UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS

MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES COHORTE 2021

Tema: PROCEDIMIENTO DE GESTIÓN DE RIESGOS DEL ÁREA INFORMÁTICA DE LA EPM-GIDSA MEDIANTE LA APLICACIÓN DE NORMAS INTERNACIONALES.

Trabajo de Titulación, previo a la obtención del Grado Académico de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones

Modalidad del Trabajo de Titulación: Proyecto de Titulación con Componente de Investigación Aplicada

Autora: Ingeniera Jessica Maricela Guevara Toalombo

Director: Ingeniero Héctor Fernando Gómez Alvarado PhD

Ambato – Ecuador

Año 2022

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por el Ingeniero Héctor Fernando Gómez Alvarado PhD, e integrado por los señores: Ingeniero Carlos Vinicio Mejía Vayas Magister, Ingeniero Fabian Rodrigo Morales Fiallos Magister, designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: "PROCEDIMIENTO DE GESTIÓN DE RIESGOS DEL ÁREA INFORMÁTICA DE LA EPM-GIDSA MEDIANTE LA APLICACIÓN DE NORMAS INTERNACIONALES" elaborado y presentado por la señora Ingeniera Jessica Maricela Guevara Toalombo, para optar por el Grado Académico de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Héctor Fernando Gómez Alvarado. PhD.
Presidente y Miembro del Tribunal

Ing. Carlos Vinicio Mejía Vayas Mg.
Miembro del Tribunal

Ing. Fabian Rodrigo Morales Fiallos Mg.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Procedimiento de gestión de riesgos del área informática de la EPM-GIDSA mediante la aplicación de normas internacionales, le corresponde exclusivamente a: Ingeniera Jessica Maricela Guevara Toalombo Autora, bajo la Dirección de Ingeniero, Héctor Fernando Gómez Alvarado PhD, Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniera Jessica Maricela Guevara Toalombo
c.c.: 1803543709
AUTORA

Ingeniero Héctor Fernando Gómez Alvarado, Phd
c.c.:1103474589
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniera Jessica Maricela Guevara Toalombo

c.c.: 1803543709

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

A la Universidad Técnica de Ambato y su excelente planta de docentes quienes con su conocimiento y experiencia plasmaron el deseo de aprender, investigar y aportar al mundo laboral.

A mi director de tesis por guiarme en esta investigación, permitiéndome desarrollar profesionalmente y seguir cultivando mis valores.

A mis compañeros maestrantes (Juan Mecánico) quien con su apoyo a pesar de la distancia geográfica se convirtieron en soporte incondicional en el transcurso de este estudio, considerándolos ahora como mis amigos.

De manera especial a la Empresa Pública Municipal para la Gestión Integral de los Desechos Sólidos del Cantón Ambato por abrirme sus puertas y permitir aportar con un grano de arena en el cumplimiento de sus objetivos institucionales.

DEDICATORIA

Este trabajo está dedicado a mi madre quien antepuso sus necesidades a la de sus hijos, apoyando a todas las decisiones y sacrificios que realizamos con el único fin de vernos feliz.

A mi esposo David quien con su paciencia y apoyo al cuidado de nuestro hijo Benjamín me permitió cumplir una meta profesional más.

A mi padre, hermanos y suegros, quienes con palabras y acciones pudieron darme fuerzas para cumplir este sueño profesional.

UNIVERSIDAD TECNICA DE AMBATO
CENTRO DE POSGRADOS

MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

TEMA:

PROCEDIMIENTO DE GESTIÓN DE RIESGOS DEL ÁREA INFORMÁTICA DE LA EPM-GIDSA MEDIANTE LA APLICACIÓN DE NORMAS INTERNACIONALES

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con Componente de Investigación Aplicada.*

AUTORA: *Ingeniera Jessica Maricela Guevara Toalombo*

DIRECTOR: *Ingeniero Héctor Fernando Gómez Alvarado PhD.*

FECHA: *Veinte y tres de agosto de dos mil veinte y dos*

RESUMEN EJECUTIVO

La era tecnológica ha permitido a las empresas automatizar los procesos repetitivos y agilitar los servicios brindados a sus usuarios, al mismo tiempo las Tecnologías de Información y Comunicación están siendo blancos fáciles contra amenazas múltiples, permitiendo la materialización de riesgos y/o perdidas parciales o totales de activos importantísimos para cualquier empresa (Castro-Maldonado & Villar-Vega, 2021)

Por lo que el propósito de este trabajo es desarrollar un procedimiento para la gestión de riesgos del área informática de la Empresa Pública Municipal para la Gestión Integral de los Desechos Sólidos del cantón Ambato aplicando normas internacionales para lo cual se revisara el fundamento teórico actual de la gestión de riesgos del área informática de la Empresa Pública Municipal para la Gestión Integral de los Desechos Sólidos del cantón Ambato, se identificara la metodología adecuada de gestión de riesgos, una vez analizada las buenas prácticas de las normas internacionales y finalmente se elaborara el procedimiento para la gestión de riesgos del área informática

de la Empresa Pública Municipal para la Gestión Integral de los Desechos Sólidos del cantón Ambato.

Mediante la observación de campo a la gestión de riesgos del área informática de la Empresa Pública Municipal para la Gestión Integral de los Desechos Sólidos del cantón Ambato y tras la aplicación de la norma internacional ISO 31000 y metodología MAGERIT, se evidencio una disminución del valor del riesgo de Ataques Intencionados de 285 a 255, los Fallos y errores no intencionados de 452.70 a 351.30 y los riesgos de Origen Industrial de 203,55 a 146,55.

Confirmando de esta manera la hipótesis de investigación de que la aplicación de la normativa internacional ISO 31000 y la metodología MAGERIT V3 redujo los valores de riesgo total de 960,75 a 772,35; además considerando que el activo principal en toda empresa es el Humano debido a la actividad directa con la información, esta investigación enfatizo la aplicación de controles hacia los riesgos de tipo Fallos y errores no intencionados producto de las acciones directas hacia la información de la empresa.

DESCRIPTORES: *ACTIVOS, COBIT, CONTROLES, GESTIÓN, INFORMÁTICA, ISO 31000, MAGERIT, PROCESO, RIESGOS, SEGURIDAD*

UNIVERSIDAD TECNICA DE AMBATO
CENTRO DE POSGRADOS

MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

THEME:

RISK MANAGEMENT PROCEDURE FOR EPM-GIDSA INFORMATION TECHNOLOGY AREA THROUGH THE APPLICATION OF INTERNATIONAL STANDARDS

DEGREE MODALITY: *Degree Project with Applied Research Component.*
AUTHOR: *Engineer Jessica Maricela Guevara Toalombo*
DIRECTED BY: *Engineer Héctor Fernando Gómez Alvarado, PhD*
DATE: *August twenty-third, two thousand and twenty-two*

EXECUTIVE SUMMARY

The technological era has allowed companies to automate repetitive processes and streamline the services provided to its users, at the same time the Information and Communication Technologies are becoming easy targets against multiple threats, allowing the materialization of risks and/or partial or total loss of very important assets for any company (Castro-Maldonado & Villar-Vega, 2021).

Therefore, the purpose of this work is to develop a risk management procedure for the IT area of the Municipal Public Company for the Integral Management of Solid Waste of the Ambato canton, applying international standards, for which the current theoretical basis of risk management of the IT area of the Municipal Public Company for the Integral Management of Solid Waste of the Ambato canton will be reviewed, the adequate risk management methodology will be identified, once the good practices of international standards have been analyzed, and finally the procedure for risk management of the IT area of the Municipal Public Company for the Integral Management of Solid Waste of the Ambato canton will be elaborated.

Through the field observation of the risk management of the IT area of the Municipal Public Company for the Integral Management of Solid Waste of the Ambato canton and after the application of the international standard ISO 31000 and MAGERIT methodology, a decrease in the value of the risk of Intentional Attacks from 285 to 255, the Failures and unintentional errors from 452.70 to 351.30 and the risks of Industrial Origin from 203.55 to 146.55 was evidenced.

Thus confirming the research hypothesis that the application of the international standard ISO 31000 and the MAGERIT V3 methodology reduced the total risk values from 960.75 to 772.35; also considering that the main asset in any company is the Human due to the direct activity with the information, this research emphasized the application of controls towards the risks of type Failures and unintentional errors resulting from the direct actions towards the company's information.

KEYWORDS: *ASSETS, COBIT, CONTROLS, INFORMÁTICA, ISO 31000, MAGERIT, MANAGEMENT, PROCESS, RISKS, SECURITY*

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1 Introducción

La inclusión de las tecnologías de la información en las organizaciones se ha convertido para muchas empresas en blancos constantes de ataques, entre estos el daño a su reputación, el delito cibernético, el riesgo político y el terrorismo por mencionar algunos de los riesgos que las organizaciones públicas y privadas de todo tipo y tamaño en el mundo deben afrontar cada vez con mayor frecuencia, por lo que según Andrade Talero, activos como servicios, hardware y equipos auxiliares son los riesgos que más afectan en una empresa por encontrarse directamente relacionados al servicio de internet, debido a la deficiente seguridad y salvaguardas o controles ejecutados. (Andrade Talero, 2021)

Sin embargo para el autor Ávila Torres, el activo más importante es el ser humano, debido a que las acciones realizadas por los empleados encargados de administrar la información afectaría gravemente al desempeño de actividades de una empresa (Avila Torres, 2021)

Por lo que la gestión de riesgos hace frente a las posibles amenazas que una organización puede tener, impidiendo que estos se materialicen en riesgos potenciales, logrando así en gran medida frenar pérdidas cuantiosas para la organización, por lo que partiendo de que la Empresa Pública Municipal para la Gestión Integral de los Desechos Sólidos del Cantón Ambato nombrada de aquí en adelante por sus siglas como EPM-GIDSA lleva a cabo prácticas para la Gestión de Riesgos únicamente en áreas que por ley los órganos de control lo exigen, sin embargo no cuenta con un procedimiento definido de Gestión de Riesgos para toda la organización, razón por la cual nace el tema de desarrollar el "Procedimiento de gestión de riesgos del área informática de la EPM-GIDSA mediante la aplicación de normas internacionales", encontrándose el presente trabajo distribuido en 5 capítulos: en el primero se aborda la problemática; el segundo corresponde a los antecedentes investigativos que sustentaron la investigación; en el tercero se detalla el marco metodológico; el cuarto capítulo contiene la discusión y los resultados de la investigación y finalmente, en el

quinto capítulo se expresan las conclusiones y recomendaciones a las que se ha llegado con el análisis realizado.

1.2 Justificación

A nivel internacional factores como la crisis crediticia de 2008, el terrorismo, el huracán Katrina, los piratas informáticos y los desastres de los viajes aéreos evidencian que los métodos utilizados para evaluar y gestionar riesgos informáticos son fundamentalmente defectuosos, por lo que ha sido necesario explorar por qué falla la gestión de riesgos, ya sea por la falta de medición y validación de métodos en su totalidad o en parte; el uso de componentes que se sabe que no funcionan; y no utilizar componentes que se sabe que funcionan (Hubbard, 2020) ha ocasionado la pérdida de información en muchas organizaciones.

En Ecuador desastres naturales como terremoto evidencio la falta de gestión de riesgos en las empresas, debido al desconocimiento del proceso, la falta de presupuesto y la complejidad que presentan las normas ISO. Probablemente los activos físicos fueron afectados, pero en sí la información pudo haberse recuperado si se hubiese contado con un adecuado plan de contingencia y procedimientos claros para la gestión de riesgos, tomándose un tiempo considerable para retomar sus operaciones (Escobar Sánchez & others, 2022).

En este contexto y con la visión de salvaguardar cualquier pérdida de información la Contraloría General del Estado mediante el examen especial a los procesos administrativos, financieros, de mantenimiento, de operación y correlativos de la EPM-GIDSA determina que en el proceso Sistemas (Clavijo Mera, 2015) no mantiene una adecuada Gestión de Riesgos debido a falta de políticas aprobadas exponiéndola a la materialización de riesgos, ocasionando perdidas considerables si estos ocurriesen. Debido a que han transcurrido seis años del mencionado examen especial, el presente desarrollo iniciará de la identificación de la metodología adecuada para el Análisis y Gestión de Riesgos (Tejena-Macias, 2018), tomando en cuenta el control interno (Ríos, 2021) y las buenas prácticas de otros estándares y guías internacionales para el manejo de riesgos (Bonilla Guerrero, 2021), proponiendo controles de seguridad así como procedimientos para la gestión de riesgos (Andrade Talero, 2021), teniendo un mayor

control de los activos, su valor y las amenazas que puedan impactar a la empresa (Tejena-Macias, 2018), además de la conservación de la información en caso de contingencia.

1.3 Objetivos

1.3.1 General

Desarrollar el procedimiento para la Gestión de Riesgos del área informática de la EPM-GIDSA aplicando normas internacionales.

1.3.2 Específicos

a. Revisar el fundamento teórico actual de la Gestión de Riesgos del área informática de la EPM-GIDSA.
b. Identificar la metodología adecuada de Gestión de Riesgos, una vez analizada las buenas prácticas de las normas internacionales.
c. Elaborar el manual de procedimiento para la Gestión de Riesgos del área informática de la EPM-GIDSA.

CAPÍTULO II
ANTECEDENTES INVESTIGATIVOS

La correcta identificación de la información confidencial, la importancia de un cortafuego, los riesgos de la navegación en línea, la afectación de los Malware, la seguridad en la red, el Phishing se consideraría factores primordiales dentro de una Gestión de Riesgos, por lo que la aplicación de normas internacionales como ISO 31000 junto con el uso de modelos de procesos de Gestión de Riesgos como MAGERIT, COBIT en la EPM-GIDSA se podrá realizar la identificación, análisis, mitigación de riesgos en el área informática.

Esto permitirá tomar las acciones correctivas respecto a las observaciones emitidas por (Clavijo Mera, 2015) de la Contraloría General del Estado en el examen especial a los procesos administrativos, financieros, de mantenimiento, de operación y correlativos de los cuales se determina que "en el proceso Sistemas, el acceso a internet, el uso de correo electrónico, de computadoras y de impresoras; así como el uso de la información digital institucional no fue regulado mediante un documento aprobado. Tampoco se delineo ni aprobó el procedimiento para conservar la información en casos de contingencia, exponiendo a la empresa perderla si estos ocurriesen. Esto ocurre debido a que no se aprobó oportunamente el Manual de políticas y procedimientos del área de sistemas, inobservando las normas de control interno 410-04 "Políticas y Procedimientos", 410-10 "Seguridad de la Tecnología de la información", 410-11 "Plan de contingencias" y 410-12 "Administración de soporte de tecnologías de información"".

Por lo que para esta investigación se inicia con revisar y analizar la literatura de investigaciones realizadas a la Gestión de Riesgos, Estándares y Metodologías de los cuales se desprende los siguientes:

Con la aplica del estándar OSSTMM en la Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas) cuyo objetivo es prevenir la fuga de información y detectar posibles vulnerabilidades en sistemas informáticos, siguiendo un proceso estructurado,

partiendo desde la identificación de vulnerabilidades existentes, así como la aplicación de controles necesarios para mitigar las amenazas encontradas garantizando la integridad y confidencialidad de la información (Velasco Trujillo, 2020).

Con la aplicación de metodología NIST SP 800-30 en la empresa textiles Jhonatex se pudo determinar amenazas, vulnerabilidades y controles de mitigación, debiendo dar el tratamiento prioritario a los riesgos catalogados con criticidad alta debido a que si se materializan causaran perdidas monetarias y de prestigio empresarial (Bonilla Guerrero, 2021).

El análisis de riesgos informáticos en las Cooperativas de Ahorro y Crédito de los segmentos 2 y 3 de la ciudad de Ambato mediante el uso de la metodología COBIT 5 propuso planes de acción con el fin de reducir el posible impacto a suceder, debiendo el personal de la Cooperativa Indígena SAC comunicar, entender, implementar, monitorear y así dar el debido tratamiento al riesgo. Además, esta propuesta al usar una metodología aceptada internacionalmente brinda a la institución financiera cumplir con los principios de la seguridad de la información sobre la confidencialidad, integridad y disponibilidad (Barrera Barragán, 2019).

El "Análisis de los conceptos, elementos y técnicas de la gestión de riesgo orientado a las pymes del sector de las telecomunicaciones basado en MAGERIT V3" determina la existencia de riesgos críticos, importantes, apreciables y bajos relacionados directa o indirectamente con el servicio de internet, servicio principal de la empresa, requiriendo mitigar mediante salvaguardas propuestas en su investigación, específicamente en los activos hardware asociados a este servicio, además considera que para la mitigación de los riesgos se requiere la aplicación de un control y esto a su vez implica la disponibilidad presupuestaria por lo que la responsabilidad de su implementación recae al área administrativa (Andrade Talero, 2021).

Luego de ejecutar el tratamiento de riesgos en los activos críticos realizados en la "propuesta de un plan de contingencia para salvaguardar los activos de información en el departamento de tecnología de la información y comunicación de la Empresa

Pública Municipal de Residuos Sólidos Rumiñahui-Aseo EPM empleando la metodología MAGERIT", obtuvo como resultado la reducción significativa del riesgo, solo 2 activos pasaron a criticidad media, requiriendo ejecutar más salvaguardas para pasar a un nivel bajo. El 90% de activos críticos siendo estos 18 de 20 fueron tratados con éxito (Aldaz Calispa & Pazmiño Sanchez, 2021).

Los resultados del estudio Análisis y evaluación de riesgos enfocada en las organizaciones públicas: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0 ayudaron a identificar amenazas potenciales, siendo las amenazas mayormente susceptibles a ciberataques los servicios, los equipos y la información debido a la ausencia de controles de seguridad, considerando para el autor de este artículo la mayor amenaza el ser humano debido a que son ellos quienes manejan la información dentro de EMAPAL-EP (Avila Torres, 2021).

El correcto uso de modelos de gestión de riesgos que puede utilizar según (Llontop Díaz, 2018) en su investigación sobre la Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks el cual mediante el modelo creado por las normas internacionales SO 17799, SO 27001 y MAGERIT concluye que el modelo utilizado ayudo eficientemente al tratamiento de los riesgos de TI, además de estar preparados para tratarlos y de ser el caso aceptarlos, así como mantener una adecuada documentación de cada incidente, ejecutando los planes de contingencia y continuidad del negocio tras un desastre (Martínez, 2018).

La fundamentación teórica para esta investigación es la siguiente:

Gestión de Riesgos

Son actividades coordinadas para dirigir y controlar la organización con relación al riesgo. Es parte de la gobernanza en el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión.

El propósito de la gestión del riesgo es la creación y la protección del valor, mejorando el desempeño, fomentando la innovación y contribuyendo a lograr los objetivos.
El riesgo se mide al combinar la probabilidad de un evento y sus consecuencias. La metodología de gestión de riesgos de los sistemas de información tiene como objetivo analizar y evaluar los factores que inciden en el riesgo, para posteriormente tratar el riesgo, monitorear y revisar continuamente el plan de seguridad. Los conceptos centrales de la metodología son los de amenaza, vulnerabilidad, activo, impacto y riesgo. La relación operativa de estos conceptos se materializa cuando una amenaza explota una o más vulnerabilidades para dañar activos, evento que impactará a la organización. Una vez identificados y evaluados los riesgos, deben ser tratados, es decir, transferidos, evitados o aceptados. El tratamiento de los riesgos se realiza sobre la base de un plan de seguridad cuidadosamente diseñado, que debe ser monitoreado, revisado y corregido continuamente según sea necesario. Se han desarrollado muchos métodos que implementan la totalidad o partes de la metodología de gestión de riesgos. Aunque la mayoría de ellos siguen de cerca la metodología descrita en las normas internacionales pertinentes, difieren considerablemente tanto en su filosofía subyacente como en sus pasos específicos (Katsikas, 2009)

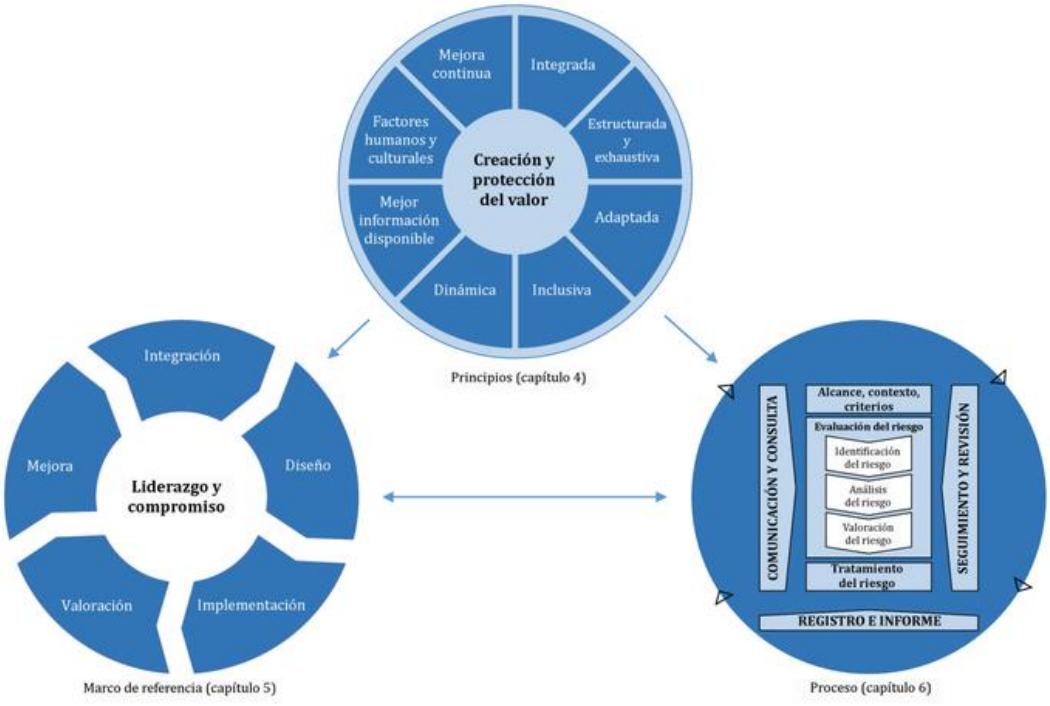
Estándares

Existen estándares de gestión de riesgos de la información como los siguientes:

- 2002 - SP 800-30 - Gestión de riesgos para los sistemas de tecnología de la información - Recomendaciones del Instituto Nacional de Normas y Tecnología;
- 2005 - ISO 27001: 2005 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información (SGSI) - Requisitos;
- 2006 - BS 7799 Parte 3: Directrices de 2006 para la gestión de riesgos de seguridad de la información;
- 2008 - ISO 27005: 2008 Tecnología de la información – "Gestión de riesgos de seguridad de la información - Técnicas de seguridad"
- 2008 - BS 31100 - Código de prácticas para la gestión de riesgos (Watson, David y Jones, 2013).

- 2018 - ISO 31000 - Gestión de riesgos - Directrices sobre principios e implementación de la gestión de riesgos, indistintamente del tamaño, fuente de capital, razón social, mercado, esta norma es aplicable a todo tipo de empresas, mediante el establecimiento de principios de un Sistema de Gestión de Riesgos, sin especificar concretamente un sector o área, además la norma busca controlar, gestionar y minimizar un riesgo de cualquier naturaleza, grado de incidencia u origen mediante la integración de la estrategia, procesos, políticas de cada empresa al Sistema de Gestión de Riesgos. Proporciona instrucciones sobre como integrar el pensamiento basado en riesgos en la organización, forma parte del liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles (ISACA, 2018b). A continuación, se presenta la figura 1 el cual describe los principios, marco de referencia y proceso de la norma ISO 31000.

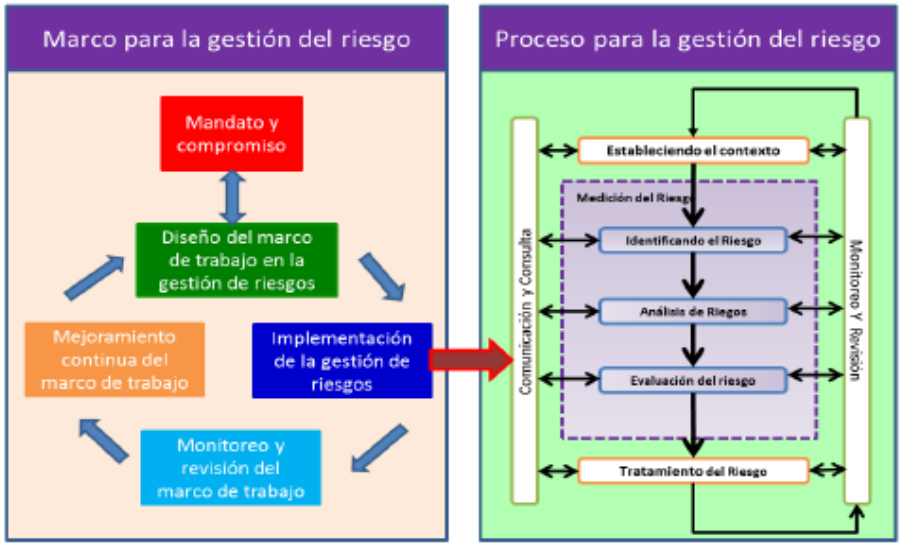
Figura 1: ISO 31000 – Gestión del riesgo



Nota. La figura resume la norma ISO 31000:2018 respecto a los principios, marco de referencia y su proceso de gestión de riesgos, tomado de *Norma Internacional ISO 31000. Administración/Gestión de Riesgos — Lineamientos Guía (*(ISACA, 2018a)*p.6), por ISACA,2018*

- AS/NZS ISO 31000:2009. – Consta de siete procesos, cada proceso actúa de manera independiente y puede ser aplicada en diferente orden, los procesos son: Establecer el contexto, identificación de los riesgos, análisis de los riesgos, evaluación de los riesgos, tratamiento del riesgo, comunicación y consulta, monitoreo y revisión (Australian et al., 2004). El resumen de la norma AS/NZS ISO 31000:2009 se describe en la figura 2 el cual sirve para entender el marco, proceso y principios.

FIGURA 2: RESUMEN DE LA NORMA AS/NZS ISO 31000:2009



Principios para la gestión del riesgo

1. Crea valor
2. Ser parte integral de los procesos
3. Ser parte de la toma de decisiones
4. Abordar explícitamente la incertidumbre
5. Ser sistemática, estructurada y oportuna
6. Basarse en la mejor información disponible
7. Es Adaptado
8. Toma en cuenta factores humanos y culturales
9. Es transparente e inclusivo
10. Es dinámica, iterativa y sensible a los cambios
11. Facilita la mejora continua y la mejora de la organización

Nota. La figura resume la norma AS/NZS ISO 31000:2009 respecto a los principios, marco y su proceso de gestión de riesgos. Tomado de *ISO 31000:2009 Risk Management (p.10), por Joint Australian New Zealand International Standard, 2004.*

Metodologías

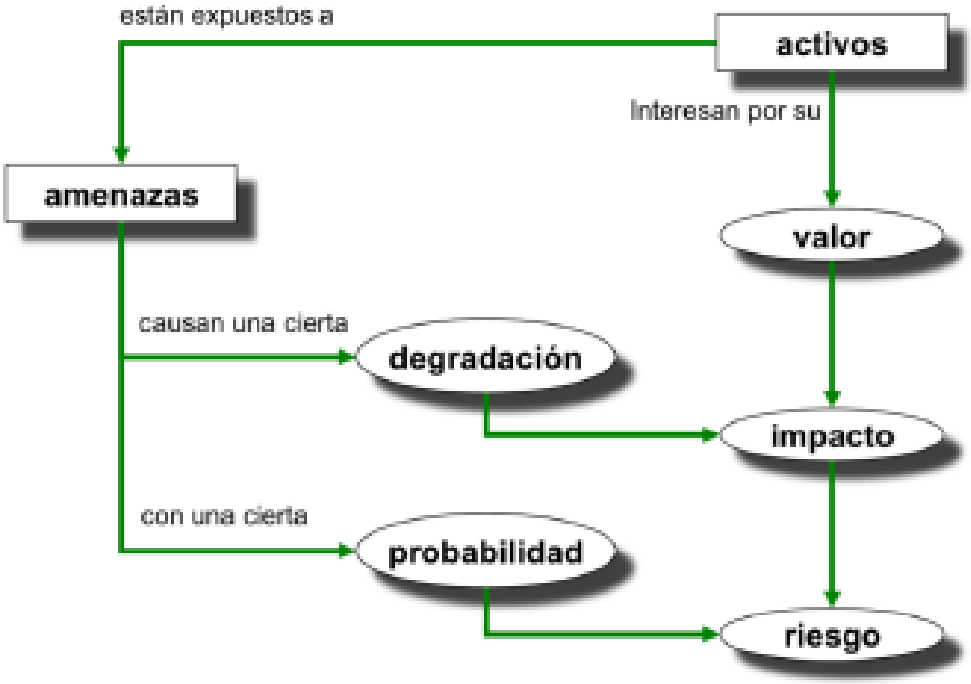
Además de los estándares descritos anteriormente, existen una serie de metodologías de gestión de riesgos que se pueden utilizar para gestionar los riesgos de seguridad de la información. Algunos utilizan descripciones de alto nivel del sistema de información en estudio; otros piden descripciones detalladas. Entre las metodologías según (Jimbo Santana & Cabrera Pantoja, 2021) se puede detallar:

- A&K analysis (the Nethgerlands);
- MARION (France);
- MEHARI (France) proporciona un modelo de evaluación de riesgos, componentes y procesos modulares. Mejora la capacidad de descubrir vulnerabilidades a través de auditorías y analizar situaciones de riesgo.
- OCTAVE (the United States) define una técnica de planificación y evaluación estratégica basada en riesgos para la seguridad
- Österreichisches IT-Sicherheitshandbuch (Austria).
- NIST - El Instituto Nacional de Estándares y Tecnología, compiló, en 1991, un informe completo sobre métodos y herramientas de gestión de riesgos.
- CRAMM (Metodología de Gestión y Análisis de Riesgos CCTA) es un método desarrollado por la organización gubernamental británica CCTA (Agencia Central de Comunicaciones y Telecomunicaciones), ahora rebautizada como Oficina de Comercio Gubernamental (OGC).
- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) proporciona una visión global y coherente de la seguridad de los sistemas de información.
- MAGERIT.- Estudia el Riesgo y el entorno asociado a este, diseñado para compañías que cuentan con servicios de tipo informático e información digital (ISACA, 2018b), permite encontrar inconsistencias no identificadas que incluso no se sospechaban de la existencia de ellas (Tejena-Macias, 2018) mediante el análisis del valor asignado a un proceso de la organización y como protegerlo

(ISACA, 2018b). Metodología que da soporte en el oportuno tratamiento y preparación para acreditaciones, certificaciones y auditorias.

El flujo de gestión de riesgos según MAGERIT esta descrita en la figura 3 el cual inicia con la identificación de los activos, su valor, el impacto que puede ocasionar si este saliera afectado, el riesgo de ocurrencia, las amenazas a las que están expuestas causando una cierta degradación y probabilidad de que ocurra un riesgo.

Figura 3: Análisis de riesgos MARGERIT



Nota. La figura resume el análisis de riesgos según MAGERITR V3. Tomado de *Libro I - Método. Ministerio de Hacienda y Administraciones Publicas (p.22), por Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012.*

- Cobit 2019.- Es un marco de referencia para el gobierno y la gestión de la información y la tecnología dirigido a toda la empresa, cuenta con 37 procesos de TI, cada proceso está definido con entradas y salidas, objetivos, métodos para medir el desempeño entre otros (ISACA, 2019).

- Principios:
  - Sistema de Gobierno: Valor para las partes interesadas, Enfoque Holístico, Sistema de Gobierno Dinámico, Separar Gobierno de Gestión, Ajustado a la necesidad empresarial, Sistema de Gobierno extremo a extremo.
  - Marco de Gobierno: Basado en modelo conceptual, Abierto y Flexible, Alineado con los principios y estándares
- Dominios
  - Objetivos de gobierno: EDM Evaluar, Dirigir y Supervisar
  - Objetivos de gestión: APO Alinear, Planear y Organizar, BAI Construir, Adquirir e Implementar, DSS Entrega, Servicio y Soporte, MEA Supervisar, Evaluar y Valorar.
- Integración con otros marcos
  - Atendiendo características propias, parámetros específicos o genéricas de la institución.
- Este marco contiene procesos, controles, medidas, indicadores y procesos para gestión y gobierno de TI y separa el gobierno de la gestión.

Monitoreo

La actividad final de gestión de riesgos es monitorear y rastrear el estado de riesgo a nivel individual. Los riesgos de alta prioridad se siguen de cerca para detectar alteraciones en su nivel de riesgo. Los indicadores de riesgo definidos anteriormente brindan advertencias tempranas de cambios significativos que pueden estar ocurriendo. Los riesgos como grupo también se sopesan como un todo para determinar si el nivel general de riesgo ha cambiado (Velásquez, 2021).

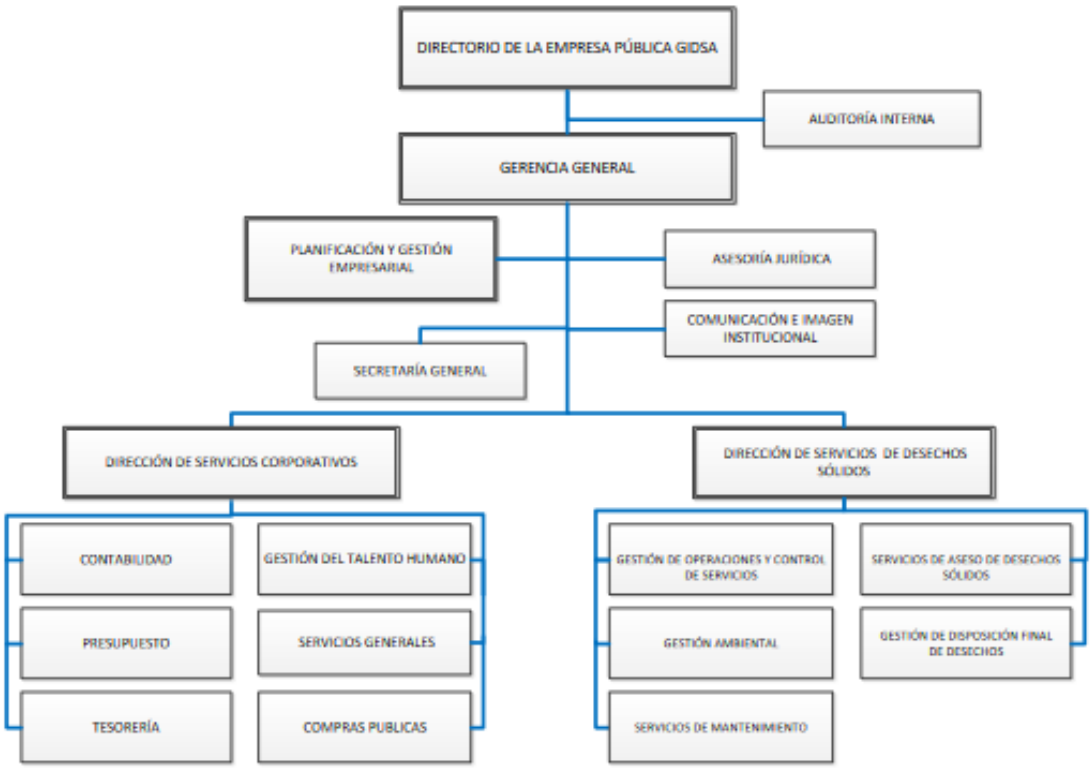
2.1. Fundamento teórico actual de la gestión de riesgos del área informática de la EPM-GIDSA

La EPM-GIDSA tiene como misión el prestar servicios de calidad en la gestión integral de desechos sólidos del cantón Ambato que contribuyen a mantener la salud,

bienestar de los habitantes y la protección del ambiente, con la participación activa de la ciudadanía y utilizando efectivamente el talento humano y los recursos.

Dentro del organigrama estructural del Estatuto Organizacional de Gestión por Procesos de la empresa descrita en la figura 4, la subárea de Tecnologías de la Información se encuentra dentro de la Coordinación de Servicios Corporativos, área Servicios Generales, considerada subárea de apoyo sin autoridad de toma de decisiones:

Figura 4**:** Organigrama estructural EPM-GIDSA



Nota: La figura describe el Organigrama estructural de la EPM-GIDA. Tomado de *Estatuto Organizacional de Gestión por procesos (p.8),* por *EPM-GIDSA.*

La Misión de Tecnologías de Información es: Proveer servicios de soporte informático y de desarrollo de tecnologías de la comunicación para el procesamiento de datos y acceso a la información, mediante la implantación de una infraestructura tecnológica actualizada y el suministro de sistemas y aplicaciones.

Las Políticas que se encuentran aprobadas dentro de Tecnologías de Información son:

- Políticas y normativas de respaldo de información (back ups): tiene como objetivo Definir y proporcionar las Políticas y Normas relacionadas con el "Respaldo de la Información (Back-Ups)" de la EPM-GIDSA, con la finalidad de atenuar los impactos para pérdida de Información para mantener la continuidad de las labores de la Empresa. Base Legal: Las Políticas y su Normativa tienen su base legal en las Normas Internas de Control de la CGE, norma 410-10 (EPM-GIDSA, 2015b).
- Manual de políticas de buen uso de tecnología y de seguridad informática: tiene como objetivo Establecer en la Empresa Pública Municipal de la Gestión Integral de Desechos Sólidos de la ciudad de Ambato EPM-GIDSA normas de buen uso y seguridad en los equipos de cómputo, de comunicación, Internet, correo electrónico y programas internos para operar en forma confiable (EPM-GIDSA, 2015a).

- Dentro del Estatuto Organizacional de Gestión por Procesos corresponde al subproceso DE LA TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN, el elaborar el plan de mitigación de riesgos operativos y el sistema de control (EPMGIDSA, 2020);

2.2. Identificación de metodología adecuada para la gestión de riesgos de la EPMGIDSA

De las normas internacionales descritos en este trabajo de investigación se detallan a continuación en la tabla 1 las características de la norma ISO 31000:2018 y AS/NZS 4360 Gestión de riesgos, para determinar cuál de estas es la que mejor se adaptan a las necesidades de la EPM-GIDSA.

TABLA 1: COMPARATIVA CARACTERÍSTICAS NORMAS INTERNACIONALES

Características	ISO 31000:2018	AS/NZS ISO 31000
Aplicación	A toda la organización	A todas las etapas de vida de una actividad, función, proyecto, producto o activo
Objetivo principal	Creación y protección del valor	Proporcionar principios y directrices genéricas para la gestión del riesgo.
Principios	Integrada, Estructurada y exhaustiva, Adaptada, Inclusiva, Dinámica, Mejor información disponible, factores humanos y culturales, mejora continua	Crear Valor, Ser parte integral de los procesos, Ser parte de la toma de decisiones, Abordar explícitamente la incertidumbre, Ser sistemática, estructurada y oportuna Basarse en la mejor información disponible, Ser adaptado, Toma en cuenta factores humanos y culturales, Es transparente e inclusivo, Es dinámica, iterativa y sensible a los cambios, Fácil la mejora continua y la mejora de la organización.
Marco de referencia	Permite integrar, diseñar, implementar, valorar y mejorar la gestión de riesgos en todas sus actividades y	Mandato y compromiso, Diseño del marco de trabajo en la gestión de riesgos.

Características	ISO 31000:2018	AS/NZS ISO 31000
	funciones significativas que den vida a la empresa, requiere apoyo de las partes interesadas en especial de la gerencia.	Implementación de la gestión de riesgos. Monitoreo y revisión del marco de trabajo. Mejoramiento continuo del marco de trabajo.
Proceso de gestión de riesgos	Establecer el contexto, Identificar el riesgo, Analizar el riesgo, Evaluación del riesgo, Tratamiento de riesgos Comunicación y consulta, Monitoreo y seguimiento	Comunicación y consulta, Establecer el contexto, Identificación del riesgo, Análisis del riesgo, Evaluación del riesgo, Tratamiento del riesgo, Monitoreo y seguimiento

Fuente: Propia / Elaborador por Jessica Guevara

La norma ISO 31000 y AS/NZS ISO 31000 dentro de sus principios, marco de referencia y proceso de gestión de riesgos mantienen una similitud en su estructura, sin embargo, considerando que el proceso de gestión de riesgos debe ser aplicable a toda la empresa y no solo a determinadas actividades, funciones, proyectos, productos o activos como lo determina la AS/NZS ISO 31000, se determina que la norma ISO 31000 es la que mejor se adapta a las necesidades de este trabajo.

Respecto a las metodologías de gestión de riesgos que tienen compatibilidad a la norma ISO 3100 se ha considerado a MAGERIT y COBIT 2019 para lo cual y con el propósito de identificar cual se adapta a la norma ISO 31000 se describe a continuación en las tablas 2 y 3 las características en común entre estos modelos:

TABLA 2: COMPARATIVA DE NORMA ISO 31000 CON METODOLOGÍA MAGERIT

Proceso de Gestión de Riesgo	Proceso de Gestión de Riesgo							
			MAGERIT V3.0					
	ISO/IEC 31000		Definir roles y responsabilidades	Establecer el contexto	Análisis de riesgos	Evaluación de riesgos	Tratamiento del riesgo	Seguimiento y Monitoreo
		Establecer el contexto	X	X				
		Identificar el riesgo			X			
		Analizar el riesgo			X			
		Evaluación del riesgo				X		
		Tratamiento de riesgos					X	
		Comunicación y consulta	X			X		
		Monitoreo y seguimiento						X

Fuente: Propia / Elaborador por Jessica Guevara

La metodología MAGERIT según lo descrito en la tabla 2 es completamente acoplable en todas las etapas del proceso de la norma ISO 31000, debido a que permite la implementación del proceso de Gestión de Riesgos dentro de un marco de trabajo, permitiendo a la Gerencia General de la EPM-GIDSA pueda tomar decisiones sobre los riesgos de Tecnologías de la Información.

TABLA 3: COMPARATIVA NORMA ISO 31000 CON METODOLOGÍA COBIT 2019

PROCESO DE GESTIÓN DE RIESGO	PROCESO DE GESTIÓN DE RIESGO							
			COBIT 2019					
	ISO/IEC 31000		Alineación de la administración de TI con el negocio	Establecimiento del contexto	Identificar amenazas y vulnerabilidades	Evaluación de riesgos	Respuesta a los riesgos	Mantenimiento y monitoreo
		Establecer el contexto	X	X				
		Identificar el riesgo			X			
		Analizar el riesgo						
		Evaluación del riesgo				X		
		Tratamiento de riesgos						
		Comunicación y consulta						
		Monitoreo y seguimiento						X

Fuente: Propia / Elaborador por Jessica Guevara

De esta comparación se determina que la metodología COBIT es acoplable en cuatro de seis etapas del proceso de Gestión de Riesgos establecido en la norma ISO 31000, dejando de lado el análisis de riesgo, el tratamiento del riesgo y la comunicación y consulta, etapas fundamentales para el desarrollo de este trabajo.

Por lo que la metodología seleccionada para este trabajo es MAGERIT V3, ya que permitirá realizar la identificación, análisis, evaluación, tratamiento, así como la aplicación de controles o salvaguardas a los riesgos informáticos, identificando los puntos más débiles de la estructura de Tecnologías de la Información de la EPM-GIDSA, así como la aplicación de políticas de seguridad y resguardo de información existentes en la EPM-GIDSA.

Además, MAGERIT V3 se acopla íntegramente con la norma ISO 31000, norma que es aplicable de manera íntegra a cualquier organización como la EPM-GIDSA.

CAPÍTULO III
MARCO METODOLÓGICO

3.1. Ubicación

La presente investigación, se realizó en la ciudad de Ambato, en la Empresa Pública Municipal para la Gestión Integral de los Desechos Sólidos del cantón Ambato EPM-GIDSA fue fundada en 2011 mediante Ordenanza de Creación, se dedica al barrido, recolección, transporte y disposición final de desechos en el cantón Ambato.

La EPM-GIDSA tiene cuatro oficinas en la ciudad distribuidas de la siguiente manera: oficinas administrativas, oficinas de talleres y bodegas, oficinas del Relleno Sanitario, oficinas de Escombrera, tomando como punto central de la investigación a las oficinas administrativas ubicadas en la Parroquia Izamba, Calles César Augusto Salazar y José Cobo, en estas oficinas se encuentran en su mayoría los activos del área informática.

3.2. Equipos y materiales

En la tabla 4, se describe los equipos y materiales utilizados para el despliegue de la presente investigación

Tabla 4: EQUIPOS Y MATERIALES UTILIZADOS

Orden	Descripción	Unidad	Cantidad	Costo unitario (USD $)	Costo total (USD $)
1	Computador	Unidad	1	400.00	400.00
2	Papel	Resma	1	4.00	4.00
3	Software	Unidad	1	400.00	400.00
4	Internet	Horas	500	0.10	50.00
5	Impresora	Unidad	1	300.00	300.00
6	Capacitación	Unidad	1	300.00	300.00
TOTAL					**1454.00**

Fuente: Propia / Elaborador por Jessica Guevara

3.3. Tipo de investigación

Investigación aplicada

El propósito de este estudio es desarrollar un procedimiento para la gestión de riesgos del área informática de la EPM-GIDSA mediante la aplicación de normas internacionales, el cual permitirá servir como guía para toda la empresa.

Investigación de campo

Los datos se obtendrán en el campo debido a que se observará y obtendré resultados esperados.

Investigación correlacional

El alcance de la investigación es de tipo correlacional debido a que a mayor nivel de cumplimiento de la norma ISO 31000 se disminuirá el valor del riesgo.

Investigación cuantitativa

El enfoque será cuantitativo debido a que en la valoración inicial se encontró falencias en los factores del examen de contraloría y luego se cubrió la necesidad con la aplicación de la norma ISO 31000 y metodología MAGERIT y porcentaje en mejora.

3.4 Prueba de Hipótesis

Planteamiento de hipótesis

La población de la investigación es generalmente una gran colección de individuos u objetos que son el foco principal de una investigación científica (Rivas,2020)

Hipótesis de investigación

La aplicación de la normativa ISO 31000 reducirá los porcentajes de riesgo de los activos del área informática de la EPM-GIDSA

Hipótesis nula

La aplicación de la normativa ISO 31000 no reducirá los porcentajes de riesgo de los activos del área informática de la EPM-GIDSA.

3.5 Población o muestra:

La población o muestra se determina en base al inventario de activos existentes en el área informática de la EPM-GIDSA siendo un total de 60 activos a los cuales según la metodología MAGERIT v3 se le asigna un valor de afectación a su disponibilidad, integridad y confidencialidad en base a los criterios de valoración de activos detallados en la tabla 5.

TABLA 5: CRITERIOS DE VALORACIÓN DE ACTIVOS

Criterio de Valoración Disponibilidad		
¿Qué importancia tendría que el activo no estuviera disponible?		
Alta (A)	3	Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la EPM-GIDSA.
Media (M)	2	Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la EPM-GIDSA.
Baja (B)	1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para el activo.
Nula (N)	0	Información cuya inaccesibilidad no afecta la actividad normal de la EPM-GIDSA.

Criterio de Valoración Integridad		
¿Qué importancia tendría que los datos fueran modificados fuera de control?		
Alta (A)	3	Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades.
Media (M)	2	Modificación de información no autorizada, pudiendo ocasionar perjuicio significativo a la EPM-GIDSA o terceros debido a la dificultad requerida para su reparación.
Baja (B)	1	Modificación de información no autorizada, pudiendo ocasionar perjuicio a la EPM-GIDSA o terceros aun cuando esta pueda repararse.
Nula (N)	0	Modificación de información no autorizada, la cual no afecta a las actividades de la EPM-GIDSA o terceros aun cuando esta pueda repararse.

Criterio de Valoración Confidencialidad		
¿Cuál es la importancia en el caso de que personas no autorizadas conozcan el dato?		
Alta (A)	3	Conocimiento y uso de información por un grupo selecto de servidores, ocasionando perjuicio a la EPM-GIDSA o terceros al ser difundida.
Media (M)	2	Conocimiento y uso de información por un grupo de servidores de la EPM-GIDSA la cual es requerida para realizar sus labores.
Baja (B)	1	Conocimiento y uso de información por todos los servidores de la EPM-GIDSA
Nula (N)	0	Conocimiento y uso de información por toda la ciudadanía dentro o fuera de la EPM-GIDSA.

El cálculo de criticidad del activo se determina buscando el valor máximo asignado a la disponibilidad, integridad o confidencialidad considerado por la Analista Informática de la EPM-GIDSA.

Por lo que de los 60 activos del área informática existentes en la EPM-GIDSA se determina que la muestra a trabajar son 42 activos informáticos con valor 3 - Alta (A) descritos en la tabla 6:

Tabla 6: POBLACIÓN O MUESTRA

#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
1	HW1 - Servidor Producción 1	TICS	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
2	HW2 - Servidor Producción 2	TICS	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
3	HW3 - Router de borde Relleno	TICS	Alta (A)	3	Alta (A)	3	Media (M)	2	3
4	HW4 - Router de borde Talleres	TICS	Alta (A)	3	Alta (A)	3	Media (M)	2	3
5	HW5 - Router de borde Matriz	TICS	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
6	HW6 - Router de borde Escombrera	TICS	Alta (A)	3	Media (M)	2	Media (M)	2	3
7	HW7 - Switch de acceso piso	TICS	Alta (A)	3	Baja (B)	1	Baja (B)	1	3
8	HW8 - Router de Core	TICS	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
9	HW9 Switch de core matriz	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
10	HW10 - Switch de acceso matriz	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
11	HW11 - Switch de acceso matriz	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3

#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
12	HW12 - Switch de acceso matriz	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
13	HW13 - Switch de acceso Talleres	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
14	HW14 - Switch de acceso Relleno	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
15	HW15 - Switch de acceso Escombrera	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
16	HW18 - Equipos Virtuales	TICS	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
17	HW19 - Puntos de acceso inalámbrico	TICS	Alta (A)	3	Baja (B)	1	Alta (A)	3	3
18	HW21 - Equipos de cómputo (escritorio, todo en uno, laptop)	TICS	Alta (A)	3	Baja (B)	1	Alta (A)	3	3
19	EA5 - Cableado de datos (utp, fibra y de alimentación)	TICS	Alta (A)	3	Nula (N)	0	Nula (N)	0	3
20	SW1 - sistema administrativo financiero	AME	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
21	SW2 - Sistema de Pesaje Camiones	Analista de Relleno Sanitario	Alta (A)	3	Alta (A)	3	Alta (A)	3	3

#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
22	SW3 - Correo	Personal Administrativo	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
23	SW4 - Sistema Documental	TIC	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
24	SW5 - Sistema de Cobros	AME	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
25	SW6 - Sistema de Talento Humano	Talento Humano	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
26	SW7 - BBDD SQL	TIC	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
27	SW8 - BBDD Oracle	TIC	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
28	SW10 - Sistema de backup	TIC	Alta (A)	3	Media (M)	2	Alta (A)	3	3
29	SW12 - Sistema Operativo Windows Linux	TIC	Alta (A)	3	Baja (B)	1	Alta (A)	3	3
30	SW13 - Hipervisor	TIC	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
31	DT1 - Copias de respaldos de información	TIC	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
32	SE2 - Servidor de nombres de dominio	TIC	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
33	SS2 - Outsourcing	TIC	Alta (A)	3	Nula (N)	0	Nula (N)	0	3

#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
34	SS3 - Proveedor de servicio de internet	CNT	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
35	RC1 - Red telefónica	TIC	Alta (A)	3	Nula (N)	0	Alta (A)	3	3
36	RC2 - Red de datos	TIC	Alta (A)	3	Nula (N)	0	Media (M)	2	3
37	RC3 – Wifi	TIC	Media (M)	2	Media (M)	2	Alta (A)	3	3
38	IN2 - Cuarto Servidores	EPMGIDSA	Alta (A)	3	Nula (N)	0	Nula (N)	0	3
39	EP3 - Usuarios internos	EPMGIDSA	Alta (A)	3	Nula (N)	0	Nula (N)	0	3
40	EP4 - Usuarios externos	EPMGIDSA	Alta (A)	3	Nula (N)	0	Nula (N)	0	3
41	DA1 -Discos	TIC	Media (M)	2	Alta (A)	3	Alta (A)	3	3
42	DA3 - Material Impreso	TIC	Alta (A)	3	Alta (A)	3	Alta (A)	3	3

3.6 Recolección de información:

La técnica de recolección de datos según Sampieri "implica elaborar un plan detallado de procedimientos que nos conduzcan a reunir datos con un propósito específico" (Jacqueline Cisneros-Caicedo et al., 2022).

La recolección de la información se realizará mediante la técnica de observación aplicando el instrumento de lista de referencia proporcionada por la Contraloría General del Estado en el examen especial, además de unas listas de cotejo que permita identificar la existencia adicional.

3.7 Procesamiento de la información y análisis estadístico:

El proceso de la información se realizará mediante el uso del marco de trabajo de la norma ISO 31000 y la metodología MAGERIT V3 permitiendo implementar el Proceso de Gestión de Riesgos mediante un marco de trabajo para que las coordinaciones y gerencia general tomen decisiones, teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Luego del análisis de resultados de la herramienta, se procede a realizar la prueba estadística de T-Student apareada de una cola.

3.8 Variables respuesta o resultados alcanzados

Mediante la aplicación de normas internacionales como la ISO 31000 Gestión de Riesgos en sistemas de información y la metodología de análisis MAGERIT V3 se podrá gestionar los riesgos existentes en el área informática de la EPM-GIDSA descritos en el siguiente cuadro:

Tipo Riesgo	Definición	Dimensión	Indicador	Cuando	Técnica / Instrumento
[A] Ataque intencionados.	Daños intencionados causados por humanos, su intención es similar a un ataque intencionado.	R12, R20, R25, R26, R27, R28, R29, R30, R31, R32, R33	Si el nivel del riesgo es mayor a 4.1	Al inicio y al final	Observación / Lista de referencia
[E] Fallos y errores no intencionados	Daño no intencionado causado por humanos, similar a un error involuntario en la naturaleza, que difiere solo en el propósito del tema	R10, R11, R13, R14, R16, R17, R18, R19, R21, R22, R23, R24, R34, R8, R9	Si el nivel del riesgo es mayor a 4.1	Al inicio y al final	Observación / Lista de referencia
[I] De Origen Industrial	Amenazas que pueden suscitarse de forma accidental o intencional debido a actividad humana de tipo industrial.	R15, R4, R5, R6, R7	Si el nivel del riesgo es mayor a 4.1	Al inicio y al final	Observación / Lista de referencia
[N] Desastres Naturales.	Eventos que pueden ocurrir sin intervención directa o indirectamente por causa humana.	R1, R2, R3	Si el nivel del riesgo es mayor a 4.1	Al inicio y al final	Observación / Lista de referencia

En el anexo 1 se detallan los riesgos agrupados por tipo de riesgo.

3.9 Procedimiento para la Gestión de riesgos del área informática de la EPM-GIDSA

El proceso de análisis de riesgos de la Empresa de Gestión de Desechos Sólidos de la ciudad de Ambato basándose en las buenas prácticas de la norma ISO 31000 y la metodología MAGERIT, está determinado con las siguientes actividades: Planteamiento de objetivo empresarial, objetivo de Unidad de Tecnología de Información, Identificación de activos, Definición de riesgos, Categorización de riesgos, Valoración cuantitativa y cualitativa, Evaluación de riesgos mediante mapa de calor, Análisis de riesgos, Valoración de controles

3.9.1 Objetivo Empresarial

Brindar servicio de barrido, recolección y disposición final de la ciudad de Ambato mediante el uso de equipos tecnológicos y de punta (EPMGIDSA, 2019).

3.9.2 Objetivo Empresarial

Proveer servicios informáticos de calidad, generar herramientas sistematizadas, versátiles y flexibles para satisfacer las necesidades institucionales y de la comunidad.

3.9.3 Identificación de activos

Un activo se le considera a todo aquel que contenga información documental de interés para la empresa, los cuales por su naturaleza deben ser salvaguardados por amenazas potenciales.

En la tabla 7 se enlista los activos, el dueño del activo, el valor promedio mensual considerado en el caso de que el activo sea afectado en su disponibilidad, el número de usuarios afectados por la pérdida de disponibilidad mensual, la valoración del activo a su disponibilidad, integridad y criticidad, determinando así la criticidad del activo. Lo dicho se ejemplifica de la siguiente manera:

TABLA 7: IDENTIFICACIÓN DE ACTIVOS

Identificación de activos					Valoración de activos						
#	Activo	Dueño de Activo	Valor monetario afectado por pérdida de disponibilidad (Mensual)	Número de usuarios afectado por pérdida de disponibilidad (mensual)	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
1	Servidor Producción 1	TICS	10000	37	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
2	Router de borde Relleno	TICS	2000	4	Alta (A)	3	Alta (A)	3	Media (M)	2	3

La valoración de activos a la disponibilidad, integridad, confidencialidad esta definidos en la tabla 5.

La criticidad es calculada en base a la metodología MAGERIT, asignando el valor más alto valorado a la disponibilidad, integridad y confidencialidad de cada activo.

3.9.4 Definición de riesgo

La definición del riesgo se lo realizara en base a los tipos de riesgos siendo estos: Fallos y errores no intencionados, Desastres Naturales, De Origen Industrial, Ataque intencionados, los riesgos están definidos en el anexo 1.

3.9.5 Categorización de riesgos

La etapa de caracterización de riesgos parte de los activos críticos a los cuales se les describe las vulnerabilidades, amenaza o riesgos, la degradación y el impacto, dando un panorama inicial de los riesgos asignados de cada activo.

La degradación es asignada con un valor porcentual de afectación de hasta el 100% a la disponibilidad, integridad, confidencialidad a cada activo.

El valor del impacto es calculado en base a la multiplicación del valor de criticidad y el máximo valor porcentual asignado a la disponibilidad, integridad y confidencialidad del activo. En la tabla 8 se ejemplifica lo antes descrito.

TABLA 8: DEFINICIÓN DEL RIESGO

Identificación de activos				Amenazas	Vulnerabilidades	Degradación			Impacto
#	Tipo	Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	Valor
1	Equipos Informáticos (Hardware) (HW)	HW1 - Servidor Producción 1	3	N1 – Fuego	Posibilidad de que el fuego acabe con el activo	100%	10%	10%	3
2	Equipos Informáticos (Hardware) (HW)	HW3 - Router de borde Relleno	3	N1 – Fuego	Posibilidad de que el fuego acabe con el activo	100%	10%	10%	3

3.9.6 Valoración de riesgos

Esta etapa se lo realiza a través de criterios de valoración de frecuencia, nivel del riesgo y el tratamiento que se le dará al riesgo, los cuales son definidas por la empresa, por lo que en las tablas 9, 10 y 11 se enuncian los criterios de valoración los cuales se utilizaran en el análisis del riesgo.

TABLA 9: CRITERIO DE VALORACIÓN DE FRECUENCIA

Criterio de valoración Frecuencia		
Frecuencia con la que ocurre o puede ocurrir dicho evento		
Muy Alto (MA)	3	A diario
Alto (A)	2	Mensualmente
Medio (M)	1	1 vez al año
Bajo (B)	0,1	Cada varios años

TABLA 10: CRITERIO DE VALORACIÓN DE NIVEL DE RIESGO

Nivel de riesgo que se asignará para ser trabado		
Muy Alto (MA)	MA	Entre 6,1 y 9
Alto (A)	A	Entre 4,1 y 6
Medio (M)	MA	Entre 2,1 y 4
Muy Bajo (MB)	MB	Entre 0 y 2

TABLA 11: CRITERIOS DE TRATAMIENTO DE RIESGO

Tratamiento del riesgo
Evitar el riesgo decidiendo no iniciar o continuar con la actividad
Aceptar o aumentar el riesgo en busca de una oportunidad
Eliminar la fuente de riesgo
Modificar la frecuencia
Modificar las consecuencias
Compartir el riesgo
Retener el riesgo con base en una decisión informada.

3.9.7 Análisis de Riesgos

El análisis de riesgo inicia asignando valores de frecuencia e impacto en base al riesgo y el activo, el producto de la valoración de la frecuencia y el impacto resulta el valor de riesgo.

Considerando los valores de la tabla 10 nivel de riesgo, los riesgos con valores superiores a 4.1 serán tratados al encontrarse dentro de los rangos alto y muy alto. El ejemplo del análisis de riesgos se describe en la tabla 12.

TABLA 12: ANÁLISIS DE RIESGOS

Activo	Riesgo			Valoración			
	#	Tipo	Descripción del riesgo	Frecuencia o Probabilidad	Impacto	Riesgo	Nivel de riesgo
HW1 - Servidor Producción 1	R1	[N] Desastres Naturales.	N1 - Fuego	0,1	3	0,3	Muy Bajo
SW7 - BBDD SQL	R9	[E] Fallos y errores no intencionados.	E2 - Errores de los usuarios	1	3	3	Medio
SW1 - Sistema Administrativo Financiero	R9	[E] Fallos y errores no intencionados.	E2 - Errores de los usuarios	2	3	6	Alto
SW5 – Sistema de Cobros	R14	[E] Fallos y errores no intencionados.	E7 - Vulnerabilidad de programas (software)	3	3	9	Muy Alto

3.9.8 Mapa de calor

Con el fin de identificar los riesgos a ser tratados, se ubica en un mapa de calor los riesgos, en el eje X el valor de probabilidad y en el eje Y el valor del impacto por cada riesgo según se puede observar en la figura 5.

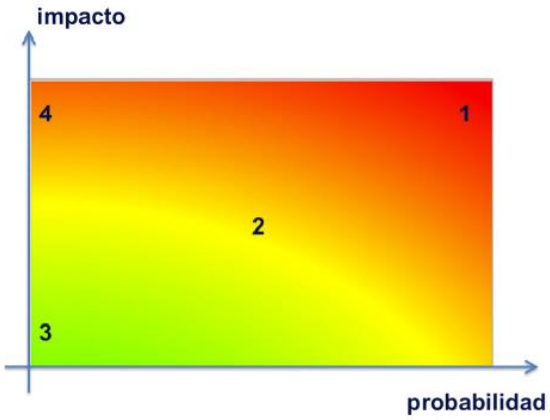
1: Franja roja: Se ubican en esta franja los riesgos con posibilidad muy probables y de muy alto impacto.

2: Franja naranja: Se ubican en esta franja los riesgos con situaciones muy probables, pero de impacto bajo o muy bajo hasta situaciones improbables y de impacto medio.

3: Franja amarilla: Se ubican en esta franja los riesgos de bajo impacto o hasta improbables.

4: Franja verde: Se ubica en esta franja los riesgos improbables, pero de muy alto impacto.

FIGURA 5: MAPA DE CALOR EL RIESGO EN FUNCIÓN DEL IMPACTO Y LA PROBABILIDAD



Nota. La figura visualiza las zonas en las que se ubican los riesgos. Tomado de *Libro I - Método. Ministerio de Hacienda y Administraciones Publicas (p.30), por Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012.*

3.9.9 Valoración de controles

La identificación riesgos con valores mayores 4.1 deben ser tratados, debiendo asignar salvaguardas o controles con el fin de tratarlos, mitigarlos, aceptarlos, transferirlos entre otros en base al siguiente modelo descrito en la tabla 13.

TABLA 13: CONTROLES

Riesgo	Registre el nombre del riesgo
Título del Control	Titulo corto que describa el control
Descripción	La definición del control debe ser especifica considerando por qué se implementa, quien o que lo implementa, como se implementa.
Dueño del control	El dueño del control se le considera a un individuo o un área específica, se debe describir el nombre del puesto y la persona encargada.
Descripción amplia sobre el monitoreo del control	Se especifica paso a paso como se valida el cumplimiento del control y su periodicidad.
Dueño del monitoreo del control	El dueño del monitoreo del control se le considera a un individuo o un área específica, se debe describir el nombre del puesto y la persona encargada.
Efectividad del control	Puede ser Efectivo, Inefectivo, Necesita Mejorar
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente Limitativo: Reduce el impacto de un incidente una vez producido Detectivo: Poder detectar errores o incidentes difíciles de predecir, detectar incidente que se está ocurriendo.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1 Resultados

Aplicando el Procedimiento para la Gestión de riesgos del área informática en base al criterio de la Analista Informática de la EPM-GIDSA descrita en la página 30 resulta la categorización del riesgo a los 42 activo, resultando el valor de Impacto descrito en el anexo 2.

Determinado el valor del impacto, se le asigna el valor de la frecuencia según los criterios enunciado en la tabla 9 y según el criterio observado por la Analista Informática de la EPM-GIDSA, para finalmente conseguir el valor del riesgo producto de la multiplicación del valor de la frecuencia y el impacto, obteniendo los siguientes resultados.

4.1.1 Resultados Pre-Implementación

4.1.1.1 [A] Ataque intencionados.

TABLA 14: PRE-IMPLEMENTACIÓN [A] ATAQUE INTENCIONADOS

Nivel de riesgo	Número	Frecuencia	Impacto	Riesgo
Alto	R20	2	3	6
	R29	2	3	6
	R31	16	24	48
Medio	R12	8	24	24
	R25	19	57	57
	R28	2	6	6
	R29	1	3	3
	R30	6	18	18
	R31	26	78	78
Muy Bajo	R12	3	90	9
	R20	0,2	6	0,6
	R25	0,3	9	0,9

Nivel de riesgo	Número	Frecuencia	Impacto	Riesgo
	R26	2,1	63	6,3
	R27	3,2	96	9,6
	R30	1	30	3
	R32	2,1	63	6,3
	R33	1,1	33	3,3
Total Riesgos Ataque Intencionado				**285**

Dentro del análisis de riesgos informático inicial, los riesgos considerados como Ataques Intencionados resulta un valor total de 285 según la tabla 14 de los cuales se debe dar tratamiento a los riesgos R20, R29, R31 por tener un nivel de riesgo Alto.

4.1.1.2 [E] Fallos y errores no intencionados

TABLA 15: PRE-IMPLEMENTACIÓN [E] FALLOS Y ERRORES NO INTENCIONADOS

Nivel de riesgo	Número	Frecuencia	Impacto	Riesgo
Muy Alto	R14	3	3	9
	R19	3	3	9
Alto	R13	2	3	6
	R16	8	12	24
	R19	4	6	12
	R21	2	3	6
	R22	4	6	12
	R23	2	3	6
	R24	2	3	6
	R34	14	21	42
	R8	6	9	18
	R9	12	18	36
Medio	R11	36	108	108
	R13	2	6	6
	R14	4	12	12
	R16	3	9	9

Nivel de riesgo	Número	Frecuencia	Impacto	Riesgo
	R19	3	9	9
	R21	18	54	54
	R24	1	3	3
	R8	1	3	3
	R9	7	21	21
Muy Bajo	R10	1,5	45	4,5
	R13	1,9	57	5,7
	R14	0,6	18	1,8
	R16	0,8	24	2,4
	R17	1,1	33	3,3
	R18	1,9	57	5,7
	R19	0,5	15	1,5
	R21	0,2	6	0,6
	R23	2,1	63	6,3
	R34	1,2	36	3,6
	R8	1,9	57	5,7
	R9	0,2	6	0,6
Total Fallos y errores no intencionados				**452,7**

Dentro del análisis de riesgos informático inicial, los riesgos considerados como Fallos y errores no intencionados resulta un valor total de 452.7 según la tabla 15 de los cuales se debe dar tratamiento a los riesgos R14, R19 por tener un nivel de riesgo Muy Alto y a los riesgos R13, R16, R19, R21, R22, R23, R24, R34, R8, R9 por tener un nivel de riesgo Alto.

4.1.1.3 [I] De Origen Industrial

TABLA 16: PRE-IMPLEMENTACIÓN [I] DE ORIGEN INDUSTRIAL

Nivel de riesgo	Número	Frecuencia	Impacto	Riesgo
Alto	R5	34	51	102
	R6	4	6	12
Medio	R15	2	6	6

Nivel de riesgo	Número	Frecuencia	Impacto	Riesgo
	R4	20	60	60
	R5	3	9	9
	R6	1	3	3
Muy Bajo	R4	1	1,5	1,5
	R5	1	1,5	1,5
	R6	2,1	3,9	2,1
	R7	2,2	64,5	6,45
Total Riesgos de Origen Industrial				**203,55**

Dentro del análisis de riesgos informático inicial, los riesgos considerados como de Origen Industrial resulta un valor total de 203.55 según la tabla 16 de los cuales se debe dar tratamiento a los riesgos R5, R6 por tener un nivel de riesgo Alto.

4.1.1.4 [N] Desastres Naturales

TABLA 17: PRE-IMPLEMENTACIÓN [N] DESASTRES NATURALES

Nivel de riesgo	Número	Frecuencia	Impacto	Riesgo
Muy Bajo	R1	2,2	66	6,6
	R2	2,2	64,5	6,45
	R3	2,2	64,5	6,45
Total Riesgos Desastres Naturales				**19,5**

Dentro del análisis de riesgos informático inicial, los riesgos considerados como Desastres Naturales resulta un valor total de 19.5 según la tabla 17 de los cuales no se evidencia ningún riesgo dentro del nivel Alto o Muy Alto para ser tratados.

4.1.1.5 Análisis

Los resultados totalizados en base al nivel del riesgo obtenidos en la pre implementación se describen en la tabla 18.

TABLA 18: RESULTADO DE ANÁLISIS DE RIESGOS INFORMÁTICOS

Tipo riesgo	Nivel de riesgo				
	Muy Bajo	**Medio**	**Alto**	**Muy Alto**	**Total**
[A] Ataque intencionados.	130	62	10		202
[E] Fallos y errores no intencionados.	139	75	28	2	244
[I] De Origen Industrial	26	26	19		71
[N] Desastres Naturales.	66				66
Total	**361**	**163**	**57**	**2**	**583**

Para lo cual se debe dar tratamiento a 57 riesgos en nivel Alto de los cuales 10 son de Ataque Intencionados, 28 de Fallos y errores no intencionados, 19 De Origen Industrial; además, 2 riesgos en nivel Muy Alto perteneciente a Fallos y errores no intencionados, por lo que se describen los controles a ejecutar con el fin de lograr disminuir la frecuencia o probabilidad de ocurrencia de riesgos sobre los activos informáticos.

Los controles detallados en la tabla 19 definen el tratamiento adecuado a los riesgos de nivel Alto y Muy alto disminuyendo de esta manera el valor de frecuencia.

TABLA 19: CONTROLES

Riesgo	**A11 - Interceptación de información (escucha)**
Título del Control	Seguridad Wireless (Wifi)
Descripción	Ejecución de políticas de buen uso de tecnología y seguridad informática, sección Administración de operaciones de equipos de cómputo, permiso de uso de internet
Dueño del control	Tecnologías de la Información, Analista y Asistente Informático
Descripción amplia sobre el monitoreo del control	El personal que ingrese a la empresa deberá firmar un acuerdo de confidencialidad de información entregado por Talento Humano. Tecnologías de la Información deberá entregar las claves de acceso en base a la matriz tecnológica según el cago a desempeñar. El empleado nuevo deberá leer el Manual de políticas de buen uso de tecnología y seguridad informática. Tecnologías de la Información cada dos meses deberá verificar los accesos otorgados a las aplicaciones a cada usuario y realizar los correctivos necesarios sobre el uso de tecnología y seguridad informática.
Dueño del monitoreo del control	Analista Informático
Efectividad del control	Efectivo
Tipo de control	Preventivo ya que permite llevar a cabo para evitar un incidente

Riesgo	**A5 - Ingeniería social**
Título del Control	Formación y concienciación
Descripción	Será responsabilidad de la dirección correspondiente solicitar la capacitación necesaria del usuario para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
Dueño del control	Talento Humano, Tecnologías de la Información, CSDS, CSC, Planificación, Gerencia General
Descripción amplia sobre el monitoreo del control	Tecnologías de la Información deberá comunicar mensualmente al personal sobre las formas de captación y/o robo de información mensualmente. El personal deberá leer y aplicar las recomendaciones emitidas.
Dueño del monitoreo del control	Analística Informático
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**A7 - Abuso de privilegios de acceso**

Título del Control	Cambios (actualizaciones y mantenimiento)
Descripción	Verificar los accesos correctos en base a las funciones que el personal desempeña en la empresa.
Dueño del control	Tecnologías de la Información
Descripción amplia sobre el monitoreo del control	Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de la EPM-GIDSA, deberán ser notificados por escrito o vía correo electrónico a la Unidad de Sistemas con el visto bueno del Coordinador del área solicitante, para realizar el ajuste.
Dueño del monitoreo del control	Analista Informático
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E1 - Fuga de información**

Título del Control	Protección criptográfica de la confidencialidad de los datos intercambiados
Descripción	Apoyándose en un método criptográfico, la información que se traslada por la empresa debe estar protegida hasta llegar al destinatario mediante el firewall.
Dueño del control	Talento Humano, Tecnologías de la Información, CSDS, CSC, Planificación, Gerencia General
Descripción amplia sobre el monitoreo del control	Tecnologías de la información deberá adquirir un certificado SSL para transporte seguro de información en la red. Verificar que el certificado SSL se encuentre activo.
Dueño del monitoreo del control	Analista Informático
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E12 - Errores de mantenimiento / actualización de programas (software)**

Título del Control	Cambios (actualizaciones y mantenimiento)
Descripción	Verificar los errores reportados por los empleados de la empresa debido al mal funcionamiento de los sistemas.
Dueño del control	Tecnologías de la Información
Descripción amplia sobre el monitoreo del control	El empleado deberá notificar a tecnologías de la información el error presentado en el sistema mediante correo electrónico. Tecnologías de la Información verificará la novedad suscitada. Tecnologías de la Información notificará mediante correo electrónico al proveedor del sistema para la corrección y/o modificación requerida. El proveedor remitirá las actualizaciones a ser instalada en las computadoras y/o servidores según sea el caso. Tecnologías de la Información instalará las actualizaciones en las computadoras y/o servidores.
Dueño del monitoreo del control	Analista Informático
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E14 - Errores de mantenimiento / actualización de equipos (hardware)**

Título del Control	Aseguramiento de la disponibilidad
Descripción	Mantener el equipo hardware actualizado tanto en hardware y software, garantizando el buen funcionamiento de las actividades de los empleados de la empresa.
Dueño del control	Tecnologías de la Información
Descripción amplia sobre el monitoreo del control	Tecnologías de la Información anualmente levantará el inventario informático del equipo informático. Tecnologías de la Información presentará un informe de estado y acciones de actualización y/o mantenimiento del equipo hardware. Tecnologías de la información presupuestará anualmente el mantenimiento de equipos informáticos, adquisición de partes y piezas para repotenciación y/o adquisición de nuevos equipos hardware para ser remplazados. Gerencia General asignará el presupuesto solicitado por Tecnologías de Información. Tecnologías de la Información elaborará el plan informático en base a la asignación presupuestaria en el año. Tecnologías de la información ejecutará el plan informático aprobado por Gerencia General.
Dueño del monitoreo del control	Analista Informático, Coordinador de Servicios Corporativos.
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E15 - Indisponibilidad del personal**

Título del Control	Formación y concienciación
Descripción	Capacitación técnica al personal informático para administración de aplicaciones.
Dueño del control	Talento Humano, Tecnologías de la información
Descripción amplia sobre el monitoreo del control	El personal solicitará a Talento Humano capacitación para el manejo de aplicaciones. Talento Humano realizará un plan de capacitación. Talento Humano comunicará la capacitación al personal solicitante. Talento Humano monitoreará el cumplimiento de las capacitaciones virtuales Tecnologías de la Información elaborará manuales de uso y comunicará sobre actualizaciones realizadas en los sistemas informáticos. El personal deberá leer los manuales proporcionados por tecnologías de información.
Dueño del monitoreo del control	Talento Humano, Tecnologías de la información
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E16 - Caída del sistema por agotamiento de recursos**

Título del Control	Protección de los Equipos Informáticos
Descripción	Realizar el monitoreo de funcionamiento de equipos hardware, así como el rendimiento de cada una de ellas.
Dueño del control	Tecnologías de la Información
Descripción amplia sobre el monitoreo del control	Tecnologías de la Información realizará el monitoreo de funcionamiento de los equipos hardware. De ser necesario realizará la adquisición de partes y piezas para mejorar el rendimiento físico del equipo. Ejecutar el plan de mantenimiento de hardware y software al parque informático.
Dueño del monitoreo del control	Analista Informático
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E2 - Errores de los usuarios**

Título del Control	Protección de las Aplicaciones Informáticas
Descripción	Verificación de fallas y vulnerabilidades en las aplicaciones de la empresa
Dueño del control	Tecnologías de la Información
Descripción amplia sobre el monitoreo del control	Los usuarios notificarán errores de funcionamiento de las aplicaciones a tecnologías de la información. Tecnologías de la información verificará el error o vulnerabilidad existente. Evaluará técnicamente la solución de la vulnerabilidad existente en la aplicación. Adquirirá nuevas tecnologías informáticas en caso de que las vulnerabilidades sean debido a obsolencia tecnológica.
Dueño del monitoreo del control	Analista Informático, Coordinador de Servicios Corporativos
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E5 - Alteración accidental de la información**
Título del Control	

	Aseguramiento de la integridad
Descripción	Verificación de información real en las aplicaciones de la empresa
Dueño del control	CSC, CSDS, Gerencia General, Planificación, Tecnologías de la Información
Descripción amplia sobre el monitoreo del control	El usuario reportará registro de información errónea en los sistemas al Coordinador de Servicios Corporativos. El coordinador de servicios corporativos dispondrá la revisión de información a Tecnologías de la Información. Tecnologías de la información verificará la información registrada y/o realizará las modificaciones requeridas. Tecnologías de la información comunicará los cambios solicitados a la unidad requirente.
Dueño del monitoreo del control	Analista Informático
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E6 - Pérdida de equipos**
Título del Control	Aseguramiento de la disponibilidad
Descripción	

	Disponer de póliza de seguro en caso de perdía del equipo, con el fin de recuperar los equipos perdidos.
Dueño del control	Administrador de seguro de bienes.
Descripción amplia sobre el monitoreo del control	El empleado notificará al administrador de seguros de bienes la pérdida del equipo. El administrador de seguro de bienes notificará a la aseguradora la reposición del bien robado. La aseguradora solicitará la documentación requerida para la reposición al Administrador de Bienes. El administrador de seguros de bienes entregará la documentación solicitada y monitoreará la devolución del bien.
Dueño del monitoreo del control	Administrador de seguro de bienes.
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E7 - Vulnerabilidad de programas (software)**
Título del Control	Cambios (actualizaciones y mantenimiento)
Descripción	

	Verificación de fallas y vulnerabilidades en las aplicaciones de la empresa
Dueño del control	Tecnologías de la Información
Descripción amplia sobre el monitoreo del control	Los usuarios notificarán errores de funcionamiento de las aplicaciones a tecnologías de la información. Tecnologías de la información verificará el error o vulnerabilidad existente. Evaluará técnicamente la solución de la vulnerabilidad existente en la aplicación. Adquirirá nuevas tecnologías informáticas en caso de que las vulnerabilidades sean debido a obsolencia tecnológica.
Dueño del monitoreo del control	Analista Informático, Coordinador de Servicios Corporativos
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E8 - Deficiencias en la organización**
Título del Control	Organización

Descripción	Verificar el manual de funciones de la empresa
Dueño del control	Talento Humano
Descripción amplia sobre el monitoreo del control	Talento Humano verificará las funciones de acuerdo al cargo a desempeñar. Talento Humano modificará de ser el caso las funciones asignadas a cada personal. Talento Humano creará la necesidad de puestos de trabajo en base a requerimientos empresariales.
Dueño del monitoreo del control	Talento Humano
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**E9 - Errores de secuencia**
Título del Control	Se aplican perfiles de seguridad

Descripción	Disponer de perfiles de usuario por usuario en cada sistema de la empresa.
Dueño del control	Tecnologías de la información, Talento Humano
Descripción amplia sobre el monitoreo del control	Tecnologías de la información asignará perfiles de usuario en base a las funciones asignadas por Talento Humano Se verificará mensualmente la asignación de perfiles de usuario en caso de salida de vacaciones y/o de la empresa.
Dueño del monitoreo del control	Analista Informático
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**I2 - Condiciones inadecuadas de temperatura o humedad**
Título del Control	Climatización

Descripción	Disponer de un adecuado clima para el buen funcionamiento de los equipos hardware en el cuarto de máquinas.
Dueño del control	Analista Informático
Descripción amplia sobre el monitoreo del control	Realizar el mantenimiento anualmente a los equipos de climatización instalado en el cuarto de máquina
Dueño del monitoreo del control	Analista Informático
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente
Riesgo	**I3 - Fallo de servicios de comunicaciones**
Título del Control	Aseguramiento de la disponibilidad
Descripción	Mantener el equipo hardware actualizado tanto en hardware y software, garantizando el buen funcionamiento de las actividades de los empleados de la empresa.
Dueño del control	Tecnologías de la Información

Descripción amplia sobre el monitoreo del control	Tecnologías de la Información anualmente levantará el inventario informático del equipo informático. Tecnologías de la Información presentará un informe de estado y acciones de actualización y/o mantenimiento del equipo hardware. Tecnologías de la información presupuestará anualmente el mantenimiento de equipos informáticos, adquisición de partes y piezas para repotenciación y/o adquisición de nuevos equipos hardware para ser remplazados. Gerencia General asignará el presupuesto solicitado por Tecnologías de Información. Tecnologías de la Información elaborará el plan informático en base a la asignación presupuestaria en el año. Tecnologías de la información ejecutará el plan informático aprobado por Gerencia General.
Dueño del monitoreo del control	Analista Informático, Coordinador de Servicios Corporativos.
Efectividad del control	Efectivo
Tipo de control	Preventivo: El que se lleva a cabo para evitar un incidente

4.1.2 Resultados Pos-Implementación

Con la aplicación de controles establecidos a los activos informáticos de la EPM-GIDSA con un valor de riesgo mayor a 4.1 y con nivel de riesgo Alto y Muy Alto, se logra cambiar la frecuencia o probabilidad de ocurrencia de riesgo a un valor de riesgo menor a 4, resultando lo siguiente:

4.1.2.1 [A] Ataque intencionados

TABLA 20 : POS-IMPLEMENTACIÓN [A] ATAQUE INTENCIONADOS

Nivel del riesgo	Número	Frecuencia	Impacto	Riesgo
Medio	R12	8	24	24
	R20	1	3	3
	R25	19	57	57
	R28	2	6	6
	R29	2	6	6
	R30	6	18	18
	R31	34	102	102
Muy Bajo	R12	3	90	9
	R20	0,2	6	0,6
	R25	0,3	9	0,9
	R26	2,1	63	6,3
	R27	3,2	96	9,6
	R30	1	30	3
	R32	2,1	63	6,3
	R33	1,1	33	3,3
Total Riesgo Ataque Intencionados				**255**

Tras la ejecución de controles detallados en la tabla 19 los riesgos considerados como Ataques Intencionados iniciaron con un valor de 285 según la tabla 14 disminuyendo según la tabla 20 a un valor de 255 debido a que el valor de la frecuencia o probabilidad de ocurrencia del riesgo ha disminuido.

4.1.2.2 [E] Fallos y errores no intencionados

TABLA 21: POS-IMPLEMENTACIÓN [E] FALLOS Y ERRORES NO INTENCIONADOS

Riesgo	Número	Frecuencia	Impacto	Riesgo
Medio	R11	36	108	108
	R13	2	6	6
	R14	5	15	15
	R16	7	21	21
	R19	6	18	18
	R21	19	57	57
	R22	2	6	6
	R24	2	6	6
	R34	7	21	21
	R8	4	12	12
	R9	13	39	39
Muy Bajo	R10	1,5	45	4,5
	R13	2	60	6
	R14	0,6	18	1,8
	R16	0,8	24	2,4
	R17	1,1	33	3,3
	R18	1,9	57	5,7
	R19	0,5	15	1,5
	R21	0,2	6	0,6
	R23	2,2	66	6,6
	R34	1,2	36	3,6
	R8	1,9	57	5,7
	R9	0,2	6	0,6
Total Riesgos Fallos y errores no intencionados				**351,3**

Tras la ejecución de controles detallados en la tabla 19 los riesgos considerados como Fallos y errores no intencionados iniciaron con un valor de 452.7 según la tabla 15

disminuyendo según la tabla 21 a un valor de 351.3 debido a que el valor de la frecuencia o probabilidad de ocurrencia del riesgo ha disminuido.

4.1.2.3 [I] De Origen Industrial

TABLA 22: POS-IMPLEMENTACIÓN [I] DE ORIGEN INDUSTRIAL

Riesgo	Número	Frecuencia	Impacto	Riesgo
Medio	R15	2	6	6
	R4	20	60	60
	R5	20	60	60
	R6	3	9	9
Muy Bajo	R4	1	1,5	1,5
	R5	1	1,5	1,5
	R6	2,1	3,9	2,1
	R7	2,2	64,5	6,45
Total Riesgos de Origen Industrial				**146,55**

Tras la ejecución de controles detallados en la tabla 19 los riesgos considerados como Fallos y errores no intencionados iniciaron con un valor de 203.55 según la tabla 16 disminuyendo según la tabla 22 a un valor de 146.55 debido a que el valor de la frecuencia o probabilidad de ocurrencia del riesgo ha disminuido.

4.1.2.4 Análisis

Los resultados de la post implementación visualizados en la figura 6 evidencia una disminución del valor del riesgo final en los tipos Ataques intencionados, Fallos y errores no intencionados, De origen Industrial; en el caso Desastres Naturales se mantiene el valor del riesgo, toda vez que los controles o salvaguardas a ejecutar dependen de la asignación presupuestaria asignada al área de Tecnologías de Información.

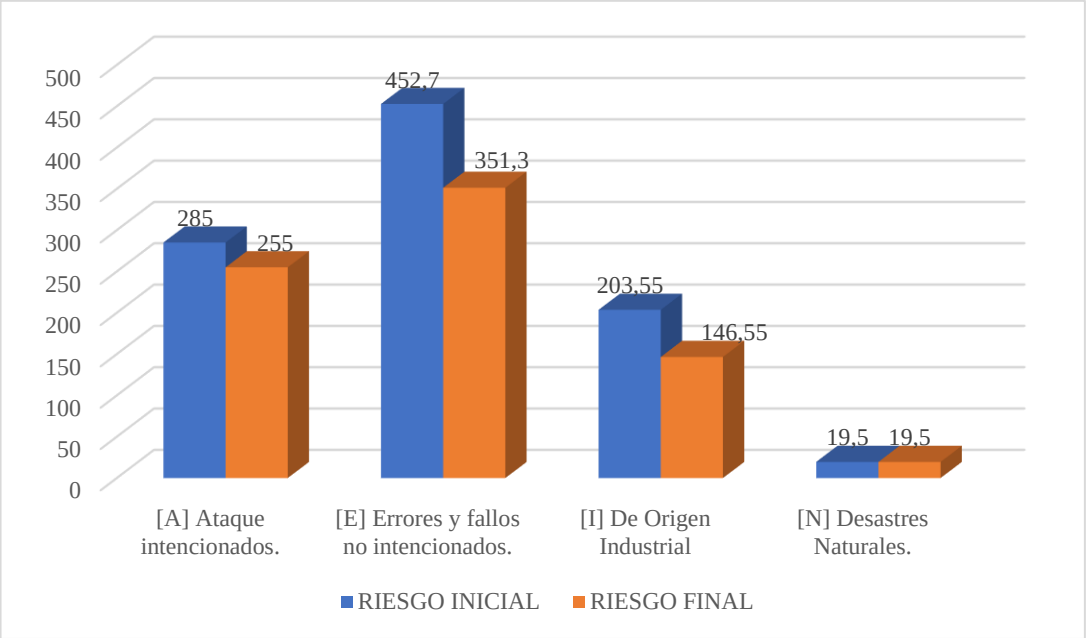


FIGURA 6: RESULTADOS POST IMPLEMENTACIÓN

4.1.3 Discusión

La información fue evaluada en la herramienta Análisis de Datos, con la función prueba T para medias de dos muestras emparejadas, de Microsoft Excel.

4.1.4 Normalidad

Para la prueba de normalidad en la que se debe aceptar la hipótesis de investigación y se consideran todas las categorías de riesgos ponderadas según la tabla 23.

TABLA 23: NORMALIDAD

TIPO DE RIESGO	RIESGO INICIAL	RIESGO FINAL
[A] Ataque intencionados.	285	255
[E] Fallos y errores no intencionados.	452,7	351,3
[I] De Origen Industrial	203,55	146,55
[N] Desastres Naturales.	19,5	19,5
Total	**960,75**	**772,35**

Una vez verificada la normalidad se decide aplicar el estadístico de T-Student con un valor de confianza del 95% para lo cual se obtuvieron los siguientes valores

TABLA 24: PRUEBA T-STUDENT

Prueba t para medias de dos muestras emparejadas		
	RIESGO INICIAL	***RIESGO FINAL***
Media	313,75	250,95
Varianza	16138,8525	10492,9425
Observaciones	3	3
Coeficiente de correlación de Pearson	0,973320335	
Diferencia hipotética de las medias	0	
Grados de libertad	2	
Estadístico t	3,017139358	
P(T<=t) una cola	0,047266466	
Valor crítico de t (una cola)	2,91998558	
P(T<=t) dos colas	0,094532932	
Valor crítico de t (dos colas)	4,30265273	

El promedio del riesgo inicial según la tabla 24 fue de 313.75, que son mayores a los riesgos que se calcularon en el riesgo final donde se da un valor de 250.95.

Por otra parte, el valor de P de una cola es el valor de significancia con el 0.05 obteniendo un valor tras el análisis de Tstudent de 0,047 por lo que nos lleva a rechazar la hipótesis nula y aceptar la hipótesis de investigación.

CAPÍTULO V
CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS

5.1 Conclusiones

Las políticas de buen uso de tecnología y de seguridad informática, así como la normativa de respaldo de información (back ups) existente como fundamentación teórica para la gestión de riesgos en el área informática de la EPM-GIDSA y descritas en el numeral 2.1 permitió iniciar con la categorización del riesgo según el anexo 2 consiguiendo los valores de impacto, así como la determinación de resultados de pre implementación sobre la gestión del riesgo.

El manual de procedimientos para la gestión de riesgos del área informática está establecido desde la identificación de activos, definición de riesgos, la categorización, la valorización, el análisis del riesgo, pudiendo de esta manera tratarlos en base a la valorización de controles establecidos a los riesgos ubicados en el mapa de calor en niveles Alto y Muy Alto.

La Gestión de Riesgos en el área de informática de la EPM-GIDSA mediante la aplicación de la norma internacional ISO 3100 y metodología Magerit V3 redujo el valor del riesgo a los Ataques Intencionados de 285 a 255; a los Errores y Fallos no Intencionados de 452.70 a 351.30; a los de Origen Industrial de 203.55 a 146,55.

Los resultados descritos en la tabla 23 evidencio que los riesgos por Fallos y errores no intencionados los cuales son originados por usuarios internos y externos de la empresa, presentaron un valor de riesgo inicial de 452.7 y tras los controles aplicados disminuyo a 351.3, evidenciando una disminución notable en el valor del riesgo al igual que los resultados mencionados en la investigación de (Aldaz Calispa & Pazmiño Sanchez, 2021) el cual detalla que “obtuvo la reducción significativa del riesgo, solo 2 activos pasaron a criticidad media, requiriendo ejecutar más salvaguardas para pasar a un nivel bajo”

El valor de los riesgos denominados Desastres Naturales no disminuye de 19,50 esto debido a que la frecuencia de ocurrencia de estos riesgos es bajas, sin embargo, en caso de materializarse el riesgo ocasionaría un impacto Muy Alto a la empresa EPM-GIDSA.

5.2 Recomendaciones

La principal limitante de la presente propuesta es no contar con el recurso humano calificado dentro del área de informática de la EPM-GIDSA para obtener un criterio adicional a la propuesta planteada, por lo que es recomendable que la empresa evalúe la contratación de personal técnico adicional al existente.

Los riegos por desastres naturales descritos en la tabla 17 no ubican a ningún riesgo dentro de los niveles medio, alto y muy alto, sin embargo, existen riesgos en el nivel muy bajo entre estos los R2 Daños por agua y R3 Desastres Naturales (terremotos, tsunami, erupciones volcánicas) con un valor de 6,45 debiendo anualmente ser monitorearlos a fin de que en el caso de suceder el impacto no impida continuar con el giro de la empresa. EPM-GIDSA.

El procedimiento de gestión de riesgos desarrollado en este trabajo puede ser aplicado en empresas públicas o privadas que tengan el mismo giro de negocio, además se puede usar la norma ISO 27500 como norma internacional para la Gestión de Riesgos con metodología MAGERIT V3 si el trabajo a desarrollar fuera específico en temas de seguridad de información.

Tras la presentación de la gestión de riesgos del área informática en la EPM-GIDA se deberá plantear la elaboración de planes de contingencia y continuidad de negocio para garantizar el funcionamiento de los servicios de la empresa, así como a la información de los clientes externos e internos, además de planes de capacitación a todo el personal de la EPM-GIDSA a fin de incentivar la participación constante sobre el cuidado y seguridad que se le debe dar a la información.

5.3 Bibliografía

Aldaz Calispa, N. I., & Pazmiño Sanchez, f. P. (2021). Propuesta de un plan de contingencia para salvaguardar los activos de información en el departamento de tecnología de la información y comunicación de la Empresa Pública Municipal de Residuos Sólidos Rumiñahui-aseo Epm empleando la metodología Magerit. In tesis. Https://dspace.ups.edu.ec/handle/123456789/19865

Andrade Talero, D. L. (2021). Análisis de los conceptos, elementos y técnicas de la gestión de riesgo orientado a las Pymes del sector de las telecomunicaciones basado en Magerit v3 [Universidad Nacional abierta y a distancia Escuela de Ciencias Básicas Tecnologías e Ingeniería Especialización en Seguridad Informática Sogamoso]. Https://repository.unad.edu.co/handle/10596/43373

Australian, J., Zealand, N., & standard, i. (2004). Iso 31000:2009 Risk Management.

Avila Torres, r. A. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-Ep basado en la metodología de Magerit versión 3.0. 7, 363–376. Https://doi.org/http://dx.doi.org/10.23857/dc.v7i4.2425

Barrera Barragán, C. G. (2019). Análisis de riesgos informáticos en las cooperativas de ahorro y crédito de los segmentos 2 y 3 en la ciudad de Ambato utilizando Cobit 5 [Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Maestría en Gerencia de Sistemas de Información]. Https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/29847

Bonilla Guerrero, J. V. (2021). Análisis de seguridad de la información aplicando la metodología NIST SP 800-30 y NIST 800-115 para la empresa textiles Jhonathex [Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos]. Https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/32301

Castro-Maldonado, J. J., & Villar-Vega, H. F. (2021). Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior. Revista modum, 3.

Clavijo Mera, M. E. (2015). Contraloría General del Estado informe de la EPM-GIDSA.pdf.

EPM-GIDSA. (2015a). Manual de políticas de buen uso de tecnología. Journal of

geotechnical and geoenvironmental engineering asce, 120(11), 1–31.

EPM-GIDSA. (2015b). Políticas y normativas (back ups).

EPMGIDSA. (2020). Estatuto organizacional de gestión por procesos. 1–42.

Escobar Sánchez, K. P., & others. (2022). Análisis de la capacidad de afrontamiento y de resiliencia de la población del cantón Chillanes, provincia Bolívar, en el terremoto de cumandá del 6 de septiembre del 2018. Quito, EC: universidad Andina Simón Bolívar, sede Ecuador.

Hubbard, D. W. (2020). The failure of risk management: Why it's broken and how to fix it. John wiley \ sons.

ISACA. (2018a). Norma Internacional ISO 31000. Administración/gestión de riesgos — lineamientos guía, 25. Https://auto-q-consulting.com.mx/muestra24.iatf.2020/norma.iso.31000.2018.espanol.pdf

ISACA. (2018b). Norma ISO 31000. 10. Https://www.isotools.org/pdfs-pro/ebook-ISO-31000-gestion-riesgos-organizaciones.pdf

ISACA. (2019). Objetivos de gobierno y gestión Cobit2019.

Jacqueline Cisneros-Caicedo, A. I., Jesús Urdánigo-Cedeño III, J., Fabián Guevara-García, a. I., & Enmanuel Garcés-Bravo, j. I. (2022). Técnicas e instrumentos para la recolección de datos que apoyan a la investigación científica en tiempo de pandemia techniques and instruments for data collection that support scientific research in pandemic times técnicas e instrumentos de coleta de dado. In núm. 1. Enero-marzo (vol. 8, pp. 1165–1185). Http://dominiodelasciencias.com/ojs/index.php/es/index

Jimbo Santana, P. R., & Cabrera Pantoja, K. L. (2021). Análisis comparativo de metodologías para el desarrollo de auditorías informáticas para organizaciones en el Ecuador considerando: análisis de riesgos, minería de datos, marcos de referencia y estándares y normas internacionales de estandarización. 1–117. Http://www.dspace.uce.edu.ec/handle/25000/25822

Katsikas, S. K. (2009). Risk management. In computer and information security handbook (pp. 605–625). Elsevier inc. Https://doi.org/10.1016/b978-0-12-374354-1.00035-2

Llontop Díaz, G. C. (2018). Gestión de riesgos de tecnologías de información de las empresas de Nephila networks.

Martínez, C. N. (2018). Propuesta de plan de continuidad de ti para el área de tecnologías de información y comunicación de Jasec. Tecnológico de Costa Rica.

Ríos, l. M. F. V.-m. F. (2021). Pequeñas y medianas empresas de Colombia.

Tejena-Macias, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo del conocimiento, 3(4), 230–244.

Velasco Trujillo, M. D. (2020). Análisis de riesgos informáticos aplicando la metodología OSSTMM para la Fundación Cultural y Educativa Ambato (Unidad Educativa Atenas) [Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos]. Https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/31786

Velásquez, J. P. R. (2021). Evaluación de la gestión de riesgos al sistema de información s/4 Hana en empresas del sector financiero Colombiano. 1–20.

Watson, David y Jones, a. (2013). Risk management. In digital forensics processing and procedures (pp. 109–176). Elsevier. Https://doi.org/10.1016/b978-1-59749-742-8.00005-4

5.4 Anexos

ANEXO 1: CLASIFICACIÓN DE RIESGOS

#	TIPO	DESCRIPCIÓN
R1	[N] Desastres Naturales.	N1 – Fuego
R2	[N] Desastres Naturales.	N2 - Daños por agua
R3	[N] Desastres Naturales.	N3 - Desastres Naturales (Terremotos, sunamis, erupciones volcánicas)
R4	[I] De Origen Industrial	I1 - Corte del suministro eléctrico
R5	[I] De Origen Industrial	I2 - Condiciones inadecuadas de temperatura o humedad
R6	[I] De Origen Industrial	I3 - Fallo de servicios de comunicaciones
R7	[I] De Origen Industrial	I4 - Desastres industriales
R8	[E] Fallos y errores no intencionados.	E1 - Fuga de información
R9	[E] Fallos y errores no intencionados.	E2 - Errores de los usuarios
R10	[E] Fallos y errores no intencionados.	E3 - Errores de re-encaminamiento
R11	[E] Fallos y errores no intencionados.	E4 - Errores del administrador
R12	[A] Ataque intencionados.	A10 - Acceso no autorizado
R13	[E] Fallos y errores no intencionados.	E6 - Pérdida de equipos
R14	[E] Fallos y errores no intencionados.	E7 - Vulnerabilidad de programas (software)
R15	[I] De Origen Industrial	I5 - Degradación de los soportes de almacenamiento de la información
R16	[E] Fallos y errores no intencionados.	E9 - Errores de secuencia

#	TIPO	DESCRIPCIÓN
R17	[E] Fallos y errores no intencionados.	E10 - Difusión de software dañino
R18	[E] Fallos y errores no intencionados.	E11 - Destrucción de información
R19	[E] Fallos y errores no intencionados.	E12 - Errores de mantenimiento / actualización de programas (software)
R20	[A] Ataque intencionados.	A11 - Interceptación de información (escucha)
R21	[E] Fallos y errores no intencionados.	E14 - Errores de mantenimiento / actualización de equipos (hardware)
R22	[E] Fallos y errores no intencionados.	E15 - Indisponibilidad del personal
R23	[E] Fallos y errores no intencionados.	E16 - Caída del sistema por agotamiento de recursos
R24	[E] Fallos y errores no intencionados.	E8 - Deficiencias en la organización
R25	[A] Ataque intencionados.	A1 - Denegación de servicio
R26	[A] Ataque intencionados.	A2 – Robo
R27	[A] Ataque intencionados.	A3 - Ataques destructivos
R28	[A] Ataque intencionados.	A4 - Extorsión
R29	[A] Ataque intencionados.	A5 - Ingeniería social
R30	[A] Ataque intencionados.	A6 - Suplantación de la identidad del usuario
R31	[A] Ataque intencionados.	A7 - Abuso de privilegios de acceso
R32	[A] Ataque intencionados.	A8 - Manipulación de equipos
R33	[A] Ataque intencionados.	A9 - Difusión de software dañino
R34	[E] Fallos y errores no intencionados.	E5 - Alteración accidental de la información

ANEXO 2: CATEGORIZACIÓN DEL RIESGO

AMENAZAS	VULNERABILIDADES	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
A1 - Denegación de servicio	Falta de mantenimiento y cumplimiento de vida útil	22	2,2	2,2	66
A10 - Acceso no autorizado	Políticas de acceso inadecuada	37,1	38	38	114
A11 - Interceptación de información (escucha)	Falencias en configuración de acceso a red interna	0,3	0,3	3	9
A2 - Robo	Inexistencia de políticas de acceso físico	21	0,2	21	63
A3 - Ataques destructivos	Inexistencia de políticas de acceso físico	32	3,15	6,2	96
A4 - Extorsión	Inexistencia de políticas de acceso lógico	2	2	2	6
A5 - Ingeniería social	Falta de capacitación al personal administrativo sobre ingeniería social	2	2	2	6

AMENAZAS	VULNERABILIDADES	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
A6 - Suplantación de la identidad del usuario	Falencias en configuración de acceso a red interna	16	16	16	48
A7 - Abuso de privilegios de acceso	Configuración inadecuada de acceso a activos	34	34	34	102
A8 - Manipulación de equipos	Falta de políticas de acceso físico y lógico	21	2	21	63
A9 - Difusión de software dañino	Antivirus desactualizado	11	11	11	33
E1 - Fuga de información	Incumplimiento en SSL	1,1	0,2	2	6
	Pérdida total o parcial de información por incontinencia verbal, medios electrónicos, papel	13,8	13,9	20,1	63
E10 - Difusión de software dañino	Fallas en el funcionamiento del software	11	11	11	33
E11 - Destrucción de información	No contar con respaldo de información	19	3,7	8,3	57
E12 - Errores de mantenimiento / actualización de programas (software)	Falta de capacitación (personal de administración)	11	11	11	33

AMENAZAS	VULNERABILIDADES	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
E14 - Errores de mantenimiento / actualización de equipos (hardware)	Falta de capacitación (personal técnico)	21	3,9	4	63
E15 - Indisponibilidad del personal	Ausencia accidental del puesto de trabajo	2	0,2	0,6	6
E16 - Caída del sistema por agotamiento de recursos	Carencia de recursos suficientes para un buen funcionamiento	22	11	11	66
E2 - Errores de los usuarios	Falta de capacitación en uso de activo	13,7	15	15	45
E3 - Errores de re-encaminamiento	Configuración errónea en red de datos	11,4	11,4	15	45
E4 - Errores del administrador	Funcionamiento erróneo del activo	36	36	36	108
E5 - Alteración accidental de la información	Falta de capacitación en uso de activo	9	19	9,9	57
E6 - Perdida de equipos	Falta de mantenimiento y cumplimiento de vida útil	22	2,2	21,1	66

AMENAZAS	VULNERABILIDADES	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
E7 - Vulnerabilidad de programas (software)	No existe una política formal de cambio de credenciales	11	11	11	33
E8 - Deficiencias en la organización	Acciones descoordinadas, errores por omisión	2	0,12	0,8	6
E9 - Errores de secuencia	Configuración de acceso a red inadecuado	6,8	15	6,7	45
I1 - Corte del suministro eléctrico	Falla en el funcionamiento del activo	20,5	2,1	2,1	61,5
I2 - Condiciones inadecuadas de temperatura o humedad	Mal funcionamiento de equipos de activo	20,5	2,1	2,1	61,5
I3 - Fallo de servicios de comunicaciones	Destrucción física de los activos de almacenamiento	2	0,2	0,2	6
	Imposibilidad de transmitir datos de un sitio a otro	2,1	0,9	0,3	6,9
I4 - Desastres industriales	Destrucción de activo debido a actividad humana	21,5	5,7	7,5	64,5
I5 - Degradación de los soportes de almacenamiento de la información	Avería o falla en el funcionamiento del activo	1	0,1	0,1	3
	Pérdida del activo	1	0,1	0,1	3

AMENAZAS	VULNERABILIDADES	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	IMPACTO
N1 - Fuego	Posibilidad de que el fuego acabe con el activo	22	2,2	2,2	66
N2 - Daños por agua	Posibilidad de que el agua acabe con el activo	21,5	2,1	2,1	64,5
N3 - Desastres Naturales	Pérdida del activo	21,5	2,1	2,1	64,5

La categorización del riesgo permite identificar el valor del impacto que puede tener un riesgo en base a las vulnerabilidades existentes en la EPM-GIDSA, el valor del impacto permitirá priorizar el riesgo a cuál se le debe ejecutar mayores controles.