 ed. Editorial 3Ciencias: marzo 2021, 111 p. [Consultado el 3 de septiembre de 2022]. Disponible en: https://www.researchgate.net/publication/349925231_Seguridad_de_la_Informacion

ARROBASYSTEM: ¿Qué es Seguridad Informática? [blog]. [Consultado 6 de septiembre de 2022].

Disponible en: <https://arrobasystem.com/pages/seguridad-informatica>.

UNIR: ¿Qué es la seguridad informática y cuáles son sus tipos? [en línea]. [Consultado: 7 de septiembre de 2022]. Disponible en: <https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/>.

ISOTOOLS EXCELLENCE: Norma ISO 27002: El dominio político de seguridad [blog]. Blog

especializado en seguridad de la información y ciberseguridad. 3 de agosto de 2017. [Consultado 4 de septiembre de 2022]. Disponible en: <https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/>

MINTIC. Gestión de riesgos [en línea]. V.3. 01 abril de 2016, 39 p. [Consultado el 26 de septiembre de 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

GOBIERNO DE ESPAÑA. MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [en línea]. V.3. Ministerio de hacienda y administraciones públicas: octubre de 2012, 127 p. [Consultado el 26 de septiembre de 2022]. Disponible en: <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>

GOBIERNO DE ESPAÑA. Normas ISO sobre gestión de seguridad de la información. [en línea]. V.3. Ministerio de educación cultura y deporte. [Consultado el 27 de septiembre de 2022]. Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

COMPLIANCE. Gestión de Riesgos y Control Interno. [en línea]. Sistema de información. [Consultado el 15 de septiembre de 2022]. Disponible en: <https://www.compliance.com.co/la-implementacion-del-proceso-de-gestion-de-riesgos-tiene-diferentes-fases/>

ALMANZA, Andres, XXI Encuesta Nacional de Seguridad Informática. Resiliencia un aspecto clave en la ciberseguridad. [en línea]. Julio 2021. [consultado el 5 noviembre de 2022]. Disponible en: https://www.researchgate.net/publication/353128911_XXI_Encuesta_Nacional_de_Seguridad_Informatica_Resiliencia_un_aspecto_clave_en_la_ciberseguridad

Gobierno digital de Colombia, Ministerio de tecnologías de la información y las comunicaciones [en línea]. 2016. Guía Gestión de riesgos.
https://gobiernodigital.mintic.gov.co/692/articles-5482_G7_Gestion_Riesgos.pdf

Presidencia de la república, Lineamientos para la administración del riesgo. [en linea]
Agosto de 2017. [consultado el 2 noviembre de 2022]. Disponible en: http://simudatsalud-risaralda.co/normatividad_inv9/gestion/L-DE-01-Administracion-Riesgo.pdf