ANALISIS DE VULNERABILIDADES DE LOS ACTIVOS EXISTENTES EN LA EMPRESA REMGING COMO MECANISMO DE MEJORA DE LOS NIVELES DE SEGURIDAD INFORMÁTICA

JAVIER FELIPE MARQUEZ PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MALAGA
2022

ANALISIS DE VULNERABILIDADES DE LOS ACTIVOS EXISTENTES EN LA EMPRESA REMGING COMO MECANISMO DE MEJORA DE LOS NIVELES DE SEGURIDAD INFORMÁTICA

JAVIER FELIPE MARQUEZ PEREZ

Proyecto de Grado – presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

ING: DANIEL FELIPE PALOMO LUNA
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MALAGA
2022

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Málaga., Fecha sustentación

DEDICATORIA

Dedico este trabajo a mi abuela que ha sido mi ruta, ha sabido acercarme al camino del conocimiento con gran acierto, me ha visto crecer y ha sido un pilar fundamental en mi vida. A todos los miembros de mi familia que me han dado el apoyo incondicional, lo que me ha hecho fortalecer mi proyecto de vida y los sueños de ser un profesional exitoso.

AGRADECIMIENTOS

A la universidad que, con sus planes de cobertura educativa, ha permitido de muchas personas logren acceder a la educación superior.

A los docentes que nos han sabido orientar en todos los procesos de construcción significativa del conocimiento.

A las directivas del CEAD de Málaga, por su constante motivación y empeño en colaborarnos con todos los procesos administrativos, de bienestar y académicos.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE IMÁGENES

pág.

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: “es cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización”[1].

AMENAZA: “circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad” [2].

ANÁLISIS DE RIESGOS: “es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de estas, a fin de determinar los Controles adecuados para tratar el riesgo” [3].

INCIDENTE DE SEGURIDAD: “cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa ejemplo a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información”[4].

---

[1] **INCIBE**. Guía glosario de seguridad. Instituto Nacional de Ciberseguridad p.8. Tomado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf.
[2] Ibid.; 8.
[3] Ibid.; p 9.
[4] Ibid.; p11.
[5] Ibid.; 24.

POLÍTICA DE SEGURIDAD: “son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información” [5].

VULNERABILIDAD: “fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos. Las empresas deben ser conscientes de estos riesgos y mantener una actitud preventiva, así como llevar un Control de sus sistemas mediante actualizaciones periódicas”[6].

[6] Ibid.; p.30.
[7] Ibid.; p.38.

RESUMEN

El trabajo se orienta hacia el análisis de los activos informáticos de la empresa REMGING, con el consentimiento de esta, planteando un estudio descriptivo aplicado, mediante el análisis de riesgos, lo que permite determinar el estado actual de la seguridad informática. Se ejecuta con la aplicación de la metodología de análisis de riesgos MAGERIT y se trabaja de acuerdo con la norma ISO/IEC 27001, analizando el riesgo de cada activo teniendo en cuenta la probabilidad de que este se materialice; analizando los activos informáticos, sus vulnerabilidades y las amenazas. De la misma manera presenta la verificación cualitativa de las dimensiones de seguridad de la información implementadas en la empresa y la determinación del sistema de Control interno informático que se puede implementar en concordancia con los resultados obtenidos en el proceso.

Se basa en los estándares y metodologías para el Análisis y la gestión de riesgos y Control Informático, retomado los fundamentos teóricos del Portal de Administración Electrónica, que aborda Metodología de Análisis y gestión de riesgos de los sistemas de información.

Palabras clave: Riesgo, análisis de riesgos, activo de información, vulnerabilidad, política de seguridad. Controles, MAGERIT.

ABSTRACT

The work is oriented towards the analysis of the IT assets of the REMGING company, proposing an applied descriptive study, through risk analysis, which allows determining the current state of IT security in the same, with the application of the methodology of MAGERIT risk analysis, as for which it works in accordance with the ISO/IEC 27001 standard, which entails calculating the risk of each asset taking into account the probability that the risk materializes; analyzing computer assets, their vulnerabilities and threats and the impact that could be generated. In the same way, it presents the qualitative verification of the information security dimensions implemented in the company and the determination of the internal computer Control system that can be implemented in accordance with the results obtained in the process.

It is based on the standards and methodologies for Risk Analysis and Management and Computer Control from computer audit techniques, taking up the theoretical foundations of the Electronic Administration Portal, (2012). MAGERIT V.3, (2013).

The project concludes with the presentation to the REMINGENIERIA company of the analysis of the causes of the main risks existing in the information system, the impacts associated with vulnerabilities especially oriented to data management and the Controls required by information security and submitting the relevant security proposal.

Keywords: Risk, risk analysis, information asset, vulnerability, security policy. Controls, MAGERIT.

INTRODUCCIÓN

El proyecto que se llevó a cabo está orientado desde la dinámica de gestión de seguridad de la información aplicado a la empresa REMGING, partiendo de la fundamentación del objetivo principal de todo sistema de gestión de la seguridad de la información. Se orienta a la protección de la integridad, confidencialidad, disponibilidad de todos los activos que existen dentro de una organización y esto sólo se lleva a cabo con éxito si se realiza un minucioso análisis de los riesgos, a los cuales pueden enfrentarse todas las organizaciones, de manera que se visualice como un insumo base, a partir del cual la empresa pueda diseñar planes y Controles necesarios para la protección de los activos.

Hoy en día muchas organizaciones se ven afectadas por serios problemas, debido a la no destinación de recursos necesarios para afrontar las amenazas, vulnerabilidades y riesgos que se generan en los activos de información, lo que ha llevado en muchas circunstancias a generar grandes pérdidas, tanto económicas como de acreditación frente a los contextos donde están inmersos las mismas. Con base en lo anterior, decide permitir el análisis de la seguridad de la información de manera que se logre acceder para identificar los riesgos a los que se enfrenta la empresa.

Se presenta así un análisis de riesgos, apoyado en los estándares y normas internacionales de la norma ISO/IEC 20071, que se orientan a minimizar todos los relacionado a la prevención de ataques, desastres, de manera que se esté a la vanguardia de estos, antes de que estos se generen y de esta forma se logra la definición del análisis de riesgos, los cuales se constituyen en un insumo importante para la empresa. Posteriormente generaron diseño de políticas claras, que permiten identificar los niveles de riesgos que se hayan encontrado, realizando el mismo atendiendo a los marcos referenciales que cobija la metodología de análisis MAGERIT versión 3.

Este proyecto se estructura en capítulos donde se visualizan los preliminares, marcos referenciales. El capítulo donde se identifican las vulnerabilidades, amenazas y riesgos de seguridad del área informática en cada uno de los activos informáticos de la empresa. El capítulo orientado al descubrimiento del riesgo para cada activo a partir de la probabilidad que la amenaza se materialice, y el capítulo orientado al reconocimiento cualitativo de las dimensiones de la seguridad de la información implementadas en la empresa. Se finaliza con el capítulo que crea el sistema de Control interno informático coherente con los resultados del análisis de riesgos de la empresa.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La empresa REMGING en su estrategia de consolidación, aún no ha llegado a la implementación de una auditoría de sistemas que se ligue a la estrategia de la Seguridad y control informático, ya que esta es un eje fundamental en su mismo funcionamiento y garantía de calidad en la prestación de sus servicios. En contactos preliminares, no se observa que se haya ejecutado una revisión de los resultados de un análisis de riesgos informáticos, para que los trabajadores y técnicos se concienticen de que toda amenaza hallada ha de ser Controlada. No se percibe mayor atención al desempeño de las funciones inherentes a cada cargo, olvidando la importancia del Control permanente en los activos y los salvaguardas que han de estar implementándose como garantía de seguridad en las diversas áreas y dominios existentes en la empresa.

La seguridad informática al ser un tema amplio, éste debe tenerse presente en todos los escenarios de la organización; por lo tanto, aún no se visualiza un buen desarrollo en el análisis que se requiere para hacer un diagnóstico del sistema informático, tratando de identificar las posibles vulnerabilidades, amenazas y fallas de seguridad existentes en el tratamiento y manejo de los activos informáticos y de la información en cada uno de los procesos. De aquí se deriva la necesidad de un profesional con las competencias que le permiten reconocer estándares y aplicar metodologías para el Análisis y la Gestión de riesgos, de igual forma que su Control pertinente y oportuno.

La empresa REMGING, fue un escenario significativo para ejecutar este proyecto aplicado, pues permitió transferir el conocimiento y las competencias desarrolladas en el transcurso de la carrera, al igual orientado al área de tecnología que involucra seguridad en redes. Se dinamiza al igual la voluntad de las partes para ejecutar un proyecto en el marco real a la expectativa de los hallazgos.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el análisis de vulnerabilidades de los activos informáticos REMGING y la generación de recomendaciones para minimizar riesgos, permitirá mejorar los niveles de seguridad de la información en esta empresa?

2. JUSTIFICACIÓN

El proyecto surge como resultado del aumento acelerado de amenazas informáticas, dentro de las cuales las empresas presentan diversas vulnerabilidades en los activos, permitiendo así a los intrusos la posibilidad de sustraer información, datos como usuarios y contraseñas en busca de un beneficio particular a espaldas de esta. Se imprime un sello de exigencia a toda organización, de orientar su acción de manera prioritaria al tema de la seguridad de la información. Grandes organizaciones ya han asumido la responsabilidad sobre los mecanismos de protección informática, y al igual, ser conscientes de que, a pesar de sus esfuerzos, se verifican fallas con procesos estructurados que buscan atacar y generar incidentes de seguridad de información. Se hace imprescindible el aseguramiento de la confidencialidad, integridad y disponibilidad de la información, en la búsqueda de llegar a mejores niveles de competitividad y beneficio tanto empresarial como para los clientes que confían en la organización para el acceso a los servicios requeridos.

El Proyecto permite establecer la metodología de gestión de seguridad informática de manera clara estructurada, al igual que la búsqueda de la dinámica de reducción del riesgo, que buscó garantizar la confidencialidad de la información y a la vez la orientación, para establecer planes de contingencia informático que garanticen la continuidad del negocio tras incidentes de gravedad. La realización del proyecto reviste vital importancia, en la medida en que dinamiza la acción como especialista en seguridad informática, realizando la transferencia del conocimiento, esencialmente en el análisis y manejo de riesgos dentro de una organización, lo que lleva la apropiación de saberes en aras de trascender en la praxis de la formación.

El proyecto permite a la empresa el mantenimiento de sus niveles de competitividad, beneficio económico, conformidad legal, e imagen empresarial obligatorios para lograr los objetivos de la organización. Es imprescindible el considerar la importancia que

revisten los datos e información, los cuales se conciben como la materia prima para la gestión de la empresa REMGING, ejecutando el desarrollo del proyecto por considerarlo un aporte significativo para seguridad informática.

El proyecto es significativo en la medida en que plantea hacer algo que no se había ejecutado en le empresa, en el momento es una necesidad prioritaria. La empresa busca crecimiento y cobertura, por ello la toma de decisiones sobre el análisis de riesgos, se revierte en la dinámica de mejoramiento continuo en todos los procesos y acciones que ejecuta en aras del cumplimiento de la misión. En la misma evaluación de los resultados del proyecto, se logra una documentación completa del análisis de riesgos y una propuesta de mitigación del riesgo orientado al manejo de datos de forma segura.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un análisis de riesgos mediante la metodología MAGERIT, sobre los activos existentes en la empresa REMGING como mecanismo de mejora de los niveles de seguridad informática.

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Identificar los riesgos de seguridad en cada uno de los activos informáticos, mediante la metodología MAGERIT.

- ✓ Analizar el riesgo asociado a cada uno de los activos de la empresa, a partir de la probabilidad que la amenaza se materialice.

- ✓ Evaluar cualitativamente las dimensiones de la seguridad de la información implementadas en la empresa, teniendo en cuenta el análisis anterior.

- ✓ Estructurar un informe de los riesgos que permita establecer recomendaciones tendientes a mejorar la seguridad de la empresa.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Seguridad de la Información. El tema de la seguridad de la información traza todo un conglomerado de estrategias, de manera que pueda estar ligado a las necesidades tanto de la organización, como de los clientes externos que acceden a los servicios relacionados con la TIC. En la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos. Se debe distinguir entre los dos, porque "forman la base y dan la razón, justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección" [7].

La seguridad de la información está directamente relacionada a los criterios de confidencialidad, integridad y disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan en la seguridad de la misma, cuyo objetivo busca en todo sentido que se involucre directamente la protección de los datos, buscando que intrusos no logren alcanzar el propósito de acceder, dentro del estado que se ha de contrarrestar y evitar la pérdida y modificación no autorizada de la información.

Además de los criterios de protección orientados a la búsqueda de confidencialidad, integridad y disponibilidad de los datos, existen diversos requisitos como la misma autenticidad, lo que ha de estar contemplado dentro de los objetivos trazados para un asertivo análisis de riesgos, dinamizando así medidas para evitar que intrusos lleguen a

[7] MARKUS Reb. Gestión de Riesgo en la Seguridad Informática [en línea]. https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

acceder maliciosamente a la información y generar grandes daños ya sea materiales o inmateriales.

4.1.2 Análisis y Gestión de Riesgos. En el proceso que se realiza dentro de la gestión del riesgo, se halla en primer escenario el análisis de este, cuyo propósito se orienta a la búsqueda de los componentes de un sistema que requieren protección, sus vulnerabilidades y las amenazas que se generan colocando en gran peligro una organización, cuyo objetivo busca la valoración del grado de riesgo. Para la ejecución de este análisis existen diversas metodologías que tiene un propósito común en el esquema de valoración del riesgo.

De acuerdo con MAGERIT, el análisis y gestión de los riesgos resulta de gran importancia en el funcionamiento de toda organización, porque permite generar conciencia de su existencia, examinarlos, tratarlos y por ende la debida preparación para enfrentar a las auditorias, certificaciones o acreditaciones gubernamentales.

La Organización Internacional (ISO/IEC 20071) define riesgo tecnológico como “La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existente de un activo o un grupo de activos, generándole pérdidas o daños” [8]. Retomando esta conceptualización la tarea se dinamiza partiendo de la comprensión, asimilación de variados elementos para poderlos trasferir significativamente a la praxis en determinada organización. Así la materialización de una amenaza puede ser mitigada en la medida en que se tenga un oportuno conocimiento, tanto de los daños que estos pueden generar, como de las diversas maneras de mitigación. La multiplicidad de metodologías de valoración de los riesgos permite la ejecución de diagnósticos previos.

[8] Norma ISO/IEC 20071, tomado de: Introducción y comprensión a los sistemas de gestión de seguridad de la información SGSI (ISO/IEC /IEC 27001-27002), [en línea].: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53580?page=13

En el ejercicio que se deriva del análisis de riesgos se hace necesario el acudir a los marcos referenciales trazados dentro de la política de seguridad en un sistema de información, dentro de la cual se plantean acciones en un orden secuencial y lógico:

- ✓ Realizar inventario y valoración de los activos.
- ✓ Identificar y valorar la amenaza que puedan afectar a la seguridad de los activos.
- ✓ Identificar las medidas de seguridad existentes.
- ✓ Identificar y evaluar las vulnerabilidades de los activos a las amenazas que les afectan.
- ✓ Identificar los objetivos de seguridad de la organización.
- ✓ Determinar sistemas de medición de riesgo.
- ✓ Determinar el impacto que produciría un ataque.
- ✓ Identificar y seleccionar las medidas de protección.

4.1.3 Auditoria. Se describe como el análisis pormenorizado de un sistema de información que permite descubrir, identificar y corregir vulnerabilidades en los activos que lo componen y en los procesos que se realizan. Centra su orientación practica en la verificación de cumplimiento de los diversos los objetivos de la política de seguridad de la organización. Permite realizar un diagnóstico de la realidad actual de una organización en lo referente a los sistemas de seguridad de la información que se ejecutan.

Como resultado de un proceso de auditoría, se han de reflejar los resultados y hallazgos, en un documento que un informe detallado que contiene:

- ✓ Descripción de las características de los activos y procesos analizados, debidamente organizados atendiendo a las áreas auditadas.

- ✓ Análisis de las relaciones y dependencias entre activos o en el proceso de la información.
- ✓ Relación y evaluación de las vulnerabilidades detectadas en cada activo o subconjunto de activos y procesos.
- ✓ Verificación del cumplimiento de la normativa en el ámbito de la seguridad.
- ✓ Propuesta de medida preventiva y de corrección.

4.1.4 Metodología MAGERIT. La metodología MAGERIT de análisis y gestión de riesgos elaborada y establecida por el Consejo Superior de Administración Electrónica de España, dentro de su marco referencial presenta todo un compendio de acciones y actividades que ha de seguir una organización que orienta sus propósitos en la línea de gestión de riesgos. Igualmente, se está actualizando en nuevas versiones para generar mayores niveles de asertividad en su aplicación en escenarios reales.

MAGERIT persigue Objetivos Directos [9]. que buscan concienciar a los responsables de las organizaciones de la información, sobre la existencia de riesgos y de la necesidad de gestionarlos, ofreciendo un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC), llevando así a la empresa a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Lo mismo que la preparación a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Esta metodología plantea una secuencia lógica para el tratamiento y análisis de riesgos que se presentan en la organización. Se tienen en cuenta todos los activos que se hallan y que involucran el tratamiento de la información como hardware, software, recurso humano, etc. Para la categorización de los activos se estructuran de acuerdo con la función que realizan, atendiendo al mismo tratamiento de la información.

[9] Ibid. pg. 27

El análisis de los riesgos se realiza mediante la ejecución de diversas tareas como se aprecia en la Tabla 1, donde se presenta el método de análisis de riesgos, el cual se basa en los activos existentes en la organización. lo cual inicia con su identificación, para llegar a la valoración de estos, sendero que permite el descubrimiento de las mismas amenazas que se presentan, logrando la estimación de estos, convirtiéndose en un insumo fundamental para el tratamiento ajustado a las necesidades.

Tabla 1. Método de análisis de riesgos

METODO DE ANÁLISIS DE RIESGOS
MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

MAR.1 – Caracterización de los activos. En esta actividad se identifican los activos importantes y como resultado de esta se genera el informe “modelo de valor”. Como

subtareas se tiene la identificación de los activos, identificación de las dependencias entre activos y valoración de los activos.

MAR.2: Caracterización de las amenazas*.* En esta actividad se identifican las principales amenazas sobre el sistema a analizar, arrojando como resultado el informe “mapa de riesgos”. Consta de dos subtareas a saber: la Identificación de las amenazas y la valoración de estas

MAR.3: Caracterización de las salvaguardas. Se identifican aquellas desplegadas en el sistema a analizar, como resultado de esta actividad se obtiene tres informes: Declaración de aplicabilidad; evaluación de salvaguardas y vulnerabilidades del sistema. Como Subtareas dentro de esta actividad se tiene la identificación de las salvaguardas y su valoración.

MAR.4: Estimación del estado de riesgo. En esta actividad se procesan todos los datos recopilados en la ejecución de las actividades anteriormente relacionadas con el fin de realizar los siguientes informes:

- ✓ Estado de riesgo: estimación de impacto y riesgo, resultado de las dos subtareas de esta actividad.
- ✓ Insuficiencias: Contiene las deficiencias o debilidades de las salvaguardas encontradas en el sistema.

4.1.5. Valoración de los activos. En toda organización y teniendo en cuenta los activos ya identificados, se dinamiza la acción de valoración del riesgo. No todos los riesgos se pueden valorar, en la medida en que sus funciones no son similares, al contrario, cada activo desempeña una función especial atendiendo a la operatividad, pues al verificar la información que fluye en cada uno desde la misma perspectiva de las dinámicas de procesamiento o el mismo almacenamiento de la información. de la organización.

4.1.6. Dimensiones de seguridad. Cada activo al ser valorado parte de las dimensiones de seguridad, como se aprecia en las Tablas 2 y 3, lo que se obtiene como resultado su posición en relación con la misma dimensión. Hay diferentes aspectos en los cuales puede actuar un Control, los cuales han de tenerse en cuenta:

[PR] Se requieren procedimientos tanto para la operación de los Controles preventivos como para la gestión de incidencias y la recuperación tras las mismas.

[PER] Política de personal, que es necesaria cuando se consideran sistemas atendidos por personal. La política de personal debe ser de formación continua.

La Tabla 2 retoma la dimensión de seguridad desde su confidencialidad.

Tabla 2. Dimensiones de valoración de activos

CODIGO	CONFIDENCIALIDAD	DESCRIPCIÓN
C	Confidencial	Restringida a un conjunto de personas de la organización
I	Uso interno	Sólo personal de la organización o terceros autorizados
P	Uso Público	Sólo personal de la organización o terceros autorizados
S	Sensible	Información que requiere Controles estrictos para su protección
N	Normal	Información que requiere Controles habituales para su protección

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Tabla 2. (Continuación)

CODIGO	CONFIDENCIALIDAD	DESCRIPCIÓN
	Baja	Información que requiere Controles mínimos para su protección
MA	Muy alta	Tiempo tolerable de interrupción menor a 2 horas
A	Alta	Tiempo tolerable mayor a 2 horas y menor a 4 horas
M	Media	Tiempo tolerable mayor a 4 horas y menor a 1 día
MB	Media Baja	Tiempo tolerable mayor a 1 día y menor a 2 días
B	Baja	Tiempo tolerable mayor a 2 días y menor a 5 días

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

La Tabla 3. retoma una valoración cuantitativa de los activos teniendo en cuenta el costo.

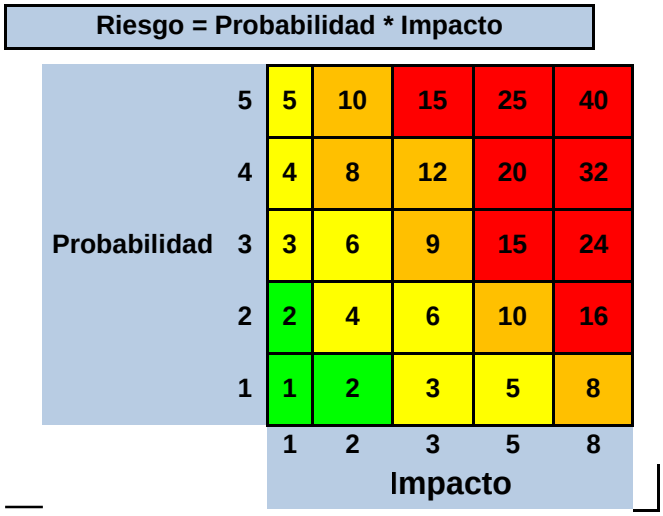
Tabla 3. Valoración cuantitativa de los activos

CODIGO	VALOR ACTIVO	VALOR	DESCRIPCION
MA	Muy Alto	5	$ 5.000.001 o más
A	Alto	4	$ 3.001.000 a $5.000.000
M	Medio	3	$ 1.501.000 a $ 1.500.000
B	Bajo	2	$ 501.000 a 1.500.000
MB	Muy Bajo	1	0 a $ 500.000

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

4.1.7 Estimación del riesgo. La estimación del riesgo es obtenida por medio de la siguiente ecuación matemática: *Riesgo = probabilidad x impacto,* ver Imagen 1.

Imagen 1. Estimación del riesgo



Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Lo anterior permite categorizar los diversos niveles como se aprecia en la Tabla 4.

Tabla 4. Nivel de riesgo

Aceptable	Retenido.
Tolerable	Para activos no críticos, y tratado como intolerable.
Intolerable	Atención inmediata y monitoreo permanente.
Extremo	Tratado en forma similar al intolerable gerencial.

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Con los resultados obtenidos con este análisis se procede a la evaluación. Para cada activo, el proceso concluye si el riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los Controles (salvaguardas) necesarios. En esta actividad se concluye el Informe de evaluación de riesgos TI, el cual es utilizado para elaborar el Plan de tratamiento de riesgos.

El objetivo general del análisis de riesgos es identificar las causas potenciales de los principales riesgos que amenazan el entorno informático. Esta identificación se realiza en una determinada área para así tener suficiente información, optando por un diseño apropiado implantación de mecanismos de Control con el fin de minimizar los efectos de eventos no deseados.

Un minucioso análisis de riesgos; identificar, definir y revisar los Controles de seguridad; determinar si se requiere incrementar las medidas de seguridad; y la identificación de los riesgos, los perímetros de seguridad, Controles de acceso y los lugares de mayor peligro, pueden hacer el mantenimiento más fácilmente.

4.2 MARCO CONCEPTUAL

Seguridad de la información: “Es la disciplina que se ocupa y señala normas procedimientos, métodos y técnicas destinadas a conseguir un sistema de información segura y confiable”[10]. Estas actividades o involucran la protección de los datos organizados y clasificados importantes para una organización evitando la filtración y vulneración de su confidencialidad y el que sea modificada y afectada su integridad, tema de interés general en la medida de que las claves de la seguridad de la información han de ser de gran confiabilidad para los usuarios de toda organización.

[10] AGUILERA L, Purificación. Seguridad informática. Protocolos de políticas de seguridad informática. Colombia, Universidad Católica, 2005. Disponible en internet: Https.//docplayer.es/5605322_protocolos:de: políticas_de_seguridad_informática_Para_Las_universidades_de_Risaralda_Jorge_Luis_villa. HTML.

Gestión de riesgos: "Selecciona la implantación de salvaguardas para conocer prevenir, impedir, reducir o controlar los riesgos identificados. La gestión de riesgos en la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis"[11]. Éste ha de ejecutarse en coordinación con los objetivos las estrategias y las políticas de la empresa, ligado a las actividades de gestión de riesgos, que permitan elaborar un plan de seguridad de manera que pueda dar cumplimiento a sus objetivos dentro del marco de la seguridad de la información. Toda organización siempre estará con cierto grado de riesgo y nunca a pesar de realizar diversas auditorías se puede llegar a cero, dado que la seguridad absoluta no existe; por lo tanto, siempre hay que aceptar un cierto nivel de riesgo el mismo que debe ser conocido y sometido a su más estricto nivel. Cuando una organización acepta el nivel de riesgo es consciente de las formas como se opera al interior de está dando la confianza al sistema de seguridad y minimizar así la incertidumbre.

MAGERIT: En el proceso de elaboración del análisis y gestión del riesgo se parte de una metodología ya experimentada, lo que conlleva a gestionar la seguridad de la información. El modelo MAGERIT, es la metodología que ha sido recomendada para el análisis de gestión de redes de riesgos porque esta permite realizar una evaluación profunda de la seguridad de los sistemas de información en toda organización. Consiste en un método formal para investigar los riesgos que soportan los sistemas de información y para recomendar las medidas apropiadas que deberían adoptarse para Controlar los riesgos dentro de una organización. Los objetivos directos se orientan a concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de minimizarlos a tiempo, al igual que ofrecer un método sistemático para el análisis de riesgos y ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo Control. Los objetivos indirectos se orientan a preparar a la organización para dinamizar estrategias de mejora.

[11] LOPEZ; Francisco, AMUTIO Miguel. Metodología y análisis de gestión de riesgos de los sistemas de información: Ministerio de administraciones públicas. 2006

MAGERIT, al igual implica la evaluación del impacto y la violación de la seguridad que tiene una organización, señalando riesgos existentes, identificando amenazas que se acechan el sistema de información y determinando la vulnerabilidad del sistema de prevención de dichas amenazas obteniendo unos resultados. Los resultados del análisis permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer prevenir, impedir, reducir o Controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus perjuicios.

Riesgo: "Probabilidad de que una amenaza informática logre convertirse en un evento real, generándose en uno o más activos causando daños o perjuicios a la organización"[12]. Dicho concepto indica lo que podría suceder a los activos, si no son protegidos asertivamente. Es necesario conocer las características importantes de cada activo, así como el peligro en las que se encuentren para lo cual será necesario analizar el sistema.

Análisis de riesgos: "Proceso sistemático para estimar la magnitud de los riesgos a que está expuesto a una organización. El análisis de riesgo aporta un modelo del sistema en términos de activos amenazas y salvaguarda y es un factor importante para Controlar todas las actividades con énfasis en su pertinencia de acuerdo con la lectura que se ejecute"[13]. El análisis de riesgos conlleva a la determinación de las circunstancias de protección en la que se encuentran los activos. Una vez identificado y analizado los riesgos se hace fundamental tomar decisiones con el fin de contrarrestar los mismos.

Amenaza: "Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir daño ya sea material o inmaterial sobre los elementos de un sistema, en el caso de seguridad informática, los elementos de información". [14]Obedeciendo que la seguridad

[12] Ibid. p 12
[13] Ibid. P 15
[14] Ibid. p 16

informática tiene como propósito garantizar la confidencialidad, integridad, disponibilidad de la seguridad de los datos e informaciones, las amenazas y la consecuencia de daños que puede causar un evento exitoso también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos informaciones

Vulnerabilidad: "Debilidad existente en los activos que se encuentran en una organización y que en determinado momento puede ser aprovechada por un ataque cibernético, de manera que se logre acceso no autorizado o de similar forma llegar a ejecutar acciones no autorizadas en un sistema informático"[15]. Las vulnerabilidades pueden permitir a los atacantes ejecutar código, acceder a la memoria de un sistema, instalar programa maligno y robar, destruir o modificar datos confidenciales. Las vulnerabilidades pueden explotarse mediante una variedad de métodos que incluyen inyección SQL, desbordamientos de *búfer, scripting* entre sitios y *kits* de explotación de código abierto que buscan vulnerabilidades conocidas y debilidades de seguridad en aplicaciones web.

4.3 ANTECEDENTES O ESTADO ACTUAL

El proyecto parte de la identificación de diversos estudios que se han ejecutado en los cuales se tienen en cuenta la gestión del riesgo dentro de diversas organizaciones con una aplicación metodológica coincidente con la planteada en el proyecto.

LUCERO Antonio y LAVERDE John, (2012). Análisis y gestión de riesgos de los sistemas de la Cooperativa de crédito y de ahorro Jardín Azuayo, Tesis de grado Especialización en seguridad informática; UNAD, Escuela de Ciencias Básicas Tecnología e Ingeniería, proponen como objetivo la aplicación de la Metodología MAGERIT versión 2., donde se

[15] Ibid. p 17

traza el diagnóstico de los riesgos hallados lo que se da como un insumo fundamental del cual se deriva un plan de gestión de riesgos que favorece la operatividad empresarial

ORTIZ MANRIQUE; Edwin Omar. (2016). Análisis de causas de riesgos en la protección de la información de la empresa Soltec-ing y recomendaciones de seguridad. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, analiza los riesgos que se presentan en la empresa con la información, a través de un diagnóstico descriptivo y aplicado, clasificando y evaluando el nivel de impacto de los riesgos de acuerdo con la escala definida por la metodología MAGERIT versión 3. Mediante el análisis de riesgo de orden cualitativo, facilitó conocer el grado de seguridad aplicada en la empresa, sugiriendo las salvaguardas necesarias con la finalidad de reducir los niveles de riesgo e impacto, culminando con el diseño de la política de seguridad buscó mejorar en los procesos, aplicando medidas correctivas y preventivas para reducir los niveles de riesgos existentes, facilitando el reconocimiento de riesgos residuales a los cuales aún se encuentra expuesto la empresa.

QUINTERO Yamile- (2015) Análisis y gestión de riesgos de los sistemas de información de la alcaldía municipal de Tuluá. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, orienta desde la aplicación de la metodología MAGERIT versión 3, se enfoca en el análisis y gestión de riesgos de los sistemas de información de la alcaldía municipal de Tuluá en el año 2015, definiendo por fases la gestión del riesgo en dos fases que incluyen la etapa de análisis y la etapa de tratamiento del riesgo, lo que contribuyó a la apropiación y transferencia del conocimiento en lo referido al análisis y tratamiento de los riesgos.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. [En

línea]. Versión 2.0.2. 49 Bogotá, 2011. Disponible en Internet: (css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf), se presenta una estrategia de preparación por parte del gobierno para soportar el sistema de administración de seguridad de la información como un modelo sostenible. Allí se describe la dinámica que debe existir en una organización para la implementación de un modelo de seguridad. Se hace énfasis en la definición de la dinámica de preparación de la organización ante cualquier análisis que se pueda realizar en este sentido, lo cual revierte vital importancia para luego aplicar medidas de seguridad con los resultados obtenidos en este proyecto.

Se busca también la continuidad en la gestión de los riesgos, retomando los consejos de implementación de métricas de la comunidad internacional referidas a los indicadores: de la norma ISO/IEC 27001, soporte documental que pretende ayudar a otros que estén trabajando en la implementación de los estándares allí contemplados. Cada organización puede modificarlos atendiendo a las necesidades la empresa seleccionada.

Las diversas actividades de gestión del riesgo y el aseguramiento de la seguridad en la información, requieren concienciación de las personas, para aceptación de pruebas pertinentes, simulacros y a la vez reflexiones para aumentar la confianza en el plano gerencial sobre las responsabilidades de cada una de las personas a la hora de buscar los mecanismos de gestión de seguridad de la información, lo cual requiere un proceso sistemático, muy bien documentado y conocido por cada uno de los miembros de la organización.

La orientación sobre temas de seguridad de la información obedece a las mismas necesidades de la empresa, por ello se puede recurrir a la información contemplada en, “lo que no se puede pasar de alto para gestionar la seguridad de la información”.[16]Se

[16] Revista Seguridad. Cultura de prevención para ti. Pu. No.22. Publisher. https://revista.seguridad.unam.mx/print/2205.

consideran aspectos fundamentales como las políticas de seguridad, la clasificación de la información corporativa, el enfoque del análisis de riesgos. A la par de la orientación retomada de la normatividad en las organizaciones políticas de seguridad de la información, donde define el documento de consignación de reglas y requisitos que debe cumplir toda la organización, las metas objetivos y procedimientos aceptables en un área determinada, proveyendo así un marco para que los empleados de una organización ejecuten las acciones óptimas para minimizar los riesgos asegurando sus activos, su protección, como accesos no autorizados, modificación divulgación o destrucción.

4.4 MARCO LEGAL

Principios para el Tratamiento de datos personales [17]. A continuación, se listan los principios que en materia de tratamiento de datos personales ha reglado el gobierno colombiano a través del Artículo 4° de la Ley Estatutaria 1581 de 2012, la cual fue reglamentada parcialmente por el Decreto Nacional 1377 de 2013.Estos son:

- ✓ Principio de legalidad: El Tratamiento de los datos personales es una actividad reglada y debe estar sujeta a las disposiciones legales vigentes aplicables.
- ✓ Principio de finalidad: El Tratamiento de datos personales debe obedecer a una finalidad legítima en consonancia con la Constitución y la Ley, por lo tanto, se debe informar al titular de los datos personales.
- ✓ Principio de libertad: El Tratamiento de datos personales sólo se puede realizar previo consentimiento expreso e informado por parte del titular, por lo tanto, estos datos no podrán ser conseguidos o divulgados sin su previa autorización. d) principio de

[17] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria de 2012. (17 octubre). Por la cual se dictan disposiciones generales para la protección de datos personales. [en línea]. Bogotá D.C.: Alcaldía de Bogotá. 2012. [Consultado el 23 de mayo, 2015]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

veracidad o calidad: Esta información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. No se pueden tratar datos parciales, incompletos, fraccionados o que induzcan a error.

- ✓ Principio de transparencia: En el Tratamiento de datos se debe garantizar al titular el derecho de obtener en cualquier momento y sin restricciones, información acerca de la existencia de cualquier tipo de dato o de información del cual es titular.
- ✓ Principio de acceso y circulación restringida: El Tratamiento de datos se sujeta a los límites que se derivan de la naturaleza de estos, en consecuencia, este tratamiento solamente podrá hacerse por personas autorizadas por el titular, por tanto, no debe estar disponible en internet u otros medios de divulgación, a excepción de la información que es pública.
- ✓ Principio de confidencialidad: Todas las personas que administren actualicen o intervengan en el Tratamiento de datos están obligadas a garantizar la reserva de la información y están obligados a mantener su confidencialidad y no revelarla a terceros inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento.
- ✓ Principio de seguridad: La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

4.5 MARCO CONTEXTUAL

Nombre de la empresa: REMGING S.A.S. como empresa orientada a las telecomunicaciones, para solucionar problemas que se presentan en determinadas áreas geográficas, donde es difícil el acceso a los servicios de internet con estrategias y aplicaciones innovadoras que se adaptan a las necesidades de los clientes, dependiendo

de los requerimientos que se planteen para la prestación del servicio y los objetos que acompañan su actividad cotidiana.

En la actualidad el acceso a la misma se encuentra en la página web, la cual ilustra y anuncia los servicios que presta, su respectivo logo, y las especificaciones de cobertura y entorno tecnológico que sustenta su operatividad.

La empresa dinamiza su visibilidad accediendo a los recursos web disponibles, y que se hallan a disposición de gran número de personas, lo que ha permitido una respuesta positiva por parte de los usuarios que buscan ser cubiertos en el plano de las diversas actividades en las que se sustentan los servicios.

Gracias a las posibilidades del mercado en línea la empresa diseña una estrategia de gran impacto, e innovadora derivada de la forma como buscan el vitrinismo, que atrae usuarios interesados en ser clientes, dada las características regionales en diversas áreas, donde el acceso a internet ha sido difícil, al igual se acompaña de avances tecnológicos pertinentes.

La Imagen 2, denominada imagen institucional se convierte en el primer acercamiento a la organización, donde se halla una descripción detallada de cada uno de los servicios y su funcionamiento, mediante imagen y caracterización que la hace diferencial de otras existentes en el contexto.

Permite percibir la existencia de un panorama completo que se caracteriza por llegar a diversas regiones con servicios de conexión esencialmente a internet. Su ubicación en la web facilita el acercamiento a la empresa desde diversos escenarios y es de ágil el acceso desde la nominación del requerimiento que cada usuario digita en esta dinámica de marketing institucional. En referencias halladas de la imagen se describe la facilidad de acceso a tipo de servicio relacionado con conectividad, redes y sistemas de acceso

superando la diversidad de dificultades que se hallan en la ubicación geográfica que ha sido asumida a partir de previo diagnóstico que ilustrado la ubicación empresarial.

Imagen 2. Imagen institucional

Fuente: REMGING. 2021. Servicios Recuperado de https://remging.com/wp-content/uploads/2020/03/housing-antena-remging.jpg

Reseña histórica: REMGING S.A.S, es una compañía de Telecomunicaciones con una trayectoria de casi 15 años en el mercado colombiano, y lleva sus servicios de conectividad a sitios donde otras empresas no llegan. Brinda servicios de internet, Telemetría, Telemedida y conectividad; así mismo, alquiler de espacio en sus torres de comunicaciones y su datacenter. Como proveedor de internet (ISP), ofrece servicios de internet inalámbrico con la mejor calidad, y siempre pensando en la necesidad de sus clientes, llegando a lugares donde ya no hay cobertura por otros operadores. Cuenta con planes tanto para hogares como clientes corporativos. Cuenta con productos y servicios fijos y móviles para Telemetría y Telemedida en el sector energético, ambiental e industrial, así como servicios técnicos en sitio o remoto.

Misión: En REMGING S.A.S cree firmemente que la tecnología es la herramienta fundamental para unir y mejorar la vida de las personas, las empresas y la sociedad en general. Con esta premisa, llevamos nuestros servicios de comunicaciones inalámbricas de conectividad y telemetría, con la mejor calidad del servicio, a aquellos sitios donde la conectividad es poca o nula, generando también un impulso económico y social en estas regiones.

Visión: REMGING S.A.S. busca ser reconocida a nivel nacional como una empresa líder en llevar servicios de conectividad y comunicaciones inalámbricas de alta calidad a sectores rurales o de poco acceso, con soluciones tecnológicas integrales de punta y competitivas, que la hacen el punto de referencia por su mejora continua y constante, capaz de enfrentar los desafíos competitivos del entorno y la globalización.

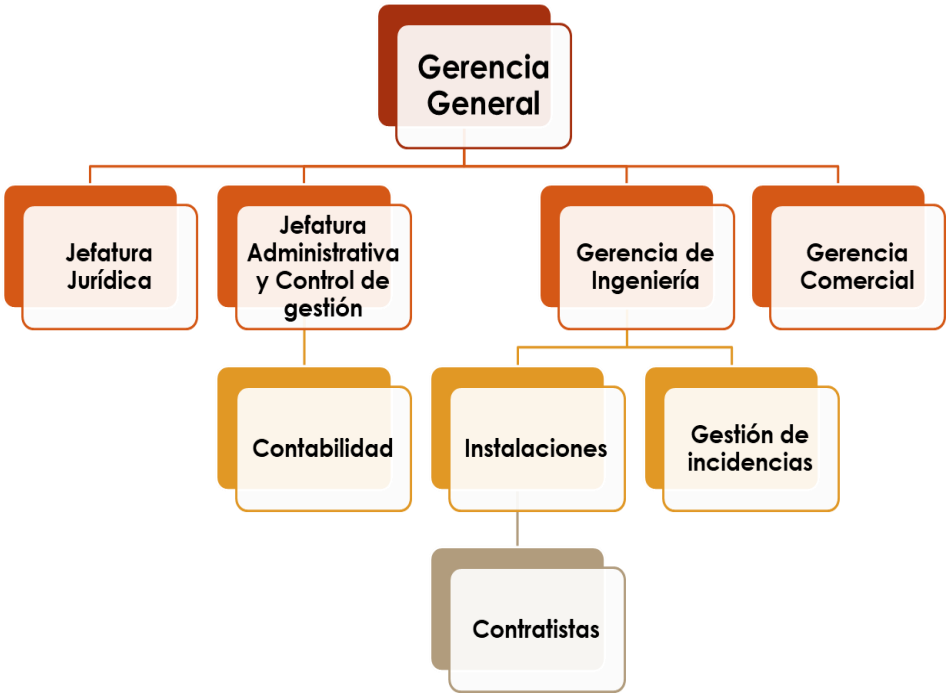
Valores: Los valores que identifican a REMGING S.A.S. son:

- ✓ Honestidad: Transparencia en la atención hacia nuestros clientes, porque así creamos credibilidad y confianza hacia ellos.
- ✓ Calidad: Buscamos que nuestros servicios cumplan con los parámetros ofrecidos.
- ✓ Pasión: En nuestra empresa somos apasionados por lo que hacemos y lo reflejamos en nuestro trabajo, porque creemos en lo que hacemos.
- ✓ Competitividad: Nuestra meta es ser los primeros en el mercado y eso lo demostramos en cada una las tareas que realizamos aportando a la Organización.
- ✓ Orientación al cliente: Buscamos adecuarnos a las necesidades de nuestros clientes, por eso estamos constantemente actualizando nuestra propuesta de valor, porque ellos son nuestro eje central.

Estructura organizacional: Está representada en un organigrama de acuerdo con la necesidad de estructuración y funcionamiento**.** La gerencia general enmarca al igual la jerarquía de la cual dependen las jefaturas jurídicas, administrativa y de control de la

gestión, la gerencia de ingeniería y gerencial comercial. La gerencia de ingeniería deriva la contabilidad, instalaciones y gestión de incidencias. Ver imagen 3.

Imagen 3. Estructura organizacional REMGING S.A.S



Fuente: Base documental REMGING S.A.S

REMGING S.A.S suministra productos y servicios fijos - móviles en el sector energético, ambiental e industrial, así como servicios técnicos en sitio o remoto. Hace parte de las empresas que plantean soluciones tecnológicas a la medida, en razón a que atienden necesidades reales en contextos de difícil acceso a redes de internet.

A nivel de servicios:

- ✓ Realiza todas las labores concernientes a la recolección de datos de información generada en los medidores multifuncionales.
- ✓ Diagnostica y repara medidores y equipos de comunicaciones.

- ✓ Alquila sim cards de operadores móviles, como parte de las soluciones a nivel de comunicaciones.
- ✓ También cuenta con personal capacitado para realizar todas las labores de telemedida como:
- ✓ Lectura de datos suministrados por los medidores en sitio, en caso de presentarse falla en el medio de comunicación.
- ✓ Normalización en sitio.
- ✓ Acompañamiento con el operador de red para realizar todas las verificaciones del estado de la telemedida.

La variedad de servicios que presta la empresa, le permite continuidad, requiriendo cualificación permanente tato de quienes administran, como de quienes se hallan en la parte operativa. De igual manera los requerimientos tecnológicos que se actualizan permanentemente se convierten en una necesidad de asignación de recursos, para su adquisición y funcionamiento a la vanguardia de los avances existentes.

El personal que labora en la empresa se enfrenta a los nuevos retos, que derivan de la necesidad de actualización de los conocimientos y el desarrollo de competencias dentro del área de telecomunicaciones, como del compendio de saberes para prestar servicios de asesorías a clientes y soluciones de casos puntuales, en mesa de ayuda o soporte técnico. El administrador y representante legal es consciente de los avances apresurados de la tecnología y al igual las innumerables empresas que se hallan en el mercado, que se esfuerzan por ofrecer calidad en los servicios y valores agregados que las hacen más llamativas a los posibles clientes.

En la Imagen 4, se puede apreciar la cobertura de los servicios de la empresa, la cual abarca un alto porcentaje del territorio del país, incluyendo áreas fronterizas, colocándola en un escenario favorable para su desarrollo y crecimiento y que puede llegar a convertirse en una de las empresas líderes a nivel nacional en la medida que involucra

servicios que se han convertido en una necesidad, tanto para las personas como para las organizaciones e instituciones.

Imagen 4. Cobertura REMGING S.A.S

Fuente: REMGING. 2021. Cobertura. Recuperada de https://remging.com/wp-content/uploads/2020/03/cobertura-remging-colombia.png

Entorno tecnológico actual: La empresa permanentemente esta direccionando su estructura tecnológica hacia nuevos desarrollos que puedan impactar en un servicio actualizado y que dé respuesta a las necesidades del entorno donde se halla inmersa, al igual que en los diversos puntos donde expande se cobertura en servicios. De esta forma se ha mantenido en el mercado y sus intervenciones permiten generar alto grado de satisfacción de los clientes. Debido a la diversidad de servicios y productos que ofrece,

REMGING S.A.S. ha utilizado un conjunto de herramientas y tecnologías para su funcionamiento tal y como se muestra en la Tabla 5, tomada de estudios de investigación "Propuesta de un sistema de información integrada para la empresa REMGING S.A.S" orientada al entorno tecnológico actual y que reposan en las fuentes documentales[18]:

Tabla 5. Entorno tecnológico actual

NOMBRE	DESCRIPCIÓN PLATAFORMA	ESPECIFICACIÓN TÉCNICA SERVIDOR	ESPECIFICACIÓN TÉCNICA CLIENTE	PROCESO IMPACTADO
WhatsUp Gold	Software utilizado para la gestión del estado de los servidores, rendimiento de los dispositivos de red, almacenamiento y servicios inalámbricos.	Servidor HP ProLiant G6, 2 Procesadores: Xeon 1.8Ghz 2 discos duros Sata: (512 GB y 128 GB) Los dos en arreglo SCSI Sata 16GB de memoria RAM Servidor tipo rack de 1 unidad	Se accede a est plataforma a través de la web.	Realización de Instalaciones Gestión de incidentes técnicos
Cisco Assistant Management	Cisco Network Assistant es utilizado para configurar y gestionar servicios comunes en switches, enrutadores que requieren gestión de manera sistematizada.	Servidor HP Proliant G7, 2 Procesadores: Xeon 2.8Ghz 1 disco duro-Sata 512 GB 32GB de memoria RAM 2 fuentes de poder	Se accede a la herramienta a través de la PC por escritorio remoto Windows server 2012 de 64 bits	Realización de Instalaciones Gestión de Incidentes Técnicos

Fuente: CISTOPHER MALDONADO, Reyes y otros. Propuesta de un sistema de información integrada para la empresa REMGING S.A.S. Universidad politécnica de Madrid. 2020

[18] CISTOPHER MALDONADO, Reyes y otros. Propuesta de un sistema de información integrada para la empresa REMGING S.A.S. Universidad politécnica de Madrid. 2020

Tabla 5. (Continuación)

NOMBRE	DESCRIPCIÓN PLATAFORMA	ESPECIFICACIÓN TÉCNICA SERVIDOR	ESPECIFICACIÓN TÉCNICA CLIENTE	PROCESO IMPACADO
Kerio Operator	Software utilizado para telefonía IP dentro de las oficinas de la compañía y para clientes	Servidor Sony G6 1 Procesador: Xeon 2.8Ghz 1 disco duro-Sata 512 GB 16GB de memoria RAM.	Se accede a esta plataforma a través de la web	Realización de Instalaciones Gestión de Incidentes Técnicos
Primestone	Plataforma utilizada para realizar lecturas a equipos de Telemedida.	Plataforma tercerizada	Se accede a esta plataforma a través de la web	Realización de Instalaciones *Gestión de Incidentes Técnicos
World office	Herramienta utilizada para llevar la contabilidad de la empresa.	Servidor HP Proliant G7 Procesador: Xeon 2.8Ghz 2 discos duros Sata 512 GB 32GB de memoria RAM Servidor tipo rack de 1 unidad	Se accede a la herramienta a través de PC por escritorio remoto Windows server 2012 de 64 bits	Gestión Contable para Compras y Ventas
Plataforma Payu	Plataforma de pagos online que procesa transacciones locales en sitios de comercio electrónico .	Plataforma tercerizada	Se accede a esta plataforma a través de la web	Gestión de Tesorería

Fuente: CISTOPHER MALDONADO, Reyes y otros. Propuesta de un sistema de información integrada para la empresa REMGING S.A.S. Universidad politécnica de Madrid. 2020

Tabla 5. (Continuación)

NOMBRE	DESCRIPCIÓN PLATAFORMA	ESPECIFICACIÓN TÉCNICA SERVIDOR	ESPECIFICACIÓN TÉCNICA CLIENTE	PROCESO IMPACTADO
Portal REMGING S.A.S.	www.REMGING S.A.S.com	Desarrollo propio	Se accede a esta plataforma a través de la web	Gestión de Ventas Atención al cliente
Correo institucional Calendario y Gestión Documental	Suite de Google	Plataforma tercerizada	Se accede a esta plataforma a través de la web	Atención al cliente Gestión de Tesorería Realización de Instalaciones Gestión de Compras Gestión de Ventas

Fuente: CISTOPHER MALDONADO, Reyes y otros. Propuesta de un sistema de información integrada para la empresa REMGING S.A.S. Universidad politécnica de Madrid. 2020

5. DISEÑO METODOLÓGICO

El trabajo se orienta hacia la análisis de las vulnerabilidades de activos informáticos de la empresa REMGING, planteando un estudio descriptivo aplicado, mediante el análisis de riesgos, lo que permite determinar el estado actual de la seguridad informática en la misma, con la aplicación de la metodología de análisis de riesgos MAGERIT, al igual se trabaja de acuerdo a la norma ISO/IEC 27001, que conlleva el "cálculo del riesgo de cada activo teniendo en cuenta la probabilidades que el riesgo se materialice. SE analizan los activos informáticos, sus vulnerabilidades y las amenazas y el impacto que se podría generar. De la misma manera presenta la verificación cualitativa de las dimensiones de seguridad de la información implementadas en la empresa, y la determinación del sistema de Control interno informático que se puede implementar en concordancia con los resultados obtenidos en el proceso"[19].

Se basa en los estándares y metodologías para el Análisis y la gestión de riesgos y Control Informático a partir de técnicas de auditoria informática, retomado los fundamentos MAGERIT V.3.

Aborda Metodología de Análisis y gestión de riesgos de los sistemas de información; ahondando en los planteado en Córdova R., N. (2012)[20] MAGERIT referidos a amenazas y vulnerabilidades más frecuentes.

[19] Norma ISO/IEC 20071, tomado de: Introducción y comprensión a los sistemas de gestión de seguridad de la información SGSI (ISO/IEC /IEC 27001-27002), Gómez, L. & Álvarez, A. 2012. *Guía de aplicación de la Norma UNE-ISO/IEC /IEC 27001 sobre seguridad en sistemas de información para pymes*. Recuperado de: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53580?page=13

[20] CORDOBA R., N. Evaluación de riesgos, Amenazas y Vulnerabilidades. (2012) Recuperado de http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova_RN/Cap5.PDF, Erb,

5.1. LOCALIZACIÓN

El trabajo orientado al análisis de riesgos se ubica en la REMGING S.A.S, ubicada en la ciudad de Bogotá, Departamento de Cundinamarca y extiende sus servicios a las áreas del departamento de difícil acceso a servicios de internet, como se precia en la Imagen 4.

Imagen 4. Localización empresa REMGING S.A.S

Fuente: REMGING. 2021. Localización. Recuperado de https://remging.com/wp-content/uploads/2021/06/housing/maps.jpg

5.2 METODOLOGÍA

Para el desarrollo de los objetivos se atiende a los marcos referenciales de la Norma ISO/IEC /IC 27001, los cuales sustentan la ruta a seguir en este tipo proyectos y que esbozan claramente el proceso para la ejecución de un Sistema de Seguridad de la Información. Por sus implicaciones que derivan del estudio al interior de la empresa y relacionado desde la base de los activos, se trabaja mediante trabajo de campo y la

ejecución de entrevistas directas y así se tiene en cuenta el acercamiento a la empresa y por lo tanto el encuentro con su representante legal, quién conoce perfectamente el funcionamiento de la misma, y a la vez posee un pleno dominio sobre los activos existentes, lo cual constituye una fortaleza en el desarrollo del proceso metodológico a seguir en el proyecto.

Se centra la atención en la herramienta más pertinente en estos casos, y es la entrevista directa conversacional, pues resulta muy efectiva para obtener datos relevantes y significativos, especialmente de la persona que ha consolidado la empresa y que fundamenta muy bien el funcionamiento y las acciones que se ejecutan al interior de esta. Las entrevistas permiten determinar, tanto los activos existentes como vulnerabilidades, conductas y conocimientos que se tienen sobre la seguridad de la información. De igual forma se orienta la entrevista con el personal y los técnicos de mantenimiento; se observan las conductas, el grado de conocimiento que ellos podían tener en seguridad informática y el análisis de la cotidianidad y movimientos que se realizan alrededor de los diferentes activos.

Tanto el representante legal, como el personal de la empresa acompañan los diversos escenarios tanto de observación de cada uno de los activos, como las respuestas que se generan enmarcadas en el estudio y que pueden representar un aporte significativo, en la medida en que ellos son quienes están cotidianamente en contacto con los activos de la organización e igualmente pueden describir en detalle cada evento que se genera en los diversos activos de la empresa, e incluso las formas que han considerado viables en el manejo de los riesgos que se presentan.

En la Tabla 6, se aprecian las fases del diseño metodológico, ruta que se siguió para el desarrollo del proyecto y que describe cada una de las fases, encaminadas a lograr los propósitos trazados y que buscan dinamizar momentos clave, logrando ubicar la cronología asertiva en este tipo de intervenciones.

Tabla. 6. Fases del diseño metodológico

FASE	DESCRIPCION
1. IDENTIFICACION DE ACTIVOS	En esta fase se realiza acercamiento directo a la empresa REMGING, con el propósito de poder indagar sobre los activos existentes para su caracterización e inicio de proceso en la Matriz MAGERIT sustento del trabajo.
2. ANALISIS DE RIESGOS	Se indaga sobre las deficiencias o fallas que se pueden identificar y que el determinado momento pueden materializarse.
3. IDENTIFICACION DE VULNERABILIDADES	Se dinamiza la transferencia del conocimiento mediante herramientas que puedan ser ejecutadas sobre sistemas de información, los activos, y lo pertinente con el estado de seguridad existente. Se identifican amenazas
4. ANALISIS DE VULNERABILIDADES	Se parte del desarrollo derivado de la ubicación de los diferentes datos hallados en la matriz MAGERIT, que conduce a la valoración de riesgos y aloja sustento válido para direccionar recomendaciones pertinentes a la empresa que son indispensables en el marco de la seguridad de la información. Se plantea el impacto de los activos, y mapa de calor.
5. RECOMENDACIONES	Se esboza el plan de tratamiento de los riesgos y los diversos Controles que se pueden aplicar en la empresa REMGING a partir de la norma ISO/IEC /IC 20071

Fuente: Autor

6. ANÁLISIS DE RESULTADOS.

6.1 IDENTIFICAR LOS RIESGOS DE SEGURIDAD EN CADA UNO DE LOS ACTIVOS INFORMÁTICOS MEDIANTE LA METODOLOGÍA MAGERIT.

Partiendo del sustento real, toda organización en cualquier momento se encuentra expuesta a riesgos, dado que, a pesar de los avances tecnológicos, no se puede estar seguro del 100% de Control de los riesgos que puedan generarse alrededor de la misma. Es de exigencia y de imperativo esencial el estar a la vanguardia de todo evento que pueda interferir negativamente dentro de los activos existentes, y que pueden ser vulnerados en determinado momento, argumento que permite sensibilizar al representante legal, que deriva en la disponibilidad para el trabajo de campo que conduce al análisis de riesgos. Para que la correcta aplicación de esta etapa se pueda generar se propone los siguientes objetivos.

- ✓ Determinar los activos más significativos que posee la empresa.
- ✓ Establecer las amenazas a las que están expuestas cada activo.
- ✓ Escoger salvaguardas apropiadas para los activos.
- ✓ Estimar el impacto si se materializa alguna amenaza.

Atendiendo a lo anterior, se diseñan dentro de la planeación del proyecto, para llegar a una asertiva tarea de análisis de riesgos, verificando así de manera metódica un ejercicio, que llevó a dibujar la realidad concreta dentro del análisis de los activos de la empresa objeto de este proyecto.

Se requiere el estudio de los referentes teóricos, atendiendo al método planteado para el análisis de amenazas y riesgos existentes en la seguridad informática, que pueden colocar en riesgo la misma empresa. De esta manera se plantea una propuesta que pueda contrarrestar o mitigar los mismos.

La metodología MAGERIT hace énfasis al análisis de los riesgos que deben minimizarse con medidas de seguridad que se generen; pues para esta metodología la atención al conocimiento de los riesgos permite que se realice un proceso fiable seguro y que genere el direccionamiento de un plan de tratamiento pertinente con la situación identificada.

Se retoma la primera fase, que se direcciona en la presencia física de la empresa, lo que permite la identificación del inventario y los activos, los cuales han de responder asertivamente a los criterios de la seguridad; disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Se requiere aquí en esta etapa la transferencia del conocimiento que derive el sustento teórico para la identificación de los activos. Se denomina activos a los recursos del sistema de información relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos. El activo esencial es la información que maneja el sistema es decir los datos. Alrededor de estos datos se pueden identificar otros activos importantes que integran los sistemas de información, como lo son los servicios que se pueden prestar gracias aquellos datos y los servicios que se necesitan para poder operar. Dentro de los hallazgos en los activos de una organización se pueden identificar:

- ✓ Las aplicaciones informáticas que permiten manejar los datos.
- ✓ Los equipos informáticos que permiten hospedar datos aplicaciones y servicios.
- ✓ La Red de comunicaciones, que permitan intercambian datos.
- ✓ Los soportes de información que son dispositivos de almacenamiento de datos.
- ✓ El equipamiento auxiliar que complementa el material informático.
- ✓ Las instalaciones que acogen equipos informáticos y de comunicaciones.
- ✓ Las personas que operan todos los elementos citados.

- ✓ Los servicios donde se halla la función que satisface una necesidad de los usuarios y allí se encuentran los servicios instrumentales, y servicios contratados a otra organización que les proporcione sus propios medios.
- ✓ Las aplicaciones se refieren a las tareas que han sido automatizadas para su desempeño en un equipo informático como los programas, aplicativos desarrollos.
- ✓ Los equipos informáticos están dados por los bienes materiales físicos destinados a soportar directa o indirectamente los servicios que presta la organización, y son depositarios de datos.
- ✓ Las redes de comunicaciones abarcan tanto instalaciones, como a medios de transporte ahí están directamente comprometidos en este servicio las redes, telefonía, servicio de Internet que pueden ser propios o contratados de la organización.
- ✓ El equipamiento auxiliar abarca todos aquellos equipos que sirven de soporte a los sistemas de información a pesar de que esto no estén directamente relacionado con los datos como las fuentes de alimentación, el generador eléctrico cableado mobiliarios cajas puentes entre otros.
- ✓ Las Instalaciones albergan toda la infraestructura donde se localizan los sistemas de información y comunicación, es decir todos los sistemas de redes y telecomunicaciones.
- ✓ El personal está involucrando todas aquellas personas tanto directivas como auxiliares personas relacionadas con los sistemas de información que involucran a una organización en su funcionamiento.

Se enmarca el reconocimiento de los activos, ver Tabla 7, partiendo de los hallados en las oficinas de operatividad de la empresa, como al igual los que se requieren para acceso remoto, los cuales están ubicados en el área de influencia hasta donde llegan los servicios que oferta la empresa. Se realiza vista a los diversos cerros para poder visualizar tanto el inventario de los activos como las condiciones en las que se encuentra tanto el activo, como los accesos a los mismos.

Tabla 7. Inventario de los activos informáticos

N°	Activos de Información	Nombre del activo de información	Proceso propietario activo
1	[S] SERVICIOS	[S] Servidor de impresión.	Oficina principal
2	[S] SERVICIOS	[S]Servidor de contabilidad	Oficina principal
3	[S] SERVICIOS	[S]Servidor de archivos.	Servidor
4	[SW] SOFTWARE	[SW] Página web	Equipos de cómputo
5	[SW] SOFTWARE	[SW] WhatsUp Gold	Equipos de cómputo
6	[SW] SOFTWARE	[SW] CISCO NETWORD	Equipos de cómputo
7	[SW] SOFTWARE	[SW] Firewall Kerio Control	Equipos
8	[HW] EQUIPAMENTO INFORMÁTICO	[HW] SW Principal	Oficina principal
9	[L] INSTALACIONES	[L] Torre salitre 15 M	El salitre
10	[HW] EQUIPAMIENTO INFORMÁTICO	[HW] Routers	Clientes
11	[L] INSTALACIONES	[L] Torre cerro norte 40 M	La Calera
12	[HW] EQUIPAMIENTO INFORMÁTICO	[HW] Computador portátil HP	Oficina principal
13	[HW] EQUIPAMIENTO INFORMÁTICO	[HW] computador portátil HP (ventas)	Oficina principal
14	[HW] EQUIPAMIENTO INFORMÁTICO	[E1] Servidor principal	Oficina principal
15	[COM] REDES DE COMUNICACIONES	[COM] puntos de acceso inalámbrico 1	Torre cerro norte
16	COM] REDES DE COMUNICACIONES	[COM] puntos de acceso inalámbrico 2	Torre salitre
17	COM] REDES DE COMUNICACIONES	[COM] puntos de acceso inalámbrico 3	Torre cerro norte
18	[P] Personal	[P] Técnicos de mantenimiento	Oficina principal
19	[P] Personal	[E1] Personal	Oficina principal

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

6.2 ANALIZAR EL RIESGO ASOCIADO A CADA UNO DE LOS ACTIVOS DE LA EMPRESA, A PARTIR DE LA PROBABILIDAD QUE LA AMENAZA SE MATERIALICE.

Para cada valoración de los activos es fundamental tener en cuenta información relevante que comprende, tanto las dimensiones en las que el activo es relevante, como la estimación de la valoración en cada dimensión. Retomando la metodología MAGERIT, partiendo de la base en que para esta matriz existen la valoración tanto cuantitativa como cualitativamente, y por lo tanto se van generando cálculo de valor de una escala cualitativa, para valorar el activo según el impacto que puede causar dentro de la organización, sus daños o pérdidas, insumo importante en este proceso la escala de valoración del riesgo, los datos son así como los resultados que analizan este trabajo en la Tabla 8.

Tabla.8. Valoración del riesgo

NOMENCLATURA	CATEGORÍA	VALORACIÓN
MA	Crítico	21 a 25
A	Importante	16 a 20
M	Apreciable	10 a 15
B	Bajo	5 a 9
MB	Despreciable	1 a 4

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

La empresa se halla en la nomenclatura M, (Muy Alta), que es una categoría critica en diversas dimensiones y luego M (Apreciable) como se observa en la Tabla 9.

Tabla 9. Valoración cualitativa de los activos de la empresa REMGING S.A.S.

	Activo	Dimensión Autenticidad	Dimensión Trazabilidad	Dimensión Confidencialidad	Dimensión Integridad	Dimensión Disponibilidad
1	[S] Servidor de impresión.	M	M	MA	MA	M
2	[S]Servidor de archivos.	MA	M	MA	MA	M
3	[SW] Pagina web	MA	M	B	M	M
4	[SW] WhatsUp Gold	M	A	MA	M	MA
5	[SW] CISCO NETWORD ASIST	M	A	M	MA	MA
6	[SW] Firewall Kerio Control	M	M	M	MA	M
7	[L] Torre el salitre 15M	B	B	MA	B	MA
8	[HW] SW Principal	M	M	MA	A	MA
9	[HW] Routers	M	M	MB	M	M
10	[L] Torre cerro norte 40M	B	M	M	M	MA
11	[S]SERVIDOR CONTABILIDAD	M	M	MA	A	MA
12	[HW] COMPUTADOR PORTATIL HP	M	M	M	M	M
13	[HW] COMPUTADOR HP (VENTAS)	M	M	M	M	M
14	[HW] Servidor Principal	M	M	MA	A	MA

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Tabla 8. (Continuación)

	Activo	Dimensión Autenticidad	Dimensión Trazabilidad	Dimensión Confidencialidad	Dimensión Integridad	Dimensión Disponibilidad
16	[COM] puntos de acceso inalámbricos (2)	B	B	MA	M	M
17	[COM] puntos de acceso inalámbricos (3)	B	B	A	MA	MA
18	[P} Técnicos en mantenimiento	M	M	MA	A	A
19	[P} Personal	B	B	M	MA	MA

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

- ✓ [S] Servidor de impresión, identificando en el resultado, el estado crítico MA, (Muy Alto) en las categorías confidencialidad e integridad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad.
- ✓ [S]Servidor de archivos, detectando en el resultado el estado crítico MA, (Muy Alto) en las categorías confidencialidad e integridad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad.
- ✓ [SW] Pagina web, se identifica en el resultado el estado crítico MA, (Muy Alto) en las categorías autenticidad, en estado M (Apreciable) se hallan las categorías, trazabilidad y en estado B (bajo) confidencialidad.
- ✓ SW] WhatsUp Gold, se ubica como resultado el estado crítico MA, (Muy Alto) en las categorías confidencialidad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad, integridad.

- ✓ [SW] CISCO NETWORD ASIST, detectando resultado el estado crítico MA, (Muy Alto) en las categorías integridad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad, confidencialidad.
- ✓ [SW] Firewall Kerio Control, ubicado en el resultado el estado crítico MA, (Muy Alto) en las categorías integridad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad, integridad.
- ✓ [L] Torre el salitre 15M, permite verificar en el resultado el estado crítico MA, (Muy Alto) en las categorías confidencialidad e integridad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad.
- ✓ [HW] SW Principal, como resultado se encuentra en el estado crítico MA, (Muy Alto) en las categorías confidencialidad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad, confidencialidad.
- ✓ [HW] Routers, corresponde el estado crítico MA, (Muy Alto) en las categorías confidencialidad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad, integridad.
- ✓ [L] Torre cerro norte 40M, presenta el estado crítico MA, (Muy Alto) en las categorías confidencialidad e integridad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad.
- ✓ [S] Servidor contabilidad, se enmarca el estado MA (muy Alto) la categoría disponibilidad; M (Apreciable) en las categorías autenticidad, trazabilidad, confidencialidad, integridad, autenticidad.
- ✓ [HW] Computador HP (ventas), aloja como resultado el estado crítico MA, (Muy Alto) en las categorías confidencialidad e integridad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad.
- ✓ [HW] Servidor Principal, se halla el estado crítico MA, (Muy Alto) en las categorías confidencialidad e integridad; en estado M (Apreciable) se hallan las categorías autenticidad, trazabilidad.
- ✓ [COM] Puntos de acceso inalámbricos´ (1), ubicados el estado crítico MA, (Muy Alto) en la categoría confidencialidad; en estado M (Apreciable) se hallan las categorías

integridad, disponibilidad, y en la categoría B (Bajo las categorías autenticidad y trazabilidad.

- ✓ [COM] Puntos de acceso inalámbricos´ (2), están en el estado crítico MA, (Muy Alto) en las categorías confidencialidad; en estado M (Apreciable) se hallan las categorías integración, autenticidad; B (Bajo) las categorías autenticidad y trazabilidad.
- ✓ [COM] Puntos de acceso inalámbricos´ (3), aloja como resultado el estado crítico MA, (Muy Alto) en las categorías, disponibilidad e integridad; en estado M (Apreciable) se hallan la categoría confidencialidad y en categoría B (Bajo) las categorías autenticidad, trazabilidad.
- ✓ [P] Técnicos en mantenimiento, caracterizados en estado crítico MA, (Muy Alto) en las categorías confidencialidad; en estado M (Apreciable) a autenticidad, trazabilidad; en estado A (Importante) se hallan las categorías integración, disponibilidad.
- ✓ [P} Personal, su resultado se halla en estado crítico MA, (Muy Alto) en las categorías disponibilidad e integridad; en estado M (Apreciable) confidencialidad; en estado B (Bajo) se hallan las categorías autenticidad, trazabilidad.

Se observa la afectación en niveles muy altos las diversas dimensiones, lo que deriva la afectación a la misma seguridad en la información que requiere la empresa para su misma operatividad; así como a su misma acreditación de los servicios que oferta. La acreditación de la empresa requiere altos niveles de seguridad en la información. Con estos resultados se puede deducir la urgente necesidad de atender a un plan de mejora pertinente con la situación que se describe en la actualidad.

Teniendo en cuenta los datos aportantes en la ejecución de la matriz MAGERIT, se puede observar en la imagen 5 esboza claramente la valoración cuantitativa de los activos, que se da en valores números, complementando el valor descriptivo que se ha ejecutado y que permite concretar con mayor efectividad el estado actual en cada uno de los activos al igual en las diversas dimensiones objeto de estudio en el proyecto y que caracteriza el valor que lo ubica en estados crítico, importante y apreciable.

Imagen 5. Valoración cuantitativa de los activos de la empresa REMGING S.A.S

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
[S] Servidor de impresión.	IMPORTANTE	15	15	25	25	15	19
[S]Servidor de archivos.	CRITICO	25	15	25	25	15	21
[SW] Pagina web	IMPORTANTE	25	15	9	15	15	16
[SW] WhatsUp Gold	IMPORTANTE	15	20	25	15	25	20
[SW] CISCO NETWORD ASIST	IMPORTANTE	15	20	15	25	25	20
[SW] Firewall Kerio Control	IMPORTANTE	15	15	15	25	15	17
[L] Torre el salitre 15M	APRECIABLE	9	9	25	9	25	15
[HW] SW Principal	IMPORTANTE	15	15	25	20	25	20
[HW] Routers	APRECIABLE	15	15	4	15	15	13
[L] Torre cerro norte 40M	IMPORTANTE	9	15	15	15	25	16
[S]SERVIDOR CONTABILIDAD	IMPORTANTE	15	15	25	20	25	20
[HW] COMPUTADOR PORTATIL HP	APRECIABLE	15	15	15	15	15	15
[HW] COMPUTADOR HP (VENTAS)	APRECIABLE	15	15	15	15	15	15
[HW] Servidor Principal	IMPORTANTE	15	15	25	20	25	20
[COM] puntos de acceso inalambricos	IMPORTANTE	9	9	20	25	25	18
[COM] puntos de acceso inalambricos	APRECIABLE	9	9	25	15	15	15
[COM] puntos de acceso inalambricos	IMPORTANTE	9	9	20	25	25	18
[P} Tecnicos en mantenimiento	IMPORTANTE	15	15	25	20	20	19
[P} Personal	IMPORTANTE	9	9	15	25	25	17

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Se puede apreciar como riesgo crítico el servidor de archivos, lo cual implica la exigencia de un tratamiento especial en un valor de 21 puntos. Le siguen con promedio de 20 puntos en el valor el servidor principal, el activo CISCO NETWOR ASIS, el WhatsApp Gold, el servidor de contabilidad, lo ubica en un riesgo importante que también requiere el análisis y gestión. En segundo orden están con puntajes de 16, 15 puntos las torres

del Salitre los computadores, portátil y el de ventas; asuntos que ameritan tener en cuenta para el mismo análisis que se viene ejecutando y las posibles intervenciones oportunas que conlleven a la minimización de los riesgos. Con 19 y 17 puntos respectivamente se halla el personal que labora en la empresa y los técnicos en riesgo calificado como importante. Es el personal un activo vital, y dentro de la empresa que ha de ser foco de atención, pues las dinámicas que se deriven para los sistemas de Seguridad de la Información requieren una mirada estricta al personal.

El mapa de calor representa gráficamente la ubicación de los riesgos dependiendo de la probabilidad que determinado riesgo pueda ocurrir, y el impacto cuantitativo o cualitativo que se produce en caso de que se materialice el riesgo. La adecuada estructuración de este mapa de riesgos que arroja la matriz MAGERIT, ayuda a mejorar el modelo de evaluación de los riesgos de la empresa y para esto se identifican detenidamente los riesgos inherentes y se analizan los eventos tanto externos como internos que están ocasionando dichos riesgos.

Los riesgos identificados se evalúan estimando la frecuencia con la que podrían aparecer y el impacto que puede tener a nivel financiero para la empresa. El mapa calor facilita así la toma de decisiones para la empresa porque refleja los riesgos más representantes en cada objetivo planteado en los procesos de planeación estratégica y al igual se pueden priorizar las acciones de acuerdo con la clasificación del mapa.

Este mapa, resulta aliado para el dueño y representante parte legal y a quienes hacen parte del equipo de trabajo, en cuanto que le va a permitir administrar adecuadamente los recursos, enfocando tiempo, dinero y personal en aquellos que puedan resultar más dañinos para el crecimiento a corto mediano y largo plazo. Por ello se da vital importancia a la difusión a todo el personal, mediante un diálogo que explica la manera como enfrentarse a un riesgo de alto impacto consecuencias de afectación a la misma empresa y de los usuarios.

El compromiso que pueden así asumir todos los miembros de la empresa va a permitir la reducción y minimización del impacto, al igual la funcionalidad de los Controles que se establecen redunda en beneficio tanto de la empresa, como de las personas que allí laboran. De igual manera el planteamiento de los controles oportunos en la empresa logra minimizar que el riesgo se materialice y de igual manera impactar negativamente en la operatividad y prestación de los servicios. La imagen 6 permite visibilizar el refuerzo de los riesgos de mayor amenaza. Se convirtió en un insumo importante presentado a la empresa para interpretar su situación de amenazas detectadas.

Imagen 6. Mapa de calor de la empresa REMGING S.A.S

		IMPACTO				
		Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
IMPACTO	**MUY ALTA**		R2	R16, R15, R11, R9, R7, R6, R5, R1	R14, R13, R12, R10, R8, R4	R3
	ALTA					
	MEDIA					
	BAJA					
	MUY BAJA					
RIESGO		**MUY BAJA**	**BAJA**	**MEDIA**	**ALTA**	**MUY ALTA**

Fuente: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Este mapa presenta el R3 como el de impacto catastrófico, le siguen con impacto son los riesgos, mayor R14, R13, R12, R10, R8, R4, Moderado R16, R15, R11, R9, R7, R6, R5, R1 y menor R2, es decir impacto moderado; lo que quiere decir que se han de dinamizar estrategias que busquen minimizar al máximo los riesgos en aras de mejorar los niveles de Seguridad en la empresa. Si bien la empresa viene manejando grandes desarrollos que le buscan al beneficio de las personas que requieren de los servicios que prestan, al igual el fortalecimiento en esta área es fundamental y quizás no haya ocupado un lugar especial dentro de la dinámica de operatividad de la empresa. Estos riesgos amenazan todas las dimensiones de seguridad establecidas. Si la empresa REMGING no establece un plan de tratamiento de manera oportuna, día a día se verificarán mayores afectaciones que hacen que el funcionamiento de la empresa se vea afectado en mayor escala.

6.3 EVALUAR CUALITATIVAMENTE LAS DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADAS EN LA EMPRESA, TENIENDO EN CUENTA EL ANÁLISIS ANTERIOR.

No se pueden identificar por simple observación, tanto los riesgos como las vulnerabilidades existentes en los activos hallados, y para ello se realiza transferencia de los marcos referenciales de la seguridad informática que responden al análisis y gestión de los riesgos, identificación de amenazas, existentes dentro de la organización, los cuales pueden generar impactos negativos en su funcionamiento, y a la vez afectan la seguridad de la información. Las vulnerabilidades en los activos pueden ser aprovechadas por personas inescrupulosas que buscan infiltrarse dentro de la información existente, con el ánimo de sustraerla, alterarla, o utilizarla con otros fines; se deriva una serie de posibles ataques en cada uno de los procesos ejecutados para el funcionamiento de esta. La empresa puede ser sometida a grandes pérdidas tanto económicas, como en su imagen corporativa dado que presenta soluciones tecnológicas a la medida y que los usuarios esperan un liderazgo en innovaciones en donde se sientan seguros con lo que están costeando. Atendiendo a los mismos propósitos generados en

el presente proyecto, como a la misma Misión y Visión empresarial, se acompaña el propósito de la garantía de la confiabilidad, confidencialidad y protección de la información internos como externos de la organización. Ver Tabla 10.

Tabla 10. Amenazas y vulnerabilidades de la empresa REMGING

Activos de Información	Nombre del activo de información	Amenazas Metodología MAGERIT	Vulnerabilidades
[S] SERVICIOS	[S] Servidor de impresión.	[E4] Errores de configuración	Muchas regalías en las cuentas de usuarios
[S] SERVICIOS	[S]Servidor de contabilidad	[A11] Acceso no autorizado	No tener Controlados los accesos.
[S] SERVICIOS	[S]Servidor de archivos.	[E15] Alteración accidental de la información	Ubicación lógica del servidor en el mismo segmento de otros elementos.
[SW] SOFTWARE	[SW] Página web	[E20] Vulnerabilidades de los programas (software)	Desarrollo del sitio web en una versión antigua.
[SW] SOFTWARE	[SW] WhatsUp Gold	[E14] Escapes de información	Fácil acceso de personal externo.
[SW] SOFTWARE	[SW] CISCO NETWORD ASIST	[I8] Fallo de servicios de comunicaciones	Un fallo podría desconectar toda una zona.
[SW] SOFTWARE	[SW] Firewall Kerio Control	[E4] Errores de configuración	Fallas en la autorización en las conexiones del firewall

FUENTE: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Tabla 10. (Continuación)

Activos de Información	Nombre del activo de información	Amenazas Metodología MAGERIT	Vulnerabilidades
[HW] EQUIPAMENTO INFORMÁTICO	[HW] SW Principal	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Permite conexión de equipos no autorizados. La amenaza de no actualización permanente facilita el acceso no controlado.
[L] INSTALACIONES	[L] Torre salitre 15 M	[I*] Desastres industriales	No hay Control de acceso ni equipos biométricos para identificación de personal, ni un registro del personal que accede.
[HW]	[HW] Routers	[E19] Fugas de información	Acceso a contraseñas y registro a personal externo.
[L] INSTALACIONES	[L] Torre cerro norte 40 M	[I*] Desastres industriales	La ubicación no cuenta con sistema de Control Biométricos que es una innovación pertinente de control de acceso y que reviste importancia.

FUENTE: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Tabla 10. (Continuación)

Activos de Información	Nombre del activo de información	Amenazas Metodología MAGERIT	Vulnerabilidades
[HW] EQUIPAMIENTO INFORMATICO	[HW] Computador portátil HP	[E20] Vulnerabilidades de los programas (software)	Versiones desactualizadas de software
[HW] EQUIPAMIENTO INFORMATICO	[HW] computador portátil HP (ventas)	[E20] Vulnerabilidades de los programas (software)	Versiones desactualizadas de software
[HW] EQUIPAMIENTO INFORMATICO	[E1] Servidor principal	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Permite conexión de equipos no autorizados
[COM] REDES DE COMUNICACIONES	[COM] puntos de acceso inalámbrico	[E4] Errores de configuración	Seguridad informática para no tener visibles las direcciones IP contra los ataques cibernautas.
[E1]	[E1] Personal	[E1] Errores de los usuarios	Falta de conocimiento.

FUENTE: Método MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

En el análisis de riesgos en los activos de información se pueden determinar asuntos importantes referidos a las amenazas según la metodología MAGERIT, y de igual forma sus vulnerabilidades. Se identificaron las posibles causalidades que las originan y que convierten esta situación en un riesgo importante para la empresa y su funcionamiento.

Estos hallazgos se pueden describir así:

- ✓ En los servicios, el servidor de archivos, se halla la gran amenaza de alteración accidental de la información, lo que lo genera la ubicación la lógica del servidor en el mismo segmento de otros elementos de la red.
- ✓ El servidor de contabilidad mantiene la amenaza de acceso no autorizado, falta de segmentación de la red, uso de VLAN y control de tráfico DMZ por parte de los usuarios, pues no se tienen Controlados los accesos de ubicación.
- ✓ El servidor de impresión presenta errores de configuración generado por la cantidad de regalías en cuentas de usuarios.
- ✓ En el software, se pude observar el activo página web, que presenta vulnerabilidades, ocasionados por el desarrollo del sitio web en una versión antigua.
- ✓ El WhatsUp Gold tiene escapes de la información, es de fácil acceso al personal externo de la misma empresa.
- ✓ El Cisco Network Active presenta fallos de servicios de Comunicaciones y se puede generar por un fallo en el servicio de acceso alámbrico que podría desconectar toda una zona al no haber redundancia.
- ✓ El firewall kerio Control, presenta errores de configuración, pues existen fallas en la autorización en las conexiones del firewall.
- ✓ El computador portátil y de venta, presentan vulnerabilidades de los programas, pues se tienen versiones desactualizadas del software.
- ✓ En las instalaciones, la torre cerro norte 40M involucra desastres industriales, en cuanto que su ubicación no cuenta con un sistema de Control ni monitoreo constante, no existe un Control de acceso ni equipos biométricos para la identificación del personal.
- ✓ Las redes de comunicaciones, en el activo perteneciente a los puntos de acceso inalámbrico, presentan errores de configuración, pues se requiere de seguridad informática para no tener visibles las direcciones IP contra los ataques cibernautas.
- ✓ Referido al personal, se tienen los técnicos de mantenimiento que constantemente presentan errores de usuarios, por falta de conocimiento en Sistemas de Seguridad

Informática y la ausencia de eventos de cualificación constante, atendiendo a las actualizaciones tecnológicas que se generan permanentemente y que han de ser apropiadas para un desempeño eficaz.

6.4 ESTRUCTURAR UN INFORME DE LOS RIESGOS QUE PERMITA ESTABLECER RECOMENDACIONES TENDIENTES A MEJORAR LA SEGURIDAD DE LA EMPRESA.

Esta fase involucra la dinámica de gestión, basada en el análisis de riesgos para conocer, prevenir, impedir, reducir o Controlar los riesgos identificados. Aquí se derivan una serie de acciones para satisfacer las necesidades detectadas por el análisis. Para esto se verifican los objetivos, las estrategias y las políticas de la empresa, ligado a las actividades de gestión de riesgos, desembocando en un plan de seguridad de manera que pueda dar cumplimiento a sus objetivos dentro del marco de la seguridad de la información.

La etapa de gestión de riesgos permite al representante legal y el personal de la empresa REMGING, el conocimiento más realista de la misma, especialmente en aquellas circunstancias que pueden afectar los procesos que se establecen de los servicios, o causar daños, perdidas, de modo que se puedan establecer prioridades y asignar requisitos de seguridad para enfrentar convenientemente estas situaciones. Los riesgos detectados cobran en especial importancia, porque pueden afectar a la empresa debido a la cantidad de activos que requieren una intervención. En la realización de este análisis de gestión del riesgo no se ejecuta de manera empírica; se identifican los marcos referenciales orientados a los sistemas de seguridad de la información, la metodología MAGERIT y al igual la verificación de las mejores estrategias para mitigar los impactos y buscar los Controles, salvaguardas oportunas. Para esto se exige un plan de seguridad y se organiza en actuaciones encaminadas para minimizar el impacto de los riesgos, la

empresa verifica la relación costo beneficio dado que la inversión en seguridad permite la continuidad sin amenazas que puedan afectar su misión.

Como el riesgo varía con el transcurso del tiempo y con las modificaciones de múltiples factores que definen dicho riesgo, esta gestión de riesgos también establece un seguimiento y la necesidad de un análisis continuo de su evolución, monitoreando los cambios surgidos y la contrastación con las situaciones iniciales, incluso después de los planes de mejora que se establecen.

El gerente y representante legal de la empresa, acepta los riesgos identificados y al igual las estrategias que deben ser asumidas; ya sea para su intervención inmediata o para la gradualidad en sus criterios y Controles para reducir los riesgos. Al aceptar objetivamente estos riesgos, se observa que satisfagan la política de la organización y cuya información se registra para ser tenida en cuenta por el personal y los técnicos de mantenimiento. Aquí pueden verificar las mejores medidas de seguridad y adoptar el plan de mejora de manera que se obtenga un nivel de seguridad para la empresa.

Una vez se concluye el trabajo del análisis de los riesgos, se pueden visibilizar los riesgos a que están expuestos los activos, lo que permite lograr una calificación atendiendo a la descripción del estado de éstos:

- ✓ Crítico en el caso de que requiere atención urgente.
- ✓ Importante en el caso de que requiere atención
- ✓ Apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento
- ✓ Bajo en el sentido de que no se van a tomar acciones para intervenirlo.

La matriz MAGERIT aloja datos, información que permite la toma de decisiones ya sea para protegerlos o para minimizar los impactos y los riesgos. Es de vital importancia el trabajo de conocer cuáles son los activos, cuáles poseen mayor nivel de riesgo, con el fin

de implementar estrategias para evitar que las amenazas se materialicen así pues hay activos que están en mayor riesgo:

- ✓ Como riesgo crítico se halla el activo, servidor de archivos. En este caso le urge a la empresa su atención.
- ✓ Como riesgo importante que deriva el requerimiento de atención, están los activos, la página Web, WhatsUP Gold, Cisco NEWORT ASIST, Firewall Kerio Control, SW principal, torre cerro norte de 40 metros, servidor de contabilidad, servidor principal, puntos de acceso inalámbrico 1 y 3. Técnicos de mantenimiento y personal.
- ✓ En riesgo apreciable se visualiza el ser objeto de estudio para su tratamiento, los activos, torre salitre de 15 metros, routers, computador portátil HP, computador HP ventas y el punto de acceso inalámbrico 2.

Una vez se visualizan los riesgos se busca la manera de trazar el plan de tratamiento de estos. Se toma la norma ISO/IEC 27001, ya que está direccionado los Controles a seguir de acuerdo con los riesgos hallados, y las medidas de seguridad de prevención para evitar daños futuros.

En la guía de buenas prácticas que ofrece sobre los Controles a implantar se direcciona a la selección de los Controles, los cuales son medidas que están orientadas a mitigar los riesgos que se hallan al ejecutar el ejercicio de la metodología MAGERIT, los cuales abarcan Controles técnicos a través de diversos procedimientos y organizativos, que han de documentarse en las mismas políticas de la empresa.

Al seleccionar la implantación de los Controles, se socializa con la persona encargada de la seguridad de la empresa y los técnicos los cuales participan activamente en los procesos de concientización y posterior implementación observando la aceptación y apropiación de los hallazgos. Se desarrollan reuniones con el personal existente en la

organización, para comunicar los resultados y a la vez socializar los Controles que se van a implementar producto del plan de tratamiento para cada uno de los riesgos.

El plan de Controles se trabaja para el establecimiento de directrices de actuación permanente, pues se exige la implantación de estos y el tratamiento de los riesgos, que permite organizar la defensa oportuna para que no se llegue a mayores impactos negativos.

En sentido de los esbozado anteriormente se atajan las emergencias y se sobrevive a incidentes para seguir, operando con mejores condiciones dentro y fuera de la organización. En el tratamiento de los riesgos se exige a mediano plazo, una planificación de las acciones que van a llevar a cabo para implementar los Controles, los que se plantean desde la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001. Corresponde al dueño de la empresa y representante legal detallar las fases, los recursos disponibles a utilizar, las diversas etapas y acciones y plazos para ejecución.

Los controles y objetivos se han seleccionado atendiendo a las necesidades prioritarias de la empresa en las condiciones actuales de la empresa, donde se logra plasmar la pertenecía del mismo y su utilidad. Se inicia atendiendo a la necesidad de la implementación de la política de seguridad orientada a la empresa, la cual sirve de soporte a la dirección de ésta con respecto a la seguridad de la información de acuerdo con las necesidades halladas y si corresponsabilidad con los reglamentos y leyes existentes.

En la Tabla 11. se presentan a la empresa tanto los objetivos como los controles pertinentes con los riesgos y amenazas detectadas. La empresa ha de contemplar esta propuesta para ser incorporada en los planes operativos, que se trazan para dinamizar un compromiso con la seguridad informática, y de la misma forma evitar que las amenazas se materialicen.

Tabla11. Objetivos y controles

PROCESO	OBJETIVOS	CONTROLES
A.5 POLÍTICA DE SEGURIDAD	Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.	Ha de existir un documento de política de seguridad de la información, el cual ha de estar visible y de pleno conocimiento por parte de todos los empleados y partes externas pertinentes y se socializado al personal que labora en la misma. La política de seguridad implementada en la empresa, necesita de la revisión periódica y ha de estar actualizándose, atendiendo a la necesidad del ser eficaz, mediante cronograma fijado con antelación, pues los constantes cambios en la información así lo requieren.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Gestionar la seguridad de la información dentro de la organización.	Corresponde al gerente y director de la empresa, el compromiso con la seguridad de la información que se gesta en la misma, de donde se deriva la asignación de responsabilidades claras, precisas y concisas, y la selección de la persona que las ha de asumir, ejecutando monitoreo permanente de las mismas.
A.7 GESTIÓN DE ACTIVOS	Lograr y mantener la protección adecuada de los activos organizacionales.	La empresa ha de tener actualizado el inventario de los activos existentes, identificando tanto su ubicación, como los responsables de estos, realizando entrega individual a los mismos. Se han de establecer las formas y reglas de uso de la información y su debido procesamiento, de acuerdo con cada uno de los activos, atendiendo a la necesidad de protección de la misma y garantía de seguridad.

Fuente: Norma ISO/IEC 27001.

Tabla 11. (continuación)

PROCESO	OBJETIVOS	CONTROLES
A.8 SEGURIDAD DE LOS RECURSOS HUMANOS	Asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal.	Los recursos humanos de la empresa, así como los usuarios de terceras partes, deben apropiar y entender lo contemplado en la política de seguridad, conociendo plenamente sus compromisos y responsabilidades asumidas. Tanto los empleados, han de leer los términos y condiciones de su trabajo en relación con la seguridad de la información, en el que han de aparecer las, funciones, responsabilidades que se asumen y aceptarlos. . Es compromiso de la dirección, el monitoreo constante a empleados, contratistas y usuarios de terceras partes, sobre la aplicación de las políticas de seguridad, atendiendo a los servicios que se prestan. La cualificación, capacitación pertinente sobre las políticas de seguridad de la información, junto a las constantes innovaciones y actualizaciones que se ejecutan, es responsabilidad del gerente de la empresa, al igual que la asignación de presupuesto y tiempo para su ejecución. Todo empleado y contratista ha de contar con las debidas certificaciones que la empresa expide ante procesos de cualificación y capacitación. Estas han de responder a las fases de avance y eventos que se generen de manera que se hallen actualizadas y evidencien el avance que se ejecuta atendiendo al plan que direcciona la misma.

Fuente: Norma ISO/IEC 27001.

Tabla 11. (Continuación)

PROCESO	OBJETIVOS	CONTROLES
A.9 SEGURIDAD FÍSICA Y DEL ENTORNO	Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización	Las áreas donde se hallan los activos de la empresa que contienen información, han de estar debidamente protegidas mediante diversas barreras, en las que se han de incluir puertas de acceso controladas con tarjeta. o diversas claves que logren limitar accesos no autorizados Se han de implementar controles de accesos con exclusividad a personal que la empresa considere se debe autorizar. Se han de cambiar las claves de estos controles una vez la persona se desvincule laboralmente. Las innovaciones que surgen en la actualidad de monitoreo mediante cámaras han de ser implementadas en las diversas áreas donde existen activos, y que puedan evidenciar los accesos en tiempos reales La empresa ha de tener el plan de protección ante daños ambientales y contar con las protecciones físicas contra los posibles daños que se pueden originar ante desastres naturales o artificiales. Deben existir las pólizas de seguro actualizadas y con especificaciones ante cada evento. Debe existir un plan de actualización y mantenimiento del equipamiento y el mantenerse a la vanguardia de las nuevas tendencias que van apareciendo, obedeciendo a los avances de la tecnología y el nivel de amenazas que surgen por parte de ciberdelincuentes.

Fuente: Norma ISO/IEC 27001.

Tabla 11. (Continuación)

PROCESO	OBJETIVOS	CONTROLES
	Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.	Las terceras partes ligadas a los servicios de la empresa, han de conocer las políticas de seguridad de la información, e implementarlas en las operaciones que se ejecutan en el marco de los servicios que presta la misma, al igual que las responsabilidades. Ha de ejecutarse un monitoreo y control periódico.
	Minimizar el riesgo de fallas de los sistemas.	Se han de desarrollar acciones que busquen minimizar los riesgos que se puedan presentar en los activos de la empresa, mediante auditorias previas, monitoreo constante, evaluación de estos.
	Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte	Ha de existir un plan de reevaluación de los riesgos para reorientar los mecanismos de intervención y actualizar las políticas existentes de seguridad, direccionando controles pertinentes a los inconvenientes y hallazgos que se puedan generar en los activos de la empresa, asegurando así la protección de la información. Ha de existir una política de respaldo de la información dentro de la política de seguridad, mediante copias de respaldo de la información y del software, validando constantemente su eficacia, y seguridad. Las copias de seguridad han de estar protegidas ante intrusos o personas inescrupulosas que puedan acceder a la información, utilizando la innovación en su implementación.

Fuente: Norma ISO/IEC 27001.

Tabla 11. (Continuación)

A.11 CONTROL DE ACCESO	Objetivo: Controlar el acceso a la información.	Se han de establecer las rutas y procedimientos formales ante el registro y cancelación de usuarios, de manera que mantengan los controles de acceso a los sistemas y servicios. Se ha de denegar oportunamente el acceso y privilegios, una vez se finalicen los contratos laborales y cese la actividad de vinculación al trabajo por parte del personal. Se debe implementar el mecanismo de identificación automática de los equipos, logrando identificar en tiempo real las conexiones que se generan en los equipos y ubicaciones específicas.

Fuente: Norma ISO/IEC 27001.

7. CONCLUSIONES

- ✓ Con la realización del proyecto, se logró realizar un análisis de riesgos mediante la metodología MAGERIT sobre los activos existentes en la empresa REMGING como mecanismo de mejora de los niveles de seguridad informática, que permite gestionar éstos visualizando de una manera clara a los daños a los que está expuesta la empresa según los grados de afectación.

- ✓ En la identificación de los riesgos, se destaca como crítico el servidor de archivos. Como riesgo importante que deriva el requerimiento de atención, están, la página Web, WhatsUP Gold, Cisco NEWORT ASIST, Firewall Kerio Control, SW principal, torre cerro norte de 40 metros, servidor de contabilidad, servidor principal, puntos de acceso inalámbrico 1 y 3. Técnicos de mantenimiento y personal.

- ✓ Al Analizar el riesgo asociado a cada uno de los activos de la empresa, a partir de la probabilidad que la amenaza se materialice, se detectan amenazas en los servicios, el software, equipos, instalaciones, y personal; lo que coloca en peligro de que estos se materialicen por alteración accidental de la información, fallas en la segmentación de la red y tráfico por parte de los usuarios, escapes de información, desconexión de zonas, afectaciones por accesos no autorizados.

- ✓ Para estructurar un informe de los riesgos que permita establecer recomendaciones tendientes a mejorar la seguridad de la empresa, se presenta al gerente los resultados de la evaluación cualitativa y cuantitativa de los activos, sus riesgos, amenazas, y los objetivos y controles que requiere en la medida que se busque garantizar seguridad de la Información y en la prestación de servicios.

- ✓ La empresa ha de implementar procesos que involucren políticas de seguridad, organizar la seguridad de la información, seguridad en los recursos humanos, gestión de activos, seguridad física del entorno, en la medida en que se halla en contante amenaza y puede ejecutar controles permanentes buscando superar las dificultades halladas.

8. RECOMENDACIONES

Para el mejoramiento de la seguridad informática en la empresa REMGING, ante todo, debe existir el equipo humano responsable del manejo de la seguridad de la información dentro de la misma. El equipo debe tener su manual de funciones con todas las tareas asignadas dentro de un plan de respuesta a incidentes definido, atendiendo a los activos existentes dentro de la misma organización.

El equipo humano de la empresa REMGING ha de estar familiarizado con la respuesta ante los incidentes de seguridad. Ha de existir la política general de gestión de incidentes diseñada para la empresa. La política de seguridad enmarca los procedimientos a seguir en la asertiva gestión de estos, las relaciones entre el equipo, la respuesta de incidentes y otros recursos humanos internos y externos, el diseño de las guías y protocolos donde están todos los procedimientos a seguir ante la ocurrencia de un incidente, el diseño del manual de funciones para el equipo que es el responsable del manejo de los incidentes de la seguridad.

Los resultados de este análisis de riesgos a la empresa REMGING, debe ser conocido por el personal que está a cargo de la seguridad informática y de los activos que se encuentran en la misma, de manera que de aquí surgen todas las políticas y los planes de gestión de los incidentes de seguridad informática, atendiendo a la posibilidad de ocurrencia de estos.

Es importante tener en cuenta el análisis de riesgos periódicos, mediante el establecimiento de auditorías, como la implementación de un sistema de seguridad en la red, e incrementar en todo lo posible la seguridad en los equipos y las diversas maneras de detección de vulnerabilidades, e identificar la importancia de los sistemas de información.

Es de reconocer la concientización de quién esté al frente de la empresa, sobre las ventajas de establecer políticas de seguridad. Para eso es necesario la asignación tanto de recursos humanos, cómo de recursos financieros que se orienten a la prevención detección y corrección de incidentes que afectan la seguridad de la información.

La empresa ha de tener en cuenta en la identificación de todos los incidentes que se han presentado al interior de esta, y los fallos ocurridos en los activos existentes. De igual forma el conocimiento de las políticas de seguridad que se llevan en el momento y que se vienen implementando, para a partir de aquí establecer el plan de gestión coherente y pertinente con las necesidades empresariales.

9. BIBLIOGRAFÍA

AGUILERA L, Purificación. Seguridad informática. Protocolos de políticas de seguridad informática. Colombia, Universidad Católica, 2005. Disponible en internet: https.//docplayer.es/5605322_protocolos:de: políticas_de_seguridad_informática_Para_Las_universidades_de_Risaralda_Jorge_Luis_villa. HTML.

AGUIRRE CARDONA, Juan David y ARISTIZABAL BETANCOURT, Catalina. Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda. Tesis de Grado: Universidad Tecnológica de Pereira. Facultad de Ingenierías, 2012.

B. Smith, Thinking about Security Monitoring and Event Correlation. bsmith@lurhq.com, 2000.
[34] Welcome to the Intrusion Detection Systems Product Survey (http://www.c3.lanl.gov/~reid/kaj/).

BOISSEAU, M., DEMANGE, M. y MUNIER, J. High Speed Networks. 1995. Recuperado de: https://onlinelibrary.wiley.com/doi/pdf/10.1002/0470841885.fmatter_indsub

BOLIVAR Yeinny, Diseño de un sistema de gestión de seguridad de la información en la intranet del Policlínico del sur Olaya Bogotá, Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2016.

BLOG ESPECIALIZADO EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. ISO/IEC 27001: ¿Qué significa la Seguridad de la Información? [En línea]. Bogotá D.C.: Blog especializado. 2015. (Recuperado en septiembre 2017.)

Disponible en http://www.pmg-ssi.com/2015/05/ISO/IEC -27001-que-significa-la-seguridad-de-la-informacion/

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria de 2012. (17 octubre). Por la cual se dictan disposiciones generales para la protección de datos personales. [en línea]. Bogotá D.C.: Alcaldía de Bogotá. 2012. [Consultado el 23 de mayo, 2015]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

CISTOPHER MALDONADO, Reyes y otros. Propuesta de un sistema de información integrada para la empresa REMGING S.A.S. Universidad politécnica de Madrid. 2020

CORDERO MORENO, José Leonardo y GARCIA REYES, Yadimir Oswaldo. Análisis de riesgo y recomendaciones de seguridad de información del hospital E.S.E San Bartolomé de Capitanejo, Santander. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2016, 84p.

CORDOBA R., N. Evaluación de riesgos, Amenazas y Vulnerabilidades. (2012) Recuperado de http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova_RN/Cap5.PDF, Erb, M. 2009. Amenazas y vulnerabilidades.

CHICANO Tejada, E. Auditoría de seguridad informática (MF0487_3). 2015. IC Editorial. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/44136

CHIRILLO, J. Hack Attacs Denied. EEUU. 2001. Recuperado de: https://www.wiley.com/en-us/Hack+Attacks+Denied%3A+A+Complete+Guide+to+Network+Lockdown-p-9780471190516

CHURCHILL, B. y JORDAN, L. Communications and Networking for the PC. EEUU: NRP. 1994 recuperado de: https://crd.lbl.gov/divisions/scidata/dst-publications-2/?sort=type

ERNST & YOUNG, Moving beyond compliance: Ernst & Young's 2008 Global Information Security Survey. En: eycom.ch [en línea]. [consultado 10 abr. 2009]. Disponible en: http://www2.eycom.ch/publications/items/giss_2008/2008_EY_GISS.pdf

GOMEZ Fernández, L. y Fernández Rivero, P. P. Cómo implantar un SGSI según UNE-EN ISO/IEC /IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. AENOR - Asociación Española de Normalización y Certificación. 2018. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624

FERNÁNDEZ Sánchez, C. M. Modelo para el gobierno de las TIC basado en las normas ISO/IEC. AENOR - Asociación Española de Normalización y Certificación. 2012. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53581

INCIBE. Guía glosario de seguridad. Instituto Nacional de Ciberseguridad. Tomado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf.

INCIBE. (2017). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. 2018. Instituto Nacional de Ciberseguridad Recuperado de https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements. 2005.

KAZEMI, Mehdi; KHAJOUEI, Hamid; NASRABADI, Hashem. “Evaluation of information security management system success factors: Case study of Municipal organization”. 2012. Vol. 6, http://www.academicjournals.org/ajbm/pdf/pdf2012/11April/Kazemi%20et%20al.pdf

KOSUTIC, Dejan. ISO 27001 gap analysis vs. risk assessment. [Online]. Publicado Enero 27 de 2014. https://advisera.com/27001academy/knowledgebase/iso-27001- gap-analysis-vs-risk-assessment/

LUCERO Antonio y LAVERDE John, Análisis y gestión de riesgos de los sistemas de la Cooperativa de crédito y de ahorro Jardín Azuayo, Tesis de grado Especialización en seguridad informática; UNAD, Escuela de Ciencias Básicas Tecnología e Ingeniería, 2012.

LOPEZ; Francisco, AMUTIO Miguel. Metodología y análisis de gestión de riesgos de los sistemas de información: Ministerio de administraciones públicas. 2006

MÉTODO MAGERIT, Tomado de: Portal de Administración Electrónica. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. 2012. Recuperado de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad de la Información
para la Estrategia de Gobierno en Línea 2.0. [En línea]. Versión 2.0.2. 49p.Bogotá, 2011. Disponible en Internet:
(css.mintic.gov.co/ap/gel4/images/Modelo_Seguridad_Informacion_2_01.pdf)

Ministerio de hacienda y administraciones públicas. MAGERIT versión 3.0 (octubre del 2012). Metodología de análisis y gestión de riesgos de los sistemas información. Gobierno de España.

MORGAN, Steve. Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. 2019 [En línea] Disponible en https://cybersecurityventures.com/jobs/ 47 WORLD ECONOMIC

Norma ISO/IEC 20071, tomado de: Introducción y comprensión a los sistemas de gestión de seguridad de la información SGSI (ISO/IEC /IEC 27001-27002), Gómez, L. & Álvarez, A. 2012. Guía de aplicación de la Norma UNE-ISO/IEC /IEC 27001 sobre seguridad en sistemas de información para pymes. Recuperado de: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53580?page=13

ORTIZ MANRIQUE; Edwin Omar, Análisis de causas de riesgos en la protección de la información de la empresa Soltec-ing y recomendaciones de seguridad. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2016.

QUINTERO Yamile, Análisis y gestión de riesgos de los sistemas de información de la alcaldía municipal de Tuluá. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2015.

Rouse, M. Search Security. 2012. Obtenido de http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

S. Bugiel, S. Heuser, and A.-R. Sadeghi, “Towards a Framework for Android Security Modules : Extending SE Android Type Enforcement to Android Middleware.” Intel Collaborative Research Institute for Secure Computing, 2012.

Security Enhancements in Jelly Bean | Android Developers Blog.” [Online]. Available: http://android-developers.blogspot.com/2013/02/security-enhancements-in-jellybean.html. [Accessed: 19-Mar-2013].

Sitio web, “GlobalSUITE compañía Audisec”: https://www.globalsuite.es/es/information-security-iso-27001/

WORLD ECONOMIC FORUM. This is what the future of cybersecurity will look like. 2017. [En línea] Disponible en https://www.weforum.org/agenda/2017/08/the-us-is-upping-its-game-againstcyber-attacks-but-the-security-industry-faces-a-huge-challenge

ANEXOS

Anexo 1. Autorización para ejecución del proyecto.

V0.1

Bogotá, 2 de noviembre de 2020

Señor:
Román Emilio Máguez Garcés
Gerente REMGING

Asunto: Autorización para la ejecución del proyecto titulado: **ANALISIS DEL NIVEL RIESGO DE LOS ACTIVOS INFORMÁTICOS PARA DETERMINAR EL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA REMGING.**

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a REMGING, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: **ANALISIS DEL NIVEL RIESGO DE LOS ACTIVOS INFORMÁTICOS PARA DETERMINAR EL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA** REMGING el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: "Realizar el análisis del nivel riesgo de los activos informáticos para determinar el estado actual de la seguridad informática en la empresa REMGING", al mismo tiempo será apoyado por los objetivos específicos: Descubrir las vulnerabilidades, amenazas y riesgos de seguridad del área informática en cada uno de los activos informáticos. Calcular el riesgo para cada activo a partir de la probabilidad que la amenaza se materialice., Verificar cualitativamente las dimensiones de la seguridad de la información implementadas en la empresa. Determinar el sistema de control interno informático coherente con los resultados del análisis de riesgos de le empresa para obtener como resultado un alto impacto en la seguridad de la empresa REMGING.

V0.1

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por REMGING.
- La empresa REMGING deberá establecer que tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de prubas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El dcumento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrerar profesional.

Firman en Bogotá D.C., a los 2 días del mes de noviembre de 2020

Cordialmente,

Javier Felipe Márquez Pérez
Estudiante UNAD

Román Emilio Márquez Garcés
Gerente REMGING

Anexo 2. Acuerdo de confidencialidad

Remging

ACUERDO DE CONFIDENCIALIDAD ENTRE JAVIER FELIPE MARQUEZ PEREZ Y REMGING

Por la **parte reveladora**
Nombre: REMGING
Dirección: Carrera 53 No 138-69 Bogotá
Teléfono: 5233022
E-mail: info@remgingenieria.com

Por la parte **receptora de la información**
Nombre: Javier Felipe Márquez Pérez
Dirección: Carrera 74 No 48A-32
Teléfono: 3007743142
E-mail: javierfelipemarquezp@gmail.com

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la REMGING, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto *aplicado con el título:* **Análisis del nivel riesgo de los activos informáticos para determinar el estado actual de la seguridad informática en la empresa** REMGING

2. Que la información de propiedad de REMGING ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación **Análisis del nivel riesgo de los activos informáticos para determinar el estado actual de la seguridad informática en la empresa** REMGING, **Javier Felipe Márquez Pérez** que para el

Dirección: Carrera 53 # 138-69 of 2. PBX: 4924720. Web: www.remging.com. Email: info@remging.com
Bogotá - Colombia

Remging

presente caso actual como **revelador, guarda y administrados** de la información de propiedad de REMGING.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad**, la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente a REMGING, así como también a no utilizar dicha información en beneficio propio ni de terceros, sólo con fines estadísticos y de mejoramiento de la empresa.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,

3. modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto **Análisis del nivel riesgo de los activos informáticos para determinar el estado actual de la seguridad informática en la empresa** REMGING lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o

intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legítima poseedora de la misma REMGING, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de REMGING.

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: Caracterización de la empresa, estado de arte de la seguridad informática, activos, amenazas, vulnerabilidades, riesgos, salvaguardas, controles aplicados, plan de auditoria.

10. La información capturada por la **parte receptora** se observará como *información cualitativa y comparativa*, no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad todo el personal ***REMGING*** no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de REMGING, ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante *Javier Felpe Márquez Pérez* se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa REMGING para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el repositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la empresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes Javier Felipe Márquez Pérez–*REMGING)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las cláusulas del presente acuerdo de confidencialidad por parte de Javier Felipe Márquez Pérez.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los 2 días del mes de noviembre de 2020

Como Parte Receptora:

Javier Felipe Márquez Pérez
Estudiante UNAD.
C.C. No.109695928 de Málaga

Por la parte reveladora:

Román Emilio Márquez Garcés
Gerente REMGING
C.C No.13927922 de Bogotá