UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

Maestría en
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

Opción de Titulación:

Proyecto de titulación con componentes de investigación aplicada y/o de desarrollo

Tema:

ANÁLISIS COMPARATIVO DE METODOLOGÍAS DE ANÁLISIS DE RIESGOS MAGERIT VS. NIST SP 800-30

Autora:

Zoila Victoria Monge LLiguicota

Director:

Rodolfo Xavier Bojorque Chasi

Cuenca – Ecuador
2023

Autora:

Zoila Victoria Monge LLiguicota
Ingeniera de Sistemas.
Candidata a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
zmonge@est.ups.edu.ec

Dirigido por:

Rodolfo Xavier Bojorque Chasi
Ingeniero de Sistemas.
Máster Universitario en Seguridad de las Tecnologías de la Información y Comunicación.
Máster Universitario en Ciencias y Tecnologías de la Computación.
Doctorado en Ciencias y Tecnologías de la Computación para Smart Cities.
rborque@ups.edu.ec

DEDICATORIA

Este trabajo está dedicado a todas las personas que, con su esfuerzo diario, contribuyen a hacer de nuestro mundo un lugar mejor. Quiero expresar mi amor y gratitud a mi querida madre, Rosa LLiguicota, quien, a pesar de la distancia, me lleva siempre en su corazón.

AGRADECIMIENTO

Mi agradecimiento más sincero a la Dirección Distrital 1401 Morona-Salud que me ha brindado la oportunidad de forjar mi carrera profesional, a la Universidad Politécnica Salesiana por constantemente estar en la vanguardia de la tecnología generando espacios de conocimiento; y finalmente mi agradecimiento especial al Ph.D Rodolfo Xavier Bojorque Chasi por su excelente calidad humana y ser la mejor guía en que este trabajo de titulación .

Tabla de Contenido

Análisis comparativo de Metodologías de Análisis de Riesgos Magerit vs. NIST SP 800-30

Autor:

Zoila Victoria Monge LLiguicota

Resumen

El presente trabajo se enfoca en el estudio comparativo de las metodologías de gestión de Riesgos MAGERIT y la NIST SP 800-30, que sirven para el análisis de los riesgos que se pueden generar por la utilización de las tecnologías de la información. Además, en este trabajo se busca la selección de la mejor metodología de gestión de riesgos a aplicarse en la Dirección Distrital 14D01 Morona-Salud para la identificación los riesgos asociados a sus operaciones.

Palabras clave:
Seguridad de la información, Metodología MAGERIT, Gestión de Riesgos.

ABSTRACT

The present work focuses on the comparative study of the risk management methodologies MAGERIT and NIST SP 800-30, which are used for the analysis of risks that can arise from the use of information technologies. In addition, this work seeks to select the best risk management methodology to be applied in the Dirección Distrital 14D01 Morona-Salud for identifying the risks associated with its operations.

Key words:

Information Security, MAGERIT Methodology, Risk Management.

INTRODUCCIÓN

A partir del inicio de la era digital las organizaciones han tenido que realizar grandes cambios en sus procesos tecnológicos, lo que conlleva asumir grandes riesgos en el área de seguridad de la información, considerando que la información representa hoy en día el valor más preciado de una organización y por ende debe contar con las medidas de seguridad adecuadas.

Por lo antes expuesto, la gestión de riesgos es uno de los elementos importantes, ya que incorpora como eje principal la prevención de sucesos de seguridad de la información como la divulgación, ingreso no autorizado, eliminación no autorizada, modificación y entre otros; sin importar la naturaleza de la información. De ahí radica la importancia que las organizaciones tengan claro a que amenazas se ven expuestos.

Cabe aclarar que la gestión de riesgos tiene dos enfoques, el generalista que se expresa mediante las metodologías y guías de buenas prácticas estipuladas en estándares como la ISO 31000:2009 o COSO;y a su vez existen enfoques específicos en cuanto seguridad para abordar el análisis de riesgos que reside en buscar el nivel de riesgo que la organización está soportando [1],con lo antes mencionado este trabajo pretende ayudar a las organizaciones a seleccionar la metodología que mejor se acopla a sus necesidades, cabe resaltar que prácticamente no existen datos sobre las metodologías en las diferentes empresas puesto que se trata de información confidencial, lo cual dificulta más el análisis entre las metodologías. Sin embargo, se conoce de la existencia de muchas metodologías que permiten a las organizaciones realizar el análisis riesgo tales como MAGERIT, Metodología de Análisis y Gestión de Riesgos de los sistemas de información [2], ISO / IEC 27005: 2008[3], siendo la norma que aporta directrices para la gestión de riesgos de seguridad de la información , NIST SP 800-30 [4], (National Institute of Standards and Technology) es la guía de gestión de riesgo para sistemas de tecnología de la información y se caracteriza por la gestión de riesgos en proyectos de TI, Mehari[5] es un modelo cuantitativo y cualitativo de gestión de

riesgos y OCTAVE[6] (Operationally Critical Threat Asset, and Vulnerability Evaluation), modelo se centra en la evaluación de los riesgos de la seguridad de la información asociados a la empresa , las cuales desde sus soluciones brindaran instrumentos para decidir en cuanto a evaluar el riesgo, se ha podido revisara como las diferentes metodologías llevan a cabo el cálculo del impacto mediante las diferentes perspectivas tanto cualitativas como cuantitativas.

Serrano y Salazar [7] presentan la metodología para evaluar los riesgos en hospitales públicos de Ecuador, en donde que MAGERIT es la opción sobresaliente para las organizaciones que deciden iniciar la gestión de seguridad en sus activos de información.

MARCOS DE REFERENCIA / FASES	NIST SP 800-30	OCTAVE ALLEGRO	MAGERIT V3.0
Caracterización del Sistema	X	X	X
Identificación de la amenaza	X	X	X
Identificación de la vulnerabilidad.	X	X	
Análisis de control	X	X	X
Determinación de la probabilidad	X	X	X
Análisis de impacto	X	X	X
Determinación del riesgo	X	X	X
Recomendaciones de control	X	X	
Documentación resultante	X		
Establecimiento de parámetros		X	X
Necesidades de seguridad			X

Tabla 1. Análisis comparativo de marcos de referencia para análisis de riesgo.
Fuente:[8]

En un caso de estudio [8] realizado sobre la evaluación y el análisis de riesgos de seguridad informática por medio del monitoreo del tráfico de red local, se estableció un análisis comparativo de marcos de referencia de las diferentes metodologías según se puede observar en la tabla 1, que NIST SP 800-30 es la mejor metodología que se adapta a los requerimientos de la organización estudiada.

Los estudios mencionados previamente se basan en el empleo de metodologías destinadas a la creación de herramientas que posibiliten la localización de vulnerabilidades, riesgos y amenazas en el ámbito de la seguridad de la información, con el propósito de salvaguardar la integridad de los datos y sistemas informáticos

1. Determinación del Problema

1.1 Antecedentes del Problema

Las entidades gubernamentales y organizaciones actualmente se enfrentan a grandes avances tecnológicos lo que les ha obligado que sus procesos se automaticen en pro de brindar un mejor servicio acorde con la misión y visión de cada empresa o institución. Al hablar de estos cambios, se asume similares riesgos que no son analizados a profundidad considerando el activo con mayor valor hoy en día para las empresas que es la información, la cual constantemente está siendo amenazada, ya sea en su integridad, disponibilidad y confidencialidad por parte de delincuentes informáticos que se aprovechan de las vulnerabilidades existentes. Según la publicación de 2022 realizada por IBM "IBM X-Force Threat Intelligence Index", en donde se exponen los sectores de la industria que experimentaron un aumento significativo en la incidencia de ataques, la extracción de información y las pérdidas sustanciales de datos durante el período que abarca desde 2020 hasta 2021.

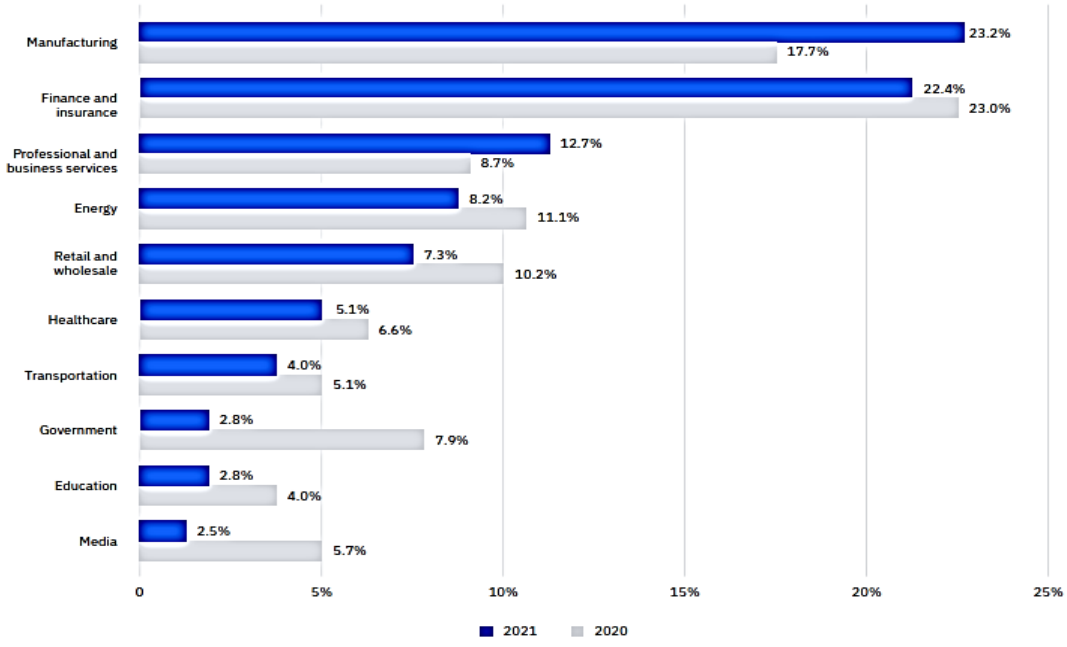

Figura 1. Ranking de sectores de la Industria con ciberataques fuente: [9]

Como se puede observar en la figura 1 para los servicios profesionales y el manufacturero en el 2021, se ha incrementado los ataques, por tal razón es esencial la protección de los activos de las empresas.

En el caso de la Dirección Distrital 14D01 Morona-Salud en el periodo de 2020 al 2021, se reportó una serie de ataques informáticos que se caracterizaron por su sofisticación y su impacto significativo. Por ejemplo, el servidor de correo electrónico del Distrito fue objeto de ataques dirigidos. Los atacantes enviaron correos electrónicos maliciosos a los usuarios del sistema, que contenían archivos adjuntos o enlaces a software malicioso. Al abrir estos archivos o hacer clic en los enlaces, los usuarios inadvertidamente permitían que los atacantes accedieran a sus cuentas de correo electrónico. Posteriormente, los atacantes utilizaron estas cuentas comprometidas para enviar correos maliciosos a otros usuarios.

1.2. Formulación del Problema

En la actualidad, existen diversas metodologías de gestión de riesgos que nos brindan la posibilidad de realizar un análisis y evaluación exhaustivos de los riesgos asociados a los sistemas de información y los activos que se ven involucrados directamente o indirectamente implicados en el procesamiento de datos en entornos empresariales; además estas herramientas tienen como línea base los conceptos de confidencialidad, disponibilidad e integridad para el manejo de la información. Por tal razón cabe plantearse para el estudio ¿Qué metodología de gestión riesgos, es adaptable, para la realización de una guía para el análisis y evaluación de riesgos de los activos de información de la Dirección Distrital 14D01 Morona-Salud?

1.3. Descripción del Problema

En la Dirección Distrital 14D01 Morona-Salud la falta de un proceso gestión de seguridad de la información conlleva que no se pueda garantizar la seguridad informática y así se vea comprometida la integridad, confiabilidad y

disponibilidad de la información. Hoy en día el despliegue de la plataforma tecnológica de la Dirección Distrital 14D01 Morona-Salud involucra información sensible, como: registros de historial clínico de los pacientes, procesos de adquisición de compras públicas, uso de correo institucional y entre otros servicios web que se utiliza en la institución mediante Internet, lo cual significa que está expuesta a ataques informáticos. Por tal razón el presente trabajo, se basa en elegir una metodología de riesgos que mejor se ajuste a las necesidades y los requerimientos de los activos de la información de la Dirección Distrital 14D01 Morona-Salud para la protección de la información.

2. Marco teórico referencial

En la actualidad las empresas están conscientes de la importancia del tratamiento de los riesgos, debido al aumento de la cantidad de casos de sucesos relacionados con la seguridad de los sistemas de información que ponen en riesgo los activos de las organizaciones [10], pero por lo general, la falta de una buena orientación en metodologías a utilizar es un factor relevante que determina la continuidad del negocio o cierre del mismo.

A continuación, se exponen conceptos básicos que engloban la seguridad de la información, seguridad informática, ciberseguridad, los activos de la información y de los procesos a seguir en el análisis y evaluación de riesgos de las metodologías MAGERIT y NIST SP 800-30.

2.1 Seguridad de la información, seguridad informática y ciberseguridad.

La seguridad de la información es la disciplina responsable de garantizar la confidencialidad, integridad y disponibilidad de la información mediante el diseño, implementación y utilización de reglas, metodologías, procedimientos y técnicas para contribuir en la gestión y defensa de la información de los sistemas de una organización. [11]

La seguridad informática se centra únicamente en la protección de la infraestructura y redes mediante la ejecución táctica y operacional de seguridad de la información de una organización. [11]

La ciberseguridad no es más que el conjunto de prácticas o estrategias apoyadas en tecnologías, ya sea para defender y/o proteger la información digital de los sistemas conectados entre sí de posibles ciberataques [12].

2.2. Activos de la información.

Los activos de la información son las pertenencias con los que cuenta la organización para llevar a cabo sus actividades diarias computacionales, estos se clasifican de la siguiente manera:

- La información: es un activo que se representa de varias formas escrita, impresa, electrónica, transmitida por correo o utilizando medios electrónicos o mediante el dialogo en un chat [13].
- Los equipos que soportan información: son la parte de hardware que posibilitan el almacenamiento y procesamiento de la información de la organización, entre estos tenemos: los servidores, computadores, portátiles, routers y switches.[14]
- Los programas o aplicaciones: en esta categoría intervienen todo lo que se conoce como software libre o comercial que se encuentra instalado en el hardware de la institución que facilita el procesamiento de la información siendo estos los sistemas operativos, programas, etc. [14]
- Los usuarios: son los individuos que de acuerdo a sus roles y responsabilidades utilizan la infraestructura tecnología de la organización, partiendo desde la alta dirección, líderes de procesos, operativos y usuarios externos. [14]
- Las instalaciones físicas: conciernen a los departamentos administrativos, cuartos de comunicaciones, y salas de reunión en fin toda la infraestructura física que forma parte de la organización. [14]
- El equipamiento auxiliar: Son dispositivos que apoyan los sistemas informáticos. [14]
- Los datos informatizados: Se refiere a la información acumulada en un archivo digital, sistemático o medio informático. [14]
- Las redes de Comunicaciones: Son aquellas interconexiones que permiten el intercambio de información ya sea dentro o fuera de la organización. [14]

- Servicios: Son las funciones que prestan los sistemas informáticos y de comunicaciones de la entidad, mediante las cuales se satisfacen la necesidad de los servidores. [14]

2.3. Gestión de Riesgos de la información

Partiendo que ya se tienen identificados de manera precisa cuáles son los riesgos que posee la entidad, como siguiente paso en la gestión de riesgos se debe establecer las medidas de defensa a implementar en la organización.

Las medidas de protección tienen que presentar un equilibrio entre el valor de la protección y el coste de exposición. Ya que de lo contrario no tendría sentido que el coste de proteger sea mayor que la materialización de una amenaza. Además, hay que considerar que uno de los elementos usados para identificar este coste se basa en que tan importante es el activo para la continuidad operacional de la empresa o entidad. En la gestión de riesgos intervienen dos conceptos que son el Análisis de Riesgos y Tratamiento (figura 2).

- Análisis de Riesgos. –Sirve para identificar a que amenazas está expuesta la empresa y valorar que podría suceder o la probabilidad de ocurrencias de las mismas.

- Tratamiento. –Ya conociendo los riesgos la empresa tiene la facultad de tratarlos, ya sea con la finalidad de evitar/eliminar, reducir/mitigar, transferir o aceptar el riesgo detectado.

Figura 2. Gestión de Riesgos Fuente: [15]

2.4. Análisis de Riesgos de la información

En la etapa de análisis de riesgos se deberá valorar todas las amenazas e identificar los riesgos más notables para la organización. Considerando que para los riesgos de será necesario realizar un plan de mitigación, en el que se empleen controles o mejoras de los ya existentes para reducir el nivel de riesgo de aquellos activos determinados previamente como críticos. En esta sección se tiene presente elementos claves para el análisis de riesgos como son los activos, los ataques que no son más que acontecimientos que pueden afectar a los activos y por último las salvaguardas que son medidas de protección contra las amenazas que posibilitan el normal desarrollo de actividades de la organización. Además, existen dos criterios de gran importancia: a) el impacto que podría darse ante un determinado riesgo y b) la probabilidad de ocurrencia del riesgo.

2.5. Evaluación de Riesgos de la información.

En esta etapa nos centraremos en deducir el nivel del riesgo dado por la valoración del impacto de un activo y el nivel de vulnerabilidad. La evaluación generalmente está relacionada a una metodología específica de análisis de riesgos, donde para cada organización se puede matizar la evaluación de acuerdo a las características propias del negocio.

2.6. Metodologías de Riesgos de la información.

La intención del presente proyecto es proporcionar un marco de toma de decisiones entre las metodologías más reconocidas (Magerit y NIST SP 800-30) que permita que el Sistema de Gestión de Seguridad de la Información (SGSI) de la organización tenga un mecanismo definido de gestión del riesgo, para ello es necesario que las

organizaciones comprendan que deben saber evaluar cualitativa y cuantitativamente la medida de madurez en materia de seguridad, esto de la mano de metodologías propuestas , con énfasis particular en la evaluación inicial que se conoce como el Gap Analysis o “Análisis de Brecha” y en función de este análisis se mide el riesgo para determinar la declaración de aplicabilidad.

MAGERIT: es una metodología que se dedica a la investigación y análisis de los riesgos, es capaz de suministrar medidas apropiadas que usarán para controlar y minimizar estas inseguridades. [16]

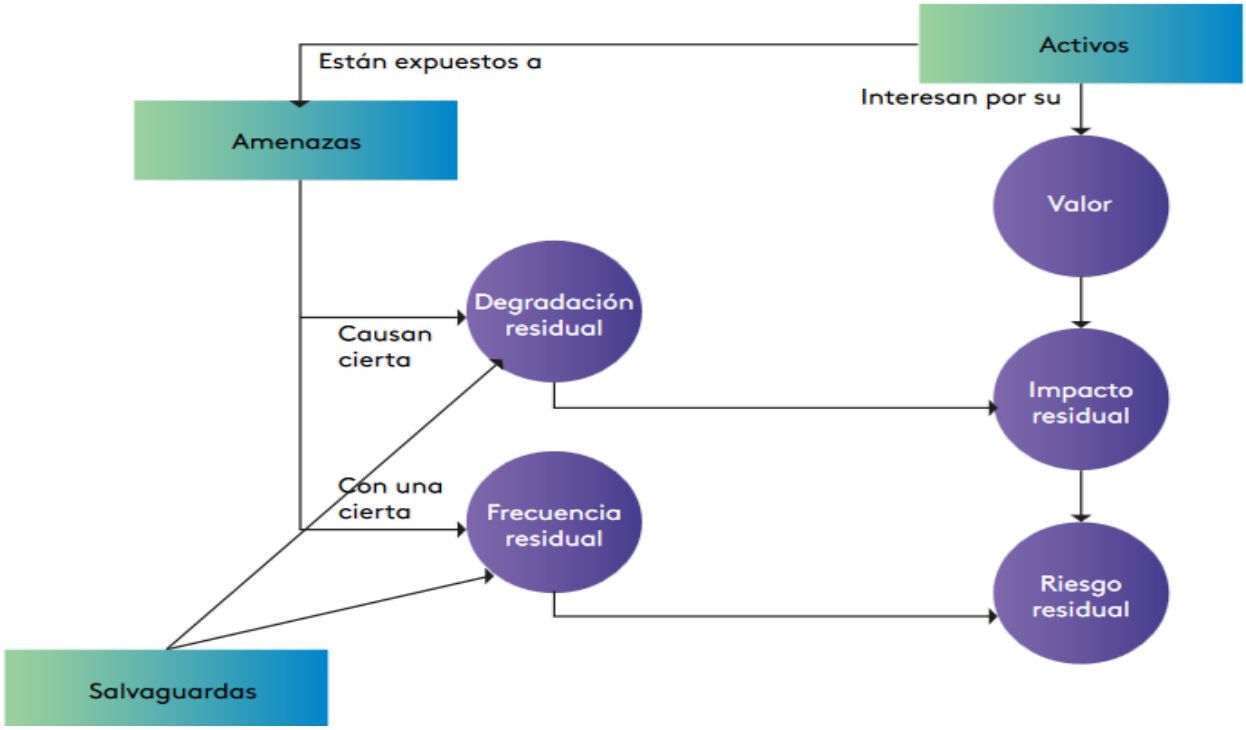

Figura 3. Diagrama de flujo de Magerit Fuente: [17]

Como se puede observar en la figura 3, la metodología de gestión de riesgos Magerit se describe de la siguiente manera:

3. Se inicia con el inventario de los activos de acuerdo al catálogo definido por la metodología.

1 Se determinan el valor de cada activo con su respetiva justificación del coste que representa para la organización.

2 Se establece la valoración de las amenazas según su frecuencia o degradación residual.

3 Se realizar el análisis de los riesgos en donde mediante el impacto residual se obtiene el riesgo residual.

4 Finalmente se fijan las medidas de mitigación o salvaguardas con la finalidad de minimizar los riesgos.

NIST SP 800-30: es una guía elaborada, por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, cuyo propósito es la gestión de riesgos de sistemas de tecnología de la información. Esta guía propone una serie de recomendaciones y actividades dirigidas a la administración de riesgos en la empresa. [18]

La metodología NIST SP 800-30 consta de nueve actividades:

- Caracterización de los sistemas, en donde se define el alcance y los temas estratégicos de la evaluación de riesgos de la organización.
- Identificación de amenazas, en la cual se establecen los orígenes para el monitoreo de las mismas.
- Identificación de vulnerabilidades, aquí se tienen un directorio de debilidades del sistema de información que podrían tener la posibilidad de ser explotadas por una amenaza.
- Análisis de controles, se tiene una lista de los controles actuales.
- Determinación de la probabilidad, se encarga de dar a conocer las polaridades existentes de acuerdo a un rating.
- Análisis de impacto, evalúa el impacto de acuerdo a tres criterios confidencialidad, disponibilidad e integridad.
- Determinación del riesgo, brinda la posibilidad de evaluar los niveles de riesgo y el riesgo como tal.

- Recomendaciones de control, en el cual se facilitan los controles que podrían ayudar a reducir el riesgo.

- Documentación de resultados, consiste en el reporte.

3. Dirección Distrital 14D01 Morona-Salud.

Con acuerdo Ministerial 00019 – 2020, publicado en el Registro Oficial No. 641 de 5 de junio, se expresa que se mantienen las 9 Coordinaciones Zonales de Salud que actualmente se encuentran en el territorio nacional, y se suprimen algunas Direcciones Distritales de Salud y se crea varias Oficinas Técnicas, derivando de esto la eliminación de la Dirección Distrital 14D02 Palora-Huamboya-Pablo VI quedando a cargo de la Dirección Distrital 14D01 Morona-Salud como Oficina Técnica 14D02.[19]

La Dirección Distrital 14D01 Morona-Salud absorbe a Oficina Técnica 14D02 y sus establecimientos de salud y entró en un proceso de grandes transformaciones de tipo tecnológico, administrativo y financiero impulsado por políticas de estado, solicitando para ello desplegar mecanismos que garanticen la eficiencia y productividad en su gestión como institución pública con calidad y calidez en la prestación de sus servicios de salud.

La Dirección Distrital 14D01 Morona-Salud es una Entidad Desconcentrada del Ministerio de Salud Pública que, a través de sus 30 establecimientos de salud, una unidad móvil de pronta respuesta y un puesto de salud en el Centro de Privación de la libertad de Macas brinda servicios de salud con calidad y calidez a la población, desarrollando acciones orientadas a la promoción de la salud, prevención de enfermedades, recuperación de la salud, rehabilitación y cuidados paliativos. Además, se brindan atención de urgencia y emergencia, se garantizan una referencia, derivación, contrarreferencia y referencia inversa adecuada.

Misión

El Ministerio de Salud Pública, ejercerá plenamente la gobernanza del Sistema Nacional de Salud, con un modelo referencial en Latinoamérica que priorice la promoción de la salud y la prevención de enfermedades, con altos niveles de atención de calidad, con calidez, garantizando la salud integral de la población y el acceso universal a una red de servicios, con la participación coordinada de organizaciones públicas, privadas y de la comunidad.

Visión

Ejercer la rectoría, regulación, planificación, coordinación, control y gestión de la Salud Pública ecuatoriana a través de la gobernanza y vigilancia y control sanitario y garantizar el derecho a la Salud a través de la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, investigación y desarrollo de la ciencia y tecnología; articulación de los actores del sistema, con el fin de garantizar el derecho a la Salud.[20]

3.1 Estructura Organizacional de la Dirección Distrital 14D01 Morona - Salud.

La Dirección Distrital 14D01 Morona-Salud es una entidad desconcentrada, pero forma parte de la coordinación Zona6 de Salud según la estructura organigrama definida por el Ministerio de Salud Pública como se puede observar en la figura 4.

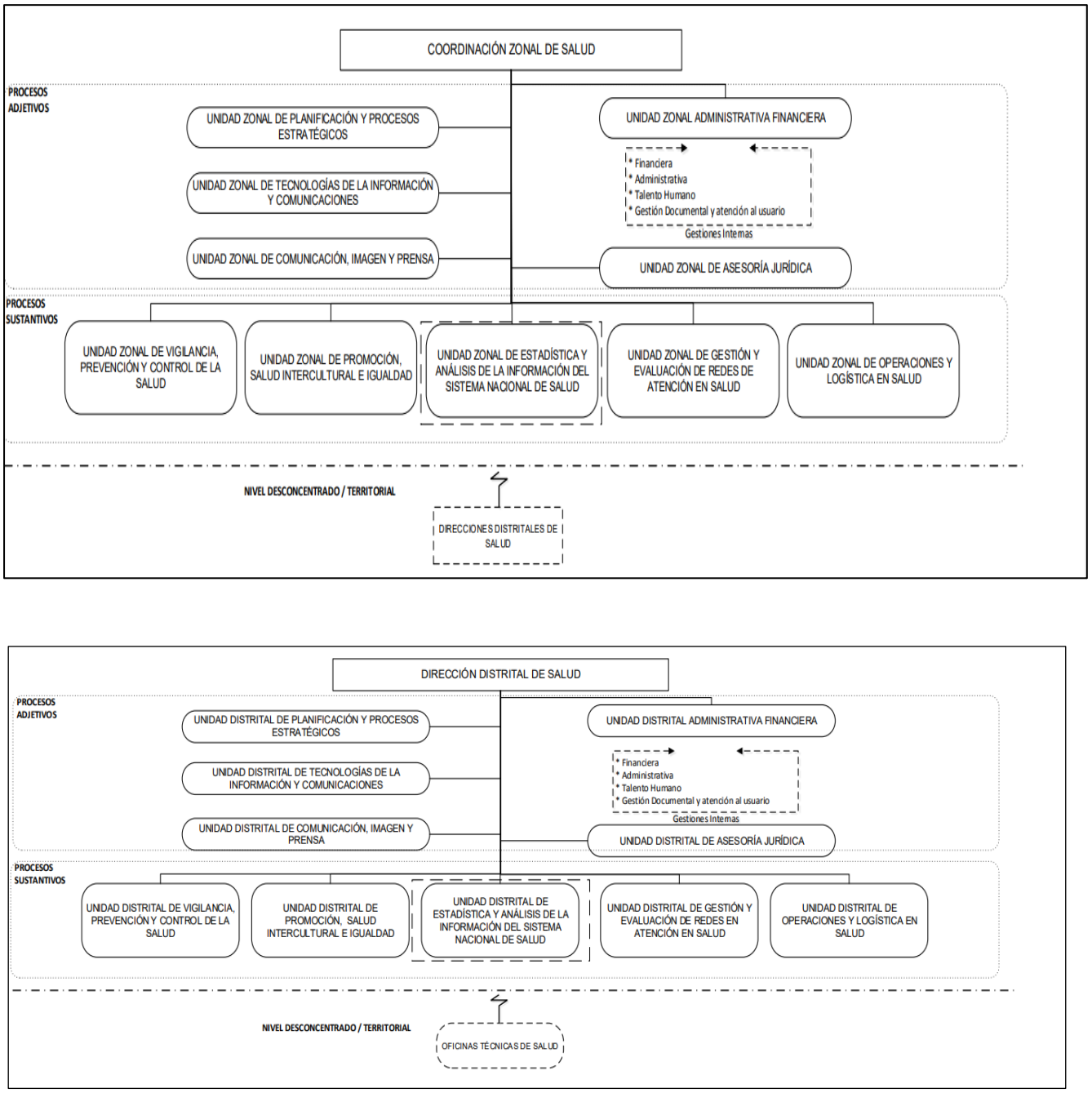

Figura 4. Estructura orgánica de la Dirección Distrital 14D01 Morona-Salud. [20]

Procesos Sustantivos: Son conocidos como los procesos agregadores de valor o los responsables de generar y administrar los productos y/o servicios orientados a los usuarios internos y externos; permitiendo así el desempeño de los objetivos estratégicos establecidos por la institución.

Procesos Adjetivos: Son aquellos que brinda asesoría y apoyo a los procesos gobernantes, sustantivos y para sí mismos, contribuyendo a la gestión institucional.

3.2 Identificación de activos de la Institución.

La identificación de los activos de la Dirección Distrital 14D01 Morona-Salud se ha considerado los procesos adjetivos y sustantivos.

Tipo de Activo	Proceso	Nombre activo	Descripción del activo.
Información	Dirección	Oficios, Memorandos, Circulares y Resoluciones.	Documentación remitida por la Dirección Distrital.
		Archivos de gestión del despacho de la dirección.	Documentos Físicos que forman parte del archivo de gestión.
	Asesoria Jurídica	Archivos de gestión del departamento de Asesoría Jurídica.	Documentos Físicos que forman parte del archivo del área Jurídica.
		Procesos Jurídicos.	Expedientes de procesos judiciales.
	Adminsitrativo Financiero	Inventarios	Documentación de ingresos y egresos de insumos médicos, insumos de laboratorio, dispositivos médicos y existencias en general.
		Contratos	Documentos de contratación pública.
		Archivos de gestión del área administrativa financiera (Talento humano, Adminis-trativo, Financiero).	Documentos físicos que forman parte de la gestión Administrativa Financiera

	Tecnologías de la Información y las Comunicaciones.	Manuales de usuario de los sistemas de información.	Documentación de los manuales de usuario y administración de los sistemas de información del distrito.
		Archivos de gestión del área de Tecnologías de la Información y las Comunicaciones.	Documentación física que forman parte de la gestión.
	Comunicación imagen y prensa.	Archivos de gestión del área de Comunicación imagen y prensa.	Documentos físicos que forman parte de la gestión.
	Planificación y procesos estratégicos.	Archivos de gestión del área de Planificación y procesos Estratégicos	Documentación en forma física que forman parte de la gestión.
	Vigilancia y Control de la salud	Archivos de gestión del área de Planificación y procesos estratégicos	Documentos físicos que forman parte de la gestión.
	Promoción, Salud Intercultural e Igualdad	Archivos de gestión del área de Planificación y procesos estratégicos	Documentos físicos que forman parte de la gestión.
	Estadística y Análisis de la Información del Sistema Nacional de Salud.	Archivos de gestión del área de Estadística y Análisis de la Información del Sistema Nacional de Salud.	Documentos físicos que forman parte de la gestión.
	Gestión en Atención de Redes en Atención de Salud.	Archivos de gestión del área de la Gestión en Atención de Redes en Atención de Salud.	Documentos físicos que forman parte de la gestión.
	Operaciones y logística de Salud.	Archivos de gestión del área de Operaciones y logística de Salud.	Documentos físicos que forman parte de la gestión.
Datos informatizados	Tecnologías de la Información y las Comunicaciones.	Base de datos.	Se refiere al conjunto de datos almacenados en la una base de datos

	Todos los procesos administrativos y agregadores de valor.	Backup de los datos.	Se refiere a todos los respaldos o copias de seguridad que se guardan en dispositivos de almacenamiento de información.
Servicios	Tecnologías de la Información y las Comunicaciones.	Servicio de DHCP.	Servicio que se entrega para la asignación de direcciones IP a los equipos que se conectan al servidor de la institución.
		Servicio de DNS.	Servicio que se brinda para resolución de nombres de dominio del servidor de la institución.
	Todos los procesos administrativos y agregadores de valor.	Servidor WEB	Servicio que acceden los funcionarios de la institución.
Programas o aplicaciones	Todos los procesos administrativos y agregadores de valor.	Antivirus	Programa que detecta virus informáticos y los elimina, protege el servidor y equipo de cómputo de la institución.
		Herramientas de ofimática y utilitarios.	Programas de ofimática tales como procesadores de texto, hojas de cálculo entre otros para facilitar el trabajo a los funcionarios en sus actividades diarias.
		Sistemas Operativos para computadoras de escritorio y portátiles.	Sistemas Operativos para computadoras de escritorio y portátiles de la institución.
	Tecnologías de la Información y las Comunicaciones.	Sistema operativo del servidor.	Sistema operativo del servidor de la institución.
Hardware	Todos los procesos administrativos y agregadores de valor.	Computadoras de escritorio.	Computadoras de escritorio de la institución.

		Portátiles	Equipo portátil de la institución.
		Impresoras	Impresoras de la institución.
		Escaneres	Escaneres de la institución.
	Tecnologías de la Información y las Comunicaciones.	Equipo servidor	Equipo informático capaz de proveer servicios a sus clientes a través de la red establecida.
		Router	Dispositivo que permite la interconexión de computadores de la entidad.
		Switches	Conmutador que permite la interconexión de computadores de la entidad.
Redes de Comunicaciones	Todos los procesos administrativos y agregadores de valor.	Central Telefónica Analógica.	Equipo de conmutación para las llamadas telefónicas entrantes y salientes en la institución.
		Red de área local	Red Local que conecta uno o más ordenadores dentro de la institución.
	Proveedor de internet	Red de internet	Infraestructura de red de proveedor para brindar el servicio de internet
Soportes de Información.	Todos los procesos administrativos, agregadores de valor y Tecnologías de la Información y las Comunicaciones.	Discos duros extraíbles portables.	Dispositivo de almacenamiento de copias de seguridad de información de la entidad.
		Discos CD y DVD.	Discos para almacenamiento digital de archivos, imágenes, sonido y de la información en general de las diferentes áreas.

		Memorias USB	Dispositivo USB para el almacenamiento digital de archivos, imágenes, sonido y de la información en general de las diferentes áreas.
Equipamiento auxiliar	Todos los procesos administrativos, agregadores de valor y Tecnologías de la Información y las Comunicaciones.	UPS	Dispositivo que se encarga de almacenar energía para durante un apagón suministrar energía a los ordenadores conectados a él.
		Equipos de climatización.	Sistema que revisa el nivel la temperatura las oficinas y cuarto de Comunicaciones.
		Equipos de extinción de incendios.	Conjunto de extintores de incendios.
		Cableado de red.	Cableado de red de la institución.
		Fibra óptica	Cableado de fibra óptica.
Instalaciones físicas	Todos los procesos administrativos, agregadores de valor y Tecnologías de la Información y las Comunicaciones.	Cuarto de Comunicaciones.	Ubicación donde se encuentran todo el equipamiento de comunicaciones como: router , switch ,central telefonica ,etc ;para la transmisión de voz y datos .
		Oficinas	Lugar de trabajo de los funcionarios.
Usuarios	Todos los procesos administrativos y agregadores de valor.	Funcionarios	Personal que labora en la institución.
		Contratistas y Terceros.	Personal que prestan sus servicios a la institución.
		Público en general.	Usuarios externos a la institución

	Tecnologías de la Información y las Comunicaciones.	Administradores del Sistema.	Personal que se encarga de la administración de los sistemas de información de la entidad.

Tabla 2. Identificación de activos Fuente: Autor.

Con el inventario de activos de la institución, se procederá a examinar cuál de las dos metodologías revisadas: MAGERIT y NIST SP800-30, están acorde con los activos de información y a los requisitos de seguridad de información que requiere el distrito.

3.3 Tabla comparativa de las Metodologías de Riesgos de la información.

En esta sección se compararán las metodologías de riesgos: Magerit y Nist PS 800-30 de acuerdo a las ventajas y desventajas que cada una de ellas.

Metodología	Ventajas	Desventajas
MAGERIT	• Se enfoca netamente en el análisis de riesgos del sector público, pero puede adaptarse a organizaciones privadas. • Posee una amplia documentación sobre los tipos de activos y amenazas. • Es una metodología que se encuentra abierta al público. • Separa los activos en grupos para identificar sus amenazas y establecer salvaguardas. • Permite realizar un análisis de riesgo cuantitativo y cualitativo.	• No contempla el monitoreo dentro sus fases. • Su implementación requiere una inversión considerable.

	• Sirve de ayuda a la organización para llevar a cabo los procesos de auditoría, certificación o acreditación. • Tiene la capacidad de traducir el riesgo en valores económicos, lo cual facilita la toma de decisiones en la organización. • Tiene una herramienta de análisis de riesgo denominada PILAR, la cual facilita su aplicación. • Contempla los objetivos de seguridad de la información: privacidad, integridad, disponibilidad, legitimidad y trazabilidad.	
NIST SP 800-3O	• Está orientada para el análisis de riesgos de la seguridad de la infraestructura Tecnologías de la Información (TI). • Posee un listado de elementos importantes para las pruebas de seguridad técnica y la evaluación. • Posee herramientas para la valoración y mitigación de inseguridades. • Vela por los sistemas informáticos que procesan, almacenan y transmiten la información.	• Dentro de su modelo no se consideran los activos.

Tabla 3. Comparativa de metodologías de riesgos: Magerit y Nist PS 800-30 [21].

De acuerdo a la tabla 2, en la metodología Magerit, que dentro de todas las ventajas la que se resalta es que poseen un mayor número de objetivos de seguridad de la información a comparación de NIST SP 800-30 que tiene la triada de la seguridad: disponibilidad, integridad y confiabilidad, y que decir sobre el tratamiento de los riesgos que igual esta ofrece.

4. MATERIALES Y METODOLOGÍA

Este estudio parte del método analítico con enfoque cualitativo para el análisis de las referencias, las mismas nos permitirán establecer las ventajas y desventajas de los modelos para la gestión de la información de las diferentes metodologías.

Posteriormente se aplicará el método comparativo para el análisis de las metodologías de riesgos Magerit y NIST SP 800-30, realizando una matriz centrada en el análisis propuesto, además con la ayuda de ciclo de Deming "Plan Do Check Act" (PDCA), pero solo nos enfocaremos en "Planear" y "Hacer" como se muestra el figura 4., para llegar a obtener conclusiones más sólidas.

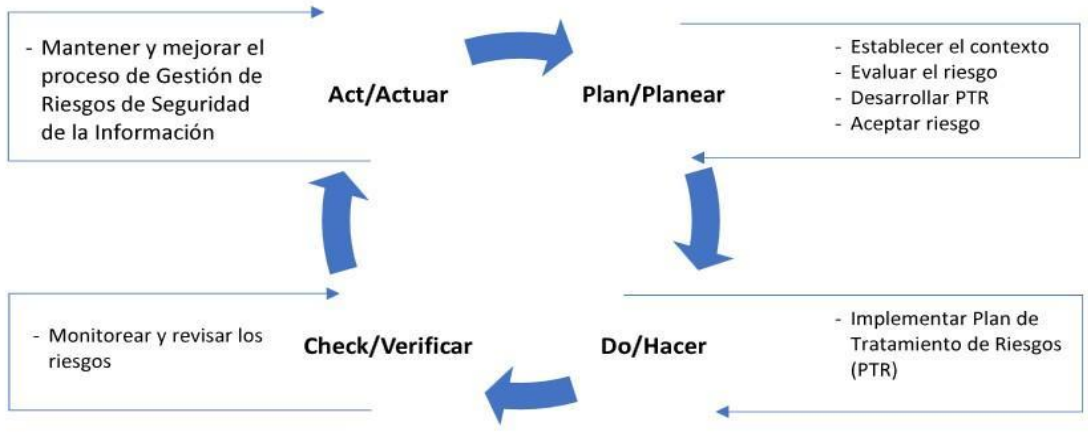

Figura 4. Análisis de riesgos en el ciclo PDCA del SGSI. Fuente: [22]

En base al conocimiento recopilado se establecerán los lineamientos que las empresas deberían considera al momento de realizar la selección de una metodología.

Finalmente se propone la aplicación de la metodología seleccionada en la Dirección Distrital 14D01 Morona-Salud en la cual se aplicarán las fases de gestión de riesgos.

5. Resultados y discusión

En este aparatado se llevará a cabo el desarrollo dos las metodologías de riesgos propuestas. Primero se procederá con la Metodología para el análisis de Riesgos es Magerit y para luego complementar el estudio en la NIST SP 800-30.

5.1. Metodología Magerit

A continuación, se iniciará definiendo los criterios de evaluación y luego se desarrollarán las etapas siguientes de análisis de gestión de riesgos.

5.1. 1 Parámetros de Evaluación.

La tabla 4, presenta por niveles los valores monetarios que tendrá cada activo de acuerdo al rango fijado.

Nivel	Abreviatura	Valor	Rango
Muy alto	MA	75000 $	Entre 50001 $ y 75000 $
Alto	A	50000 $	Entre 30001 $ y 50000 $
Medio	M	30000 $	Entre 10001 $ y 30000 $
Bajo	B	10000 $	Entre 1001 $ y 10000 $
Muy bajo	MB	1000 $	Entre 100 $ y 1000 $

Tabla 4. Valoración de Activos.

En la tabla 5, se realiza la categorización de la vulnerabilidad de acuerdo al nivel de frecuencia que se espera que ocurra los eventos o situaciones específicas.

Nivel	Abreviatura	Valor	Descripción
Extremadamente frecuente	EF	0,9973	1 vez cada día
Muy frecuente	MF	0,1425	1 vez cada semana
Frecuente	F	0,0329	1 vez cada mes
Frecuencia normal	FN	0,0055	1 vez cada 6 meses
Poco frecuente	PF	0,0027	1 vez al año

Tabla 5. Clasificación de la vulnerabilidad.

La valoración de impacto se clasifica según la relevancia de ciertos factores eventos o situaciones como se demuestra en la tabla 6.

Nivel	Abreviatura	Valor
Crítico	C	90%
Alto	A	75%
Medio	M	50%
Bajo	B	20%

Tabla 6. Valoración del impacto.

En la implementación de acciones concretas para reducir tanto las posibles consecuencias negativas de un evento de seguridad como las oportunidades que los atacantes pueden aprovechar para explotar debilidades en el sistema se puede observar en la tabla 7.

Nivel	Abreviatura	Valor
Alta	A	90%
Media	M	60 %
Baja	B	30 %
Nula	N	0%

Tabla 7. Disminución del impacto y de la vulnerabilidad

La tabla 8, presenta una clasificación de riesgos en cinco niveles diferentes: Muy alto, Alto, Medio, Bajo y Muy bajo. Cada nivel tiene una abreviatura correspondiente para facilitar su identificación en la documentación y un valor que representa una estimación del impacto económico que podría tener la materialización de un riesgo en ese nivel. Además, se proporciona un rango de valores para cada nivel que especifica el rango de pérdidas económicas esperadas.

Nivel	Abreviatura	Valor	Rango
Muy alto	MA	100000 $	Entre 70001 $ y 100000 $
Alto	A	70000 $	Entre 50001 $ y 70000 $
Medio	M	50000 $	Entre 1001 $ y 50000 $
Bajo	B	1000 $	Entre 101 $ y 1000 $
Muy bajo	N	100 $	Entre 1 $ y 100 $

Tabla 8. Nivel del riesgo.

Justificación de los Activos: En la tabla 9 se expone el valor final que tomará cada activo en base al valor parcial (valor de reposición, configuración, uso y pérdida); además se establece los valores para cada parámetro, teniendo como resultado el valor a considerar con relación a la valoración de los activos.

Grupo	Descripción	Valoración cuantitativa	Valoración cualitativa	Valor de reposición	Valor de uso	Valor de configuración	Valor de pérdida	Valor final	Valor a considerar
[P] Personal	Administrador de sistemas	75000 $	MA	40000 En caso de ausencia definitiva, el sistema completo quedaría sin soporte	0	0	10060 Se considera el valor de sueldo de un día, más las actividades que se estancarían por su ausencia.	50060	75000
[P] Personal	Funcionarios	10000 $	B	10000 En caso de ausencia definitiva, el sistema completo quedaría sin soporte	0	0	1000 Se considera el valor de sueldo de un día, más las actividades que se estancarían por su ausencia.	10000	10000
[COM] Redes comunicaciones	Red de internet	10000 $	B	0	5500 Considerando que se manejan procesos internos en base a la asistencia	0	0	5500	10000

[COM] Redes comunicaciones	Red de área local	10000 $	B	2000 Valor que cubre cableado estructurado	3500 Considerando que se manejan procesos internos en base a la asistencia.	500 Se toma en cuenta el trabajo interno del personal de TICs	3000 Aunque habrían grandes pérdidas, se priorizaría en reparar la conectividad de los equipos que manejan procesos críticos	9000	10000
[COM] Redes comunicaciones	Central Telefónica Analógica.	10000 $	B	3000 Valor que cubre cableado telefónico	0	500 Configuración de la Central Telefónica.	0	3500	10000
[Media] Soportes de información	Discos duros extraíbles portables	10000 $	B	0	0	0	10000 Al contar con información sensible	10000	10000
[Media] Soportes de información	Discos CD y DVD.	10000 $	B	0	0	0	4000 Al ser información de la área financiera	4000	10000
[Media] Soportes de información	Memorias USB	10000 $	B	0	0	0	2000 Al ser información de las áreas de la institución	6500	10000
[SW] Software - Aplicaciones informáticas	Sistemas Operativos para computadoras de escritorio y portátiles.	10000 $	B	3100 Actualización del sistema operativo.	0	0	0	3100	10000
[SW] Software - Aplicaciones informáticas	Herramientas de ofimática y utilitarios.	10000 $	B	4100 Actualización de software	0	30 Configuración del sistema	0	4130	10000
[HW] Equipamiento informático (hardware)	Computadoras de escritorio.	10000 $	B	980 Se valora el computador de escritorio.	20 Información generada en un día laboral	0	0	1000	10000

[HW] Equipamiento informático (hardware)	Portátiles	10000 $	B	1200 Se valora un computador portátil.	20 Información generada en un día laboral	0	0	1220	10000
[HW] Equipamiento informático (hardware)	Equipo Servidor	50000 $	A	6500 Se considera solo el valor del equipo	2000 Considera el uso por día de varios procesos	1500 Contempla configuración de todos los procesos	8000 Considera valores por pérdida de labores en varias áreas	18000	50000
[HW] Equipamiento informático (hardware)	Switches	10000 $	B	200 Solo de valores de equipos	1000 Representa uso laboral de varias áreas	100 Contempla valor de instalación dado que no son switches administrables	3000 Valor por pérdida en varias áreas interconectadas	4300	10000
[HW] Equipamiento informático (hardware)	Escaneres	10000 $	B	1000 Se considera solo el valor del equipo	0	0	0	1000	10000
[HW] Equipamiento informático (hardware)	Router	75000 $	MA	350 Se consideran el valor de la licencia del Router Cloud en Distrito Central y Unidad de salud	0	60 Debido a que solo se configuran en el Router Cloud de central y cliente	2000 Tomando en cuenta el trabajo que quedaría suspendido por la falta de conectividad	2410	10000
[HW] Equipamiento informático (hardware)	Impresoras	1000 $	BM	600 Se considera solo el valor del equipo	0	0	0	600	1000
D] Datos / Información	Backup (copias de seguridad).	10000 $	B	0		0	5000 Al ser información de la área financiera y talento humano	5000	1000

D] Datos / Información	Base de datos.	10000 $	B	0	1200 la reconfiguración de las bases de datos	0	2000 Al ser información de las áreas de la institución	3200	10000
D] Datos / Información	Archivos de gestión de las áreas.	10000 $	B	0	0	0	2000 Al ser información de las áreas de la institución	2000	10000
D] Datos / Información	Guía de usuario de los sistemas de información.	10000 $	B	0	1200 Costo de elaboración.	0		1200	10000
[S] Servicios	Servicio de DHCP	1000 $	BM	0	0	30 Configuración del sistema	0	30	1000
[S] Servicios	Servicio de DNS	1000 $	BM	0	0	30 Configuración del sistema	0	30	1000
[S] Servicios	Servidor WEB	1000 $	BM	0	0	30 Configuración del sistema	0	30	1000
[AUX] Equipamiento auxiliar	UPS	10000 $	B	2400 Valores correspondientes a UPS instalados en cuartos de comunicación y biométricos.	1000 Teniendo en cuenta que la red de suministro eléctrico es muy inestable	0	3000 Valor por pérdida de interconexión caída	6400	10000
[AUX] Equipamiento auxiliar	Equipos de climatización	10000 $	B	1400 Valor para la adquisición de equipos de climatización	0	0	0	1400	10000
[AUX] Equipamiento auxiliar	Equipos de extinción de incendios.	1000 $	BM	150 Valor de extintor de incendios	0	0	0	150	1000

[AUX] Equipamiento auxiliar	Cableado de red	10000 $	B	2000 Valor que cubre cableado estructurado.	0	0	0	2000	10000
[AUX] Equipamiento auxiliar	Fibra óptica	10000 $	B	1500 Valor de fibra óptica	0	0	0	1500	10000
[L] Instalaciones	Oficinas	50000 $	A	25000Considera el espacio fisico de todas las oficinas administrativas	0	0	0	25000	50000
[L] Instalaciones	Cuarto de Telecomunicaciones	75000 $	MA	35000 Considera el espacio físico	2000 Valor generado por día	0	25000 Valor del espacio más información y equipos instalados en el lugar	62000	75000

Tabla 9. Justificación de los Activo

A continuación, se muestran las tablas 10 y 11, las cuales permiten establecer la valoración cuantitativa y cualitativa de los activos con criterios de valoración determinados.

Nivel	Abreviatura	Valor
Muy Alto	MA	750000 $
Alto	A	50000 $
Medio	M	30000 $
Bajo	B	10000 $
Muy bajo	MB	1000 $

Tabla 10. Criterio de valoración de los Activos.

Nº	Código	Grupo	Descripción	Valoración cuantitativa	Valoración cualitativa
1	P-01	[P] Personal	Administrador de sistemas.	75000	MA
2	P-02	[P] Personal	Funcionarios	10000	B
3	R-01	[COM] Redes comunicaciones	Red de internet	10000	B
4	R-02	[COM] Redes comunicaciones	Red de área local	10000	B
5	R-03	[COM] Redes comunicaciones	Central Telefónica Analógica.	10000	B
6	M-01	[Media] Soportes de información	Discos duros extraíbles portables	10000	B
7	M-02	[Media] Soportes de información	Discos CD y DVD.	10000	B
8	M-03	[Media] Soportes de información	Memorias USB	10000	B
9	S-01	[SW] Software - Aplicaciones informáticas	Sistemas Operativos para computadoras de escritorio y portátiles	10000	B
10	S-02	[SW] Software - Aplicaciones informáticas	Herramientas de ofimática y utilitarios.	10000	B
11	H-01	[HW] Equipamiento informático (hardware)	Computadoras de escritorio.	10000	B
12	H-02	[HW] Equipamiento informático (hardware)	Portátiles	10000	B
13	H-03	[HW] Equipamiento informático (hardware)	Equipo Servidor	50000	A
14	H-04	[HW] Equipamiento informático (hardware)	Switches	10000	B
15	H-05	[HW] Equipamiento informático (hardware)	Escáneres	10000	B

16	H-06	[HW] Equipamiento informático (hardware)	Router	10000	MA
17	H-07	[HW] Equipamiento informático (hardware)	Impresoras	1000	BM
18	D-01	D] Datos / Información	Backup (copias de seguridad).	1000	B
19	D-02	D] Datos / Información	Base de datos.	10000	B
20	D-03	D] Datos / Información	Archivos de gestión de Las áreas.	10000	B
21	D-04	D] Datos / Información	Guía de usuario de los sistemas de información.	10000	B
22	S-01	[S] Servicios	Servicio de DHCP	1000	BM
23	S-02	[S] Servicios	Servicio de DNS	1000	BM
24	S-03	[S] Servicios	Servidor WEB	1000	BM
25	A-01	[AUX] Equipamiento auxiliar	UPS	10000	B
26	A-02	[AUX] Equipamiento auxiliar	Equipos de climatización	10000	B
27	A-03	[AUX] Equipamiento auxiliar	Equipos de extinción de incendios.	1000	BM
28	A-04	[AUX] Equipamiento auxiliar	Cableado de red	10000	B
29	A-05	[AUX] Equipamiento auxiliar	Fibra óptica	10000	B
30	L-01	[L] Instalaciones	Oficinas	50000	A
31	L-02	[L] Instalaciones	Cuarto de Telecomunicaciones	75000	MA

Tabla 11. Valoración de los Activos.

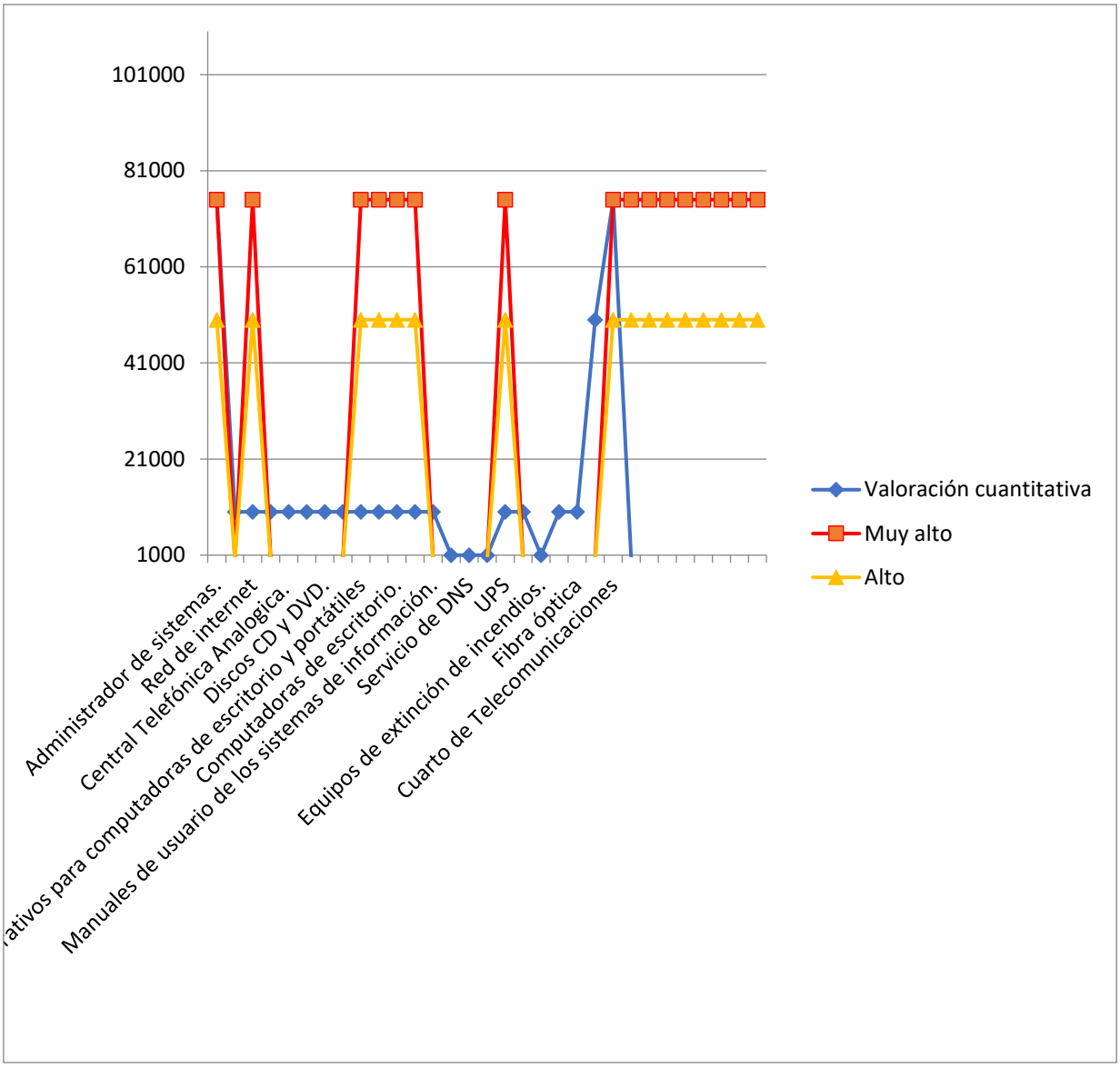

Figura.5: Valoración Cuantitativa de los Activos. Fuente: Autor

Con se puede observar en la figura 5, los activos que se encuentra en un nivel “Muy Alto” y “Alto” tendrán un tratamiento preferencial ya que su valor es representativo para el Distrito.

Salvaguardas: Una vez ya identificados los activos que representan mayor nivel de riesgo se definirán las salvaguardas con el fin de reducir el riesgo de ataque. La tabla 12 resume las diferentes salvaguardas para los activos.

Nº	Código	Descripción	Activo
1	SG-001	Sistema de alarma	P-01 Administrador de sistemas. L-01 Oficinas L-02 Cuarto de Telecomunicaciones.
2	SG-002	Claves de activación/desactivación. Sistema de alarma.	H-03 Equipo Servidor
3	SG-003	Contratos de confidencialidad de plantilla	P-01 Administrador de sistemas F-01 Data Center
4	SG-004	Formación del personal en seguridad.	P-01 Administrador de sistemas L-02 Cuarto de Telecomunicaciones
5	SG-005	Mantenimiento de la climatización.	F-02 Cuarto de Telecomunicaciones.
6	SG-006	Póliza de seguro contra accidentes.	P-01 Administrador de sistema
7	SG-007	Póliza de seguro contra desastres naturales.	H-03 Equipo Servidor L-01 Oficinas L-02 Cuarto de Telecomunicaciones.
8	SG-008	Sistema de circuito cerrado.	H-03 Equipo Servidor
9	SG-009	Firewall	H-03Equipo Servidor
10	SG-010	Baterías de respaldo eléctrico.	F-02 Cuarto de Telecomunicaciones.
11	SG-011	Póliza de seguro de bienes.	H-03Equipo Servidor L-01 Oficinas
12	SG-012	Copias de seguridad de datos	H-03 Equipo Servidor
13	SG-013	Antivirus	H-03 Equipo Servidor
14	SG-014	Software copias seguridad.	H-03 Equipo Servidor
15	SG-015	Control de acceso.	L-02 Cuarto de Telecomunicaciones.
16	SG-016	Sistema de generador eléctrico de planta.	L-02 Cuarto de Telecomunicaciones.
17	SG-017	Implementación de un sistema de pruebas automatizadas	
18	SG-018	Mantenimiento preventivo	H-03 Equipo Servidor
19	SG-019	Contratación de almacenamiento en la nube	

Tabla 12. Salvaguardas Fuente: Autor.

Cálculo de Riesgo Intrínseco: Se realiza el cálculo de acuerdo al listado de activos de la tabla 10; primero nos enfocamos en el riesgo intrínseco diario por amenaza desarrollado en las tablas 13 ,14,15 y 16, con la finalidad de hallar el nivel de riesgo asociado a un activo en un día en particular, sin considerar las medidas de seguridad implementadas, lo que es útil para comprender la situación de riesgo en un momento dado y priorizar las acciones de mitigación a corto plazo. Y una vez determinado el riesgo intrínseco diario por amenaza, se procede a realizar a el cálculo de riesgo intrínseco anual por amenaza, el cual considera las mismas amenazas y vulnerabilidades que el riesgo intrínseco diario; pero con la diferencia que este se proyecta en un horizonte temporal más amplio (un año), siendo útil para planificar medidas de mitigación a medio y largo plaza con el objetivo de establecer políticas de seguridad a largo plazo.

Riesgo intrínseco			P-01		P-02		R-01		R-02		R-03		M-01		M-02		M-03		S-01		S-02		H-01	
			Administrador de sistemas.		Funcionarios		Red de internet		Red de área local		Central Telefónica Analógica.		Discos duros extraíbles portables		Discos CD y DVD.		Memorias USB		Sistemas Operativos para computadoras de escritorio y portátiles.		Herramientas de ofimática y utilitarios.		Computadoras de escritorio.	
N °	Código	AMENAZA	$ 75.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00	
1	AM-01	Desastre natural					0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%
			0,0000		0,0000		20,2500		20,2500		20,2500		20,2500		20,2500		20,2500		20,2500		20,2500		20,2500	
2	AM-02	Ataque físico					0,00270	90%	0,00270	90%	0,0027	20%	0,0027	20%	0,0027	20%	0,0027	20%	0,0027	20%	0,0329	20%	0,0055	50%
			0,0000		0,0000		24,3000		24,3000		5,4000		5,4000		5,4000		5,4000		5,4000		65,8		27,5000	
3	AM-03	Fallo / avería de equipo					0,00270	75%	0,00270	75%	0,00270	75%	0,00270	90%	0,0027	50%	0,0027	50%	0,0027	75%	0,0027	75%	0,0055	50%
			0,0000		0,0000		20,2500		20,2500		20,2500		24,3000		13,5000		13,5000		20,2500		20,2500		27,5000	
4	AM-04	Avería climatización					0,00550	90%	0,00550	90%	0,00550	90%							0,0027	50%				
			0,0000		0,0000		49,5000		49,5000		49,5000		0,0000		0,0000		0,0000		13,5000		0,0000		0,0000	
5	AM-05	Fallos suministro eléctrico					0,03290	90%	0,03290	90%	0,03290	90%			0,0027	50%	0,0027	50%	0,0027	90%	0,0027	20%	0,0027	90%
			0,0000		0,0000		296,1000		296,1000		296,1000		0,0000		13,5000		13,5000		24,3000		5,4000		24,3000	

6	AM-06	Robo personal interno					0,00270	90%	0,00270	90%	0,0027	50%															0,0055	20%		
			0,0000		0,0000		24,3000		24,3000		13,5000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		11,0000			
7	AM-07	Robo personas externas					0,00270	90%	0,00550	90%	0,0027	50%	0,00270	20%													0,0055	20%		
			0,0000		0,0000		24,3000		49,5000		13,5000		5,4000		0,0000		0,0000		0,0000		0,0000		0,0000		11,0000			
8	AM-08	Ataque informático					0,03290	90%	0,00550	90%			0,0027	20%	0,0027	50%	0,0027	50%	0,0027	50%	0,0027	50%								
			0,0000		0,0000		296,1000		49,5000		0,0000		5,4000		13,5000		13,5000		13,5000		13,5000		0,0000					
9	AM-09	Indisponibilidad física					0,00270	90%	0,00550	90%					0,0027	50%	0,0027	50%	0,0027	50%	0,0027	50%	0,0027	75%				
			0,0000		0,0000		24,3000		49,5000		0,0000		0,0000		13,5000		13,5000		13,5000		13,5000		20,2500					
10	AM-10	Indisponibilidad lógica					0,00550	90%											0,0027	75%	0,0027	20%						
			0,0000		0,0000		49,5000		0,0000		0,0000		0,0000		0,0000		0,0000		20,2500		5,4000		0,0000					
11	AM-11	Indisponibilidad personal	0,0027	90%	0,0027	90%	0,00550	90%																				
			182,2500		24,3000		49,5000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000					
12	AM-12	Errores humanos	0,0027	20%	0,0027	75%	0,00550	0,9000																				
			40,5000		20,2500		49,5000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000					
13	AM-13	Indisponibilidad de comunicaciones					0,00550	90%	0,00550	90%	0,00270	20%			0,0027	20%	0,0027	20%					0,0027	20%				
			0,0000		0,0000		49,5000		49,5000		5,4000		0,0000		5,4000		5,4000		0,0000		5,4000		0,0000					
14	AM-14	Error de diseño	0,0027	75%																								
			151,8750		0,0000				0,0000		0,0000		0,0000		0,0000		0,0000		0,0000				0,0000					
15	AM-15	Acceso no autorizado a sistemas	0,0055	20%			0,0027	90%	0,0027	90%																		
			82,5000		0,0000		24,3000		24,3000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000					
16	AM-16	Divulgación no autorizada	0,0027	90%			0,0027	50%	0,0027	50%																		
			182,2500		0,0000		13,5000		13,5000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000					
17	AM-17	Fallo en copias																										
			0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000					
18	AM-18	Fallos de software																	0,0027	50%								
			0,0000				0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		13,5000		0,0000		0,0000					
19	AM-19	Carencia de mantenimiento software					0,00550	20%	0,00550	20%									0,0027	50%								
			0,0000		0,0000		11,0000		11,0000		0,0000		0,0000		0,0000		0,0000		13,5000		0,0000		0,0000					

20	AM-20	Fallo en las comunicaciones					0,00270	50%									0,0027	20%	0,0027	50%	0,0027	50 %								
			0,0000		0,0000		13,5000		0,0000		0,0000		0,0000		0,0000		5,4000		13,5000		13,5000		0,0000							
21	AM-21	Eliminación no autorizada					0,03290	50%	0,03290	50%			0,0055	20 %			0,0027	75%												
			0,0000		0,0000		164,5000		164,5000		0,0000		11,0000		0,0000		20,2500		0,0000		0,0000		0,0000							
22	AM-22	Pérdida de información	0,0055	75 %					0,00270	50%			0,0027	90 %																
			309,3750		0,0000		0,0000		13,5000		0,0000		24,3000		0,0000		0,0000		0,0000		0,0000		0,0000							
23	AM-23	Coacción	0,0027	90 %																										
			182,2500		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000							
24	AM-24	Extravío de documentos	0,0027	75 %																										
			151,8750		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000							
25	AM-25	Negligencia	0,0027	90 %																										
			182,2500		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000							
26	AM-26	Difusión a personas no autorizadas	0,0027	90 %					0,00270	0,7500			0,0027	75 %	0,0027	75%														
			182,2500		0,0000		0,0000		20,2500		0,0000		20,2500		20,2500		0,0000		0,0000		0,0000		0,0000							
27	AM-27	Manipulación de equipamiento					0,00270	50%	0,00270	50%	0,0027	50%											0,0027	20%						
			0,0000		0,0000		13,5000		13,5000		13,5000		0,0000		0,0000		0,0000		0,0000		0,0000		5,4000							
		Riesgo intrínseco diario por activo	**$ 1.647,38**		**$ 44,55**		**$ 1.217,70**		**$ 893,25**		**$ 437,40**		**$ 116,30**		**$ 105,30**		**$ 110,70**		**$ 171,45**		**$ 163,00**		**$ 147,20**							
		Riesgo intrínseco anual por activo	**$ 601.291,88**		**$ 16.260,75**		**$ 444.460,50**		**$ 326.036,25**		**$ 159.651,00**		**$ 42.449,50**		**$ 38.434,50**		**$ 40.405,50**		**$ 62.579,25**		**$ 59.495,00**		**$ 53.728,00**							

Tabla 13. Cálculo de Riesgo Intrínseco parte 1 Fuente: Autor

Riesgo intrínseco			H-02		H-03		H-04		H-05		H-06		H-07		D-01		D-02		D-03		D-04	
			Portátiles		Equipo Servidor		Switches		Escáneres		Router		Impresoras		Backup (copias de seguridad).		Base de datos.		Archivos de gestión de Las áreas.		Manuales de usuario de los sistemas de información.	
Nº	Código	AMENAZA	$ 10.000,00		$ 50.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00		$ 1.000,00		$ 1.000,00		$ 10.000,00		$ 10.000,00		$ 10.000,00	
1	AM-01	Desastre natural	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	50%
			20,2500		101,2500		20,2500		20,2500		20,2500		2,0250		2,0250		20,2500		20,2500		13,5000	
2	AM-02	Ataque físico	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%			0,0027	90%	0,00270	90%						
			20,25		101,25		20,25		20,25		0,0000		2,4300		2,4300		0,0000		0,0000		0,0000	
3	AM-03	Fallo / avería de equipo	0,0055	50%	0,0055	50%	0,0027	75%	0,0027	75%	0,0027	75%	0,0055	50%	0,00270	75%	0,0027	20%	0,00270	75%	0,00270	75%
			27,5000		137,5000		20,2500		20,2500		20,2500		2,7500		2,0250		5,4000		20,2500		20,2500	
4	AM-04	Avería climatización			0,0055	75%	0,0055	75%			0,0055	75%			0,00550	50%						
			0,0000		206,2500		41,2500		0,0000		41,2500		0,0000		2,7500		0,0000		0,0000		0,0000	
5	AM-05	Fallos suministro eléctrico	0,0027	90%									0,0329	90%	0,03290	90%					0,0027	90%
			24,3000								0,0000		29,6100		29,6100		0,0000		0,0000		24,3000	
6	AM-06	Robo personal interno	0,0055	20%	0,0055	20%	0,0055	75%	0,0055	75%			0,0027	75%	0,00270	90%			0,0027	50%		
			11,0000		55,0000		41,2500		41,2500		0,0000		2,0250		2,4300		0,0000		13,5000		0,0000	
7	AM-07	Robo personas externas	0,0055	20%	0,0027	75%	0,0027	75%	0,0027	75%			0,0027	75%	0,00270	50%	0,00270	50%	0,0027	50%		
			11,0000		101,2500		20,2500		20,2500		0,0000		2,0250		1,3500		13,5000		13,5000		0,0000	
8	AM-08	Ataque informático											0,0027	50%	0,03290	90%					0,0027	50%
			0,0000		0,0000		0,0000		0,0000		0,0000		1,3500		29,6100		0,0000		0,0000		13,5000	
9	AM-09	Indisponibilidad física	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%			0,0027	75%	0,00270	75%						
			20,2500		101,2500		20,2500		20,2500		0,0000		2,0250		2,0250		0,0000		0,0000		0,0000	
10	AM-10	Indisponibilidad lógica			0,0027	20%							0,0027	75%	0,00550	75%					0,0027	50%
			0,0000		27,0000		0,0000		0,0000		0,0000		2,0250		4,1250		0,0000		0,0000		13,5000	

11	AM-11	Indisponibilidad personal									0,0027	90%	0,0027	0,9000	0,00550	90%								
			0,0000		0,0000		0,0000		0,0000		24,3000		2,4300		4,9500		0,0000		0,0000		0,0000			
12	AM-12	Errores humanos									0,0027	20%	0,0027	75%	0,00550	0,9000								
			0,0000		0,0000		0,0000		0,0000		5,4000		2,0250		4,9500		0,0000		0,0000		0,0000			
13	AM-13	Indisponibilidad de comunicaciones													0,00550	50%								
			0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		2,7500		0,0000		0,0000		0,0000			
14	AM-14	Error de diseño									0,0027	75%	0,0027	75%										
			0,0000		0,0000		0,0000		0,0000		20,2500		2,0250				0,0000		0,0000		0,0000			
15	AM-15	Acceso no autorizado a sistemas									0,0055	20%									0,0027	20%		
			0,0000		0,0000		0,0000		0,0000		11,0000		0,0000		0,0000		0,0000		0,0000		5,4000			
16	AM-16	Divulgación no autorizada									0,0027	90%			0,0027	50%	0,0027	50%	0,0027	50%				
			0,0000		0,0000		0,0000		0,0000		24,3000		0,0000		1,3500		13,5000		13,5000		0,0000			
17	AM-17	Fallo en copias																						
			0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		0,0000			
18	AM-18	Fallos de software			0,00270	50%									0,00270	50%								
			0,0000		67,5000		0,0000		0,0000		0,0000				1,3500		0,0000		0,0000		0,0000			
19	AM-19	Carencia de mantenimiento software			0,00550	20%							0,0027	90%	0,00550	20%					0,0027	20%		
			0,0000		55,0000		0,0000		0,0000		0,0000		2,4300		1,1000		0,0000		0,0000		5,4000			
20	AM-20	Fallo en las comunicaciones											0,00270	75%	0,00270	50%								
			0,0000		0,0000		0,0000		0,0000		0,0000		2,0250		1,3500		0,0000		0,0000		0,0000			
21	AM-21	Eliminación no autorizada													0,03290	50%					0,0055	75%		
			0,0000		0,0000		0,0000		0,0000		0,0000		0,0000		16,4500		0,0000		0,0000		41,2500			
22	AM-22	Pérdida de información									0,0055	75%					0,00270	50%	0,0027	50%	0,0027	50%		
			0,0000		0,0000		0,0000		0,0000		41,2500		0,0000		0,0000		13,5000		13,5000		13,5000			
23	AM-23	Coacción									0,0027	90%												
			0,0000		0,0000		0,0000		0,0000		24,3000		0,0000		0,0000		0,0000		0,0000		0,0000			
24	AM-24	Extravío de									0,0027	75%							0,0027	75%	0,0027	75%		

		documentos	0,0000		0,0000		0,0000		0,0000		20,2500		0,0000		0,0000		0,0000		20,2500		20,2500	
25	AM-25	Negligencia									0,0027	90%										
			0,0000		0,0000		0,0000		0,0000		24,3000		0,0000		0,0000		0,0000		0,0000		0,0000	
26	AM-26	Difusión a personas no autorizadas									0,0027	90%					0,00270	0,7500	0,0027	50%	0,0027	75%
			0,0000		0,0000		0,0000		0,0000		24,3000		0,0000		0,0000		20,2500		13,5000		20,2500	
27	AM-27	Manipulación de equipamiento	0,0027	20%	0,0027	90%	0,0027	90%	0,0027	90%	0,0027	90%	0,0027	50%								
			5,4000		121,5000		24,3000		24,3000		24,3000		1,3500		0,0000		0,0000		0,0000		0,0000	
		Riesgo intrínseco diario por activo	**$ 139,95**		**$ 1.074,75**		**$ 208,05**		**$ 166,80**		**$ 325,70**		**$ 58,55**		**$ 112,63**		**$ 86,40**		**$ 128,25**		**$ 191,10**	
		Riesgo intrínseco anual por activo	**$ 51.081,75**		**$ 392.283,75**		**$ 75.938,25**		**$ 60.882,00**		**$ 118.880,50**		**$ 21.370,75**		**$ 41.109,95**		**$ 31.536,00**		**$ 46.811,25**		**$ 69.751,50**	

Tabla 14. Cálculo de Riesgo Intrínseco parte 2 Fuente: Autor

Riesgo intrínseco			S-01		S-02		S-03		A-01		A-02		A-03		A-04		A-05	
			Servicio de DHCP		Servicio de DNS		Servidor WEB		UPS		Equipos de climatización		Equipos de extinción de incendios.		Cableado de red		Fibra óptica	
Nº	Código	AMENAZA	$ 1.000,00		$ 1.000,00		$ 1.000,00		$ 10.000,00		$ 10.000,00		$ 1.000,00		$ 10.000,00		$ 10.000,00	
1	AM-01	Desastre natural	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	50%	0,0027	50%	0,0027	75%	0,0027	75%	0,0027	75%
			2,0250		2,0250		2,0250		13,5000		13,5000		2,0250		20,2500		20,2500	
2	AM-02	Ataque físico	0,0027	20%	0,0027	20%	0,0027	75%	0,0329	20%	0,0055	50%	0,0027	75%	0,0027	75%	0,0027	75%
			0,5400		0,5400		2,0250		65,8		27,5000		2,025		20,25		20,25	
3	AM-03	Fallo / avería de equipo	0,00270	75%	0,00270	75%	0,0027	75%	0,0027	75%	0,0055	50%	0,00270	75%	0,00270	75%	0,00270	75%
			2,0250		2,0250		2,0250		20,2500		27,5000		2,0250		20,2500		20,2500	
4	AM-04	Avería climatización	0,00550	50%	0,00550	50%	0,00550	50%	0,00550	50%	0,00550	90%	0,0055	75%	0,0055	75%	0,0055	75%
			2,7500		2,7500		2,7500		27,5000		49,5000		4,1250		41,2500		41,2500	
5	AM-05	Fallos suministro eléctrico	0,0027	50%	0,0027	50%	0,0027	75%	0,0027	20%	0,1425	20%			0,0055	75%	0,0055	75%
			1,3500		1,3500		2,0250		5,4000		285,0000							
6	AM-06	Robo personal interno							0,0055	75%	0,0055	75%	0,0055	75%	0,0055	75%	0,0055	75%
			0,0000		0,0000		0,0000				41,2500		4,1250		41,2500		41,2500	
7	AM-07	Robo personas externas											0,0027	75%	0,0027	75%	0,0027	75%
			0,0000		0,0000		0,0000		0,0000		0,0000		2,0250		20,2500		20,2500	
8	AM-08	Ataque informático	0,0027	50%	0,0027	50%	0,0027	50%	0,0027	50%								
			1,3500		1,3500		1,3500		13,5000		0,0000		0,0000		0,0000		0,0000	
9	AM-09	Indisponibilidad física	0,0027	50%	0,0027	50%			0,0027	50%	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%
			1,3500		1,3500		0,0000		13,5000		20,2500		2,0250		20,2500		20,2500	
10	AM-10	Indisponibilidad lógica					0,0027	75%	0,0027	20%								
			0,0000		0,0000		2,0250		5,4000		0,0000		0,0000		0,0000		0,0000	
11	AM-11																	

		Indisponibilidad personal	0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
12	AM-12	Errores humanos																						
			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
13	AM-13	Indisponibilidad de comunicaciones	0,0027	20%		0,0027	20%					0,0027	20%											
			0,5400			0,5400			0,0000			5,4000			0,0000			0,0000			0,0000			0,0000	
14	AM-14	Error de diseño																						
			0,0000			0,0000			0,0000						0,0000			0,0000			0,0000			0,0000	
15	AM-15	Acceso no autorizado a sistemas																						
			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
16	AM-16	Divulgación no autorizada																						
			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
17	AM-17	Fallo en copias																						
			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
18	AM-18	Fallos de software				0,0027	50%		0,0027	50%														
			0,0000			1,3500			1,3500			0,0000			0,0000			0,0000			0,0000			0,0000	
19	AM-19	Carencia de mantenimiento software							0,0027	50%		0,0027	50%											
			0,0000			0,0000			1,3500			13,5000			0,0000			0,0000			0,0000			0,0000	
20	AM-20	Fallo en las comunicaciones	0,0027	20%		0,0027	20%		0,0027	50%		0,0027	50%											
			0,5400			0,5400			1,3500			13,5000			0,0000			0,0000			0,0000			0,0000	
21	AM-21	Eliminación no autorizada	0,0027	75%		0,0027	75%																	
			2,0250			2,0250			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
22	AM-22	Pérdida de información																						
			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
23	AM-23	Coacción																						
			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
24	AM-24	Extravío de documentos																						
			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
25	AM-25	Negligencia																						
			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	
26	AM-26	Difusión a personas no autorizadas																						
			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000			0,0000	

27	AM-27	Manipulación de equipamiento							0,0027	20%	0,0027	20%								
			0,0000		0,0000		0,0000		5,4000		5,4000		0,0000		0,0000		0,0000			
		Riesgo intrínseco diario por activo	**$ 14,50**		**$ 15,85**		**$ 18,28**		**$ 202,65**		**$ 469,90**		**$ 18,38**		**$ 183,75**		**$ 183,75**			
		Riesgo intrínseco anual por activo	**$ 5.290,68**		**$ 5.783,43**		**$ 6.670,38**		**$ 73.967,25**		**$ 171.513,50**		**$ 6.706,88**		**$ 67.068,75**		**$ 67.068,75**			

Tabla 15. Cálculo de Riesgo Intrínseco diario parte 3 Fuente: Autor

Riesgo intrínseco			**S-01**		**S-02**		**L-01**		**L-02**			
			Servicio de DHCP		Servicio de DNS		Oficinas		Cuarto de Telecomunicaciones		**RIESGO INTRÍNSECO DIARIO POR AMENAZA**	**RIESGO INTRÍNSECO ANUAL POR AMENAZA**
Nº	**Código**	**AMENAZA**	$ 1.000,00		$ 1.000,00		$ 50.000,00		$ 75.000,00			
1	AM-01	Desastre natural	0,0027	75%	0,0027	75%	0,0027	75%	0,0027	75%		
			2,0250		2,0250		101,2500		151,8750		**$ 202,50**	**$ 73.912,50**
2	AM-02	Ataque físico	0,0027	20%	0,0027	20%	0,0027	75%	0,0027	75%		
			0,5400		0,5400		101,25		151,875		**$ 189,15**	**$ 69.039,75**
3	AM-03	Fallo / avería de equipo	0,00270	75%	0,00270	75%	0,00270	90%				
			2,0250		2,0250		121,5000		0,0000		**$ 207,55**	**$ 75.755,75**
4	AM-04	Avería climatización	0,00550	50%	0,00550	50%	0,0055	75%	0,0055	75%		
			2,7500		2,7500		206,2500		309,3750		**$ 162,00**	**$ 59.130,00**
5	AM-05	Fallos suministro eléctrico	0,0027	50%	0,0027	50%	0,0055	75%	0,0055	75%		
			1,3500		1,3500		206,2500		309,3750		**$ 993,60**	**$ 362.664,00**
6	AM-06	Robo personal interno					0,0055	75%	0,0055	75%		
			0,0000		0,0000		206,2500		309,3750		**$ 84,10**	**$ 30.696,50**

7	AM-07	Robo personas externas					0,0027	75%	0,0027	75%		
			0,0000		0,0000		101,2500		151,8750		$ 114,70	$ 41.865,50
8	AM-08	Ataque informático	0,0027	50%	0,0027	50%			0,0027	90%		
			1,3500		1,3500		0,0000		182,2500		$ 405,00	$ 147.825,00
9	AM-09	Indisponibilidad física	0,0027	50%	0,0027	50%	0,0027	75%	0,0027	75%		
			1,3500		1,3500		101,2500		151,8750		$ 168,30	$ 61.429,50
10	AM-10	Indisponibilidad lógica							0,0027	75%		
			0,0000		0,0000		0,0000		151,8750		$ 75,15	$ 27.429,75
11	AM-11	Indisponibilidad personal										
			0,0000		0,0000		0,0000		0,0000		$ 256,05	$ 93.458,25
12	AM-12	Errores humanos										
			0,0000		0,0000		0,0000		0,0000		$ 110,25	$ 40.241,25
13	AM-13	Indisponibilidad de comunicaciones	0,0027	20%	0,0027	20%						
			0,5400		0,5400		0,0000		0,0000		$ 120,60	$ 44.019,00
14	AM-14	Error de diseño										
			0,0000		0,0000		0,0000		0,0000		$ 151,88	$ 55.434,38
15	AM-15	Acceso no autorizado a sistemas					0,0027	75%	0,0027	75%		
			0,0000		0,0000		101,2500		151,8750		$ 131,10	$ 47.851,50
16	AM-16	Divulgación no autorizada										
			0,0000		0,0000		0,0000		0,0000		$ 209,25	$ 76.376,25
17	AM-17	Fallo en copias										
			0,0000		0,0000		0,0000		0,0000		$ -	$ -
18	AM-18	Fallos de software			0,0027	50%						
			0,0000		1,3500		0,0000		0,0000		$ 13,50	$ 4.927,50
19	AM-19	Carencia de mantenimiento software							0,0027	75%		
			0,0000		0,0000		0,0000		151,8750		$ 35,50	$ 12.957,50
20	AM-20	Fallo en las comunicaciones	0,0027	20%	0,0027	20%						
			0,5400		0,5400		0,0000		0,0000		$ 45,90	$ 16.753,50
21	AM-21	Eliminación no autorizada	0,0027	75%	0,0027	75%						
			2,0250		2,0250		0,0000		0,0000		$ 360,25	$ 131.491,25
22	AM-22	Pérdida de información										
			0,0000		0,0000		0,0000		0,0000		$ 347,18	$ 126.718,88
23	AM-23	Coacción										

			0,0000		0,0000		0,0000		0,0000		$ 182,25	$ 66.521,25
24	AM-24	Extravío de documentos	0,0000		0,0000		0,0000		0,0000		$ 151,88	$ 55.434,38
25	AM-25	Negligencia	0,0000		0,0000		0,0000		0,0000		$ 182,25	$ 66.521,25
26	AM-26	Difusión a personas no autorizadas	0,0000		0,0000		0,0000		0,0000		$ 243,00	$ 88.695,00
27	AM-27	Manipulación de equipamiento	0,0000		0,0000		0,0000		0,0027	20%	$ 51,30	$ 18.724,50
									40,5000			
		Riesgo intrínseco diario por activo	**$ 14,50**		**$ 15,85**		**$ 1.246,50**		**$ 2.214,00**			
		Riesgo intrínseco anual por activo	**$ 5.290,68**		**$ 5.783,43**		**$ 454.972,50**		**$ 808.110,00**			

Tabla 16. Cálculo de Riesgo Intrínseco parte 4 Fuente: Autor

5.2. Metodología NIST SP800-30.

La metodología NIST SP800-30 es un enfoque de evaluación de riesgos ampliamente utilizado en ciberseguridad. Contando con un proceso sistemático que ayuda a las organizaciones a identificar, evaluar y mitigar los riesgos de seguridad de la información de forma efectiva.

5.2.1 Caracterización de sistemas.

En esta sección se realizará el análisis de riegos los activos que forman parte de la institución.

IDENTIFICACIÓN DE ACTIVOS		
Categoría de Activo	**Nombre Activo**	**Descripción del activo**
Personas	Administrador de sistemas, funcionarios.	Recurso Humano de la institución.
Comunicaciones	Red de internet, Red de área local, Central Telefónica Analógica, Servicio de DHCP, Servicio de DNS, Servidor WEB	Son servicios por la institución y entre otros.
Información	Backup, Base de datos, Archivos de información de las áreas, Guías de usuario de los sistemas implementados, Memorias USB, Discos duros extraíbles portables, DVD y Discos CD.	La información que se almacena en medios físico o digital.
Software	Sistemas Operativos para computadoras de escritorio y portátiles, herramientas de ofimática y utilitarios.	Aplicaciones, herramientas de software.

Hardware	Computadoras de escritorio, Portátiles, Impresoras, Escáneres, Equipo Servidor, Switches y Router.	Equipos físicos
Infraestructura física	Oficinas, Cuarto de Telecomunicaciones.	Instalaciones Físicas

Tabla 17. Identificación de los Activos. Fuente: Autor.

5.2.2 Identificación de amenazas.

Considerando que una amenaza se define como cualquier evento intencionado o mal intencionado que puede ocasionar un daño en el sistema [23], estas se clasificarán de acuerdo a su categoría de activo. En esta etapa se establecen las Amenazas representadas por una "A" y las Oportunidades con una "O".

Software	A: Ataques cibernéticos, fallas en los sistemas de información o aplicativos, mala configuración, etc. O: Actualización de las aplicaciones en tiempo real, Políticas de uso adecuado de recursos Tecnológicos.
Hardware	A: Fallas en la alimentación eléctrica, sobrecalentamiento, problemas de humedad, robos, daño en piezas y partes, mala configuración, sobrecarga eléctrica, golpes, falta de disposición presupuestaria para la renovación de equipos tecnológico, etc. O: Amplio parque informático, Políticas de uso adecuado de recursos Tecnológicos.
Personas	A: Falta de personal en áreas estratégicas, falta de coordinación. O: Personal motivado, Personal especializado.
Infraestructura física	A: Infraestructura deficiente, el acceso no autorizado al centro de datos, acceso a personas no autorizadas a la documentación física, fuego, inundación, terremoto, etc. O: Oficinas.

Tabla 18. Identificación de los Amenazas y Oportunidades. Fuente: Autor.

5.2.3 Identificación fuentes de amenazas.

Dentro del marco de la metodología NIST SP 800-30, se presenta una categorización de las fuentes de amenazas que resulta adaptable a diversas organizaciones, incluyendo el caso específico de la Dirección Distrital 14D01 Morona-Salud. En la Tabla 19, se pueden observar las distintas fuentes de amenazas, agrupadas en cuatro categorías: adversidad, factores ambientales, aspectos estructurales y eventos accidentales.

Tipo de Fuente de Amenaza	**Subtipo**	**Fuente de Amenaza**	**Descripción**
Adversidad	Individual	Agente interno Agente Externo	Individuos, colectivos, entidades u naciones que investigan con el propósito de aprovechar la vulnerabilidad de la organización ante los recursos cibernéticos.
Accidental	Humano	Privilegios de administrador Usuario	Acciones incorrectas llevadas a cabo por individuos durante el desempeño de sus tareas habituales.
Estructural	Equipamiento tecnológico de la información área Tecnologías.	Comunicaciones	Deficiencia en los sistemas, condiciones ambientales o software debido a la degradación, agotamiento de recursos u otras situaciones que exceden los límites operativos previstos.
	Controles Ambientales	Fuente de energía.	
	Software	Redes Aplicativos de uso general.	
Ambiental	Desastre natural o provocado por el hombre	Terremoto Incendio	Eventos catastróficos de origen natural y fallos en infraestructuras críticas que son vitales para la organización, pero que escapan al control de esta última.

Tabla 19. Identificación de fuentes de amenaza Fuente: [4]

Identificadas las amenazas procederemos a listar los acontecimientos que pueden suscitar, las mismas que están agrupados en ocho tipos diferentes: Agente Externo, Agente Interno, Usuario, Administrador, Comunicaciones, Fuente de Alimentación, Terremoto, Incendio, Red y Aplicativos de uso global determinados por su relevancia como se observa en la tabla 20 y 21.

Valor	**Descripción**
Confirmado	El evento de amenaza ha sido visto por la organización
Esperado	El evento de amenaza ha sido visto por los compañeros de la organización
Anticipado	El evento de amenaza ha sido reportado por una fuente confiable
Predicho	El evento de amenaza ha sido predicho por una fuente confiable
Posible	El evento de amenaza ha sido descrito por alguna fuente creíble
N/A	El evento de amenaza no es aplicable

Tabla 20. Relevancia de los eventos Fuente: [4]

Fuentes de Amenazas	**Eventos de Amenazas**	**Relevancia**
Agente Externo	Realiza tácticas de suplantación en línea.	Posible
	Creación de una página web falsa.	Posible
	Elaborar certificados adulterados	Posible
	Comprometer la integridad al realizar acciones como la creación, eliminación o modificación de datos en sistemas de información de acceso público.	Posible
	Comprometer la integridad al contaminar o dañar datos esenciales.	Posible
	Llevar a cabo acciones de captura de comunicaciones	Posible
	Acceder de manera no autorizada.	Posible
	Adquirir datos confidenciales mediante la monitorización de redes externas.	Posible
	Explotar VPNs.	Posible
Agente Interno	Distribuir software malicioso previamente identificado en los sistemas de información internos de la organización, como, por ejemplo, a través de correos electrónicos con virus.	Predicho
	Aprovechar las vulnerabilidades presentes en los sistemas de información internos de la organización.	N/A

	Revelar la vulnerabilidad del software de los sistemas de información esenciales de la organización	Posible
	Inducir la difusión de información importante y/o confidencial por parte de usuarios con autorización	N/A
	Logre acceso no autorizado.	N/A
	Obtener datos o información confidencial de sistemas de información de acceso público.	N/A
Usuario	Incorpore software malicioso específico en los sistemas de información de la organización y en sus componentes.	Posible
	Poner en riesgo los sistemas de información cruciales mediante la obtención de acceso físico.	N/A
	Realizar tácticas de ingeniería social que involucran a individuos externos con el fin de obtener información.	N/A
	Provocar la revelación de información crucial y/o confidencial por parte de usuarios con autorización.	N/A
Administrador	Inyectar software malicioso personalizado en los sistemas de información de la organización de acuerdo con las configuraciones del sistema.	N/A
	Aprovechar sistemas de información que están expuestos a Internet y que tienen configuraciones incorrectas o no autorizadas.	N/A
	Realizar intentos de inicio de sesión por fuerza bruta / ataques de adivinación de contraseñas.	Posible
	Realizar ingeniería social basada en información privilegiada para obtener información	N/A
	Explotar las debilidades presentes en los sistemas de información internos de la organización.	N/A
	Causar la divulgación no autorizada y/o la indisponibilidad al exponer información confidencial.	N/A
Comunicaciones	Falla en recursos tecnológicos	Posible

	Degradación o eliminación de elementos tecnológicos.	Posible
	Perdida de equipos.	Posible
Fuente de energía	Falla de energía eléctrica.	Posible
	Sobrecalentamiento de componentes.	Posible
Red	Incidente en la prestación del servicio de internet.	Posible
	La falta de disponibilidad de servicios críticos (por ejemplo, correo electrónico o sitio web)	Posible
	Alteración de la integridad de los datos.	Posible
Aplicativos de uso general.	Ineficiencia en las aplicaciones debido a problemas de funcionamiento del software.	Posible
Terremoto	Terremoto en localización en el Cuarto de Telecomunicaciones.	Esperado
Incendio	Incendio en localización en el Cuarto de Telecomunicaciones.	Esperado

Tabla 21. Eventos de Amenazas Fuente: [4]

5.2.4. Identificación de vulnerabilidades y Condiciones Predispuestas.

5.2.4.1 Identificación de vulnerabilidades.

Para la identificación de las vulnerabilidades la metodología NIST SP 800-30 nos provee de valores cualitativos a la severidad de las vulnerabilidades cómo se puede observar tabla 22.

Valores Cualitativos	**Descripción**
Muy Alta	La vulnerabilidad está exhibida, aprovechable, y la explotación puede resultar en impactos severos. Controles de seguridad o remedios no están implementados ni planeados; o no hay medida identificada para remediar la vulnerabilidad.

Alta	La vulnerabilidad es una intranquilidad importante, en función de cuán frágil es la vulnerabilidad, cuán fácilmente puede explotarse y/o la gravedad de los efectos potenciales de su explotación. Control de Seguridad está proyectado, pero no implementado, existen controles de compensación que son mínimamente efectivos.
Moderado	La vulnerabilidad es una alarma importante, en función de cuán indefensa es la vulnerabilidad, cuán fácilmente puede explotarse y/o la gravedad de los efectos potenciales de su explotación. Control de seguridad o remediación está parcialmente implementado y algo efectivo.
Baja	La vulnerabilidad es de preocupación baja, pero la efectividad del remedio puede ser mejorado. Control de seguridad u otro remedio está completamente implementado y algo efectivo.
Muy Baja	La vulnerabilidad no es preocupante. Control de seguridad u otro remedio está completamente implementado, evaluado y efectivo.

Tabla 22: Severidad de las vulnerabilidades. Fuente: [4]

Una vez ya entendida la severidad de la vulnerabilidad se procede a identificar las vulnerabilidades como se observa en la tabla 23.

Identificador	**Vulnerabilidad Identificada**	**Severidad de la Vulnerabilidad**
V01	Descubrimiento de Información.	Moderado
V02	Hurto de Información.	Moderado
V03	Ausencia de sistemas de comprobación de la integridad de los certificados.	Baja
V04	Ausencia de directrices para la gestión de la información.	Baja

V05	Ausencia de registro de las lecturas de acceso a los archivos.	Baja
V06	Comunicaciones indefensas.	Baja
V07	Falta de aplicación de política de control de acceso	Baja
V08	Insuficientes mecanismos de defensa perimetral y de redes	Baja
V09	Falta de cifrado.	Baja
V10	Falta de control de licenciamiento de software.	Baja
V11	Carencia de un enfoque de gestión y administración de vulnerabilidades en los activos de tecnología de la información.	Moderado
V12	Falta de actualización de software	Baja
V13	Contraseñas inseguras	Moderado
V14	Falta de renovación de equipamiento obsoleto.	Moderado
V15	Falta de un protocolo para la eliminación de medios de almacenamiento.	Moderado
V16	Robo de equipamiento.	Moderado

V17	Mal funcionamiento de UPS.	Moderado
V18	Inadecuación de la infraestructura para respaldar la alimentación eléctrica de una UPS.	Moderado
V19	Falta de un medio de respaldo adicional.	Moderado
V20	Ausencia de protocolos y prácticas de contingencia.	Moderado
V21	Ausencia de copias de seguridad.	Baja
V22	Falta de planes de contingencia.	Baja
V23	Falta de actualización de planes de contingencia.	Baja
V24	Falta de actualización de planes de contingencia.	Baja

Tabla 23. Identificación de vulnerabilidades. Fuente: [4]

5.2.4.2 Condiciones Predispuestas

Las Condiciones predispuestas son circunstancias que influyen ya sea para maximizar o comprimir la probabilidad de un evento de ataque que haya sido iniciado y resulte en cualquier tipo de impacto, la Metodología de NIST SP 800-30 provee taxonomías para las condiciones predispuestas la cual se pueden ver en la Tabla 24, descritas con el identificador de CP, en cambio que la omnipresencia de las condiciones predispuesta es calificada basándose en la tabla 25 provista por NIST SP 800-30.Y en la tabla 26 ya se identifican las condiciones predispuestas.

Tipos de Condiciones Predispuestas	Descripción
RELACIONADA A LA INFORMACION - Seguridad de la información clasificada Nacionalmente. - Compartimientos - Información no clasificada Controlada - Información Identificable Personal - Programa de Acceso Especial - Determinado por Acuerdo - NOFORN - Propiedad	Requiere manipular la información (a medida que se crea, transmite, almacena, procesa y / o muestra) de una manera específica, debido a su sensibilidad (o falta de sensibilidad), requisitos legales o reglamentarios y / o acuerdos contractuales u otros acuerdos organizativos.
TECNICA - Arquitectura - Cumplimiento de la norma técnica. - Uso de productos específicos o línea de productos. - Soluciones y / o enfoques para la colaboración basada en el usuario y el intercambio de información. - Asignación de funciones de seguridad específicas a controles comunes. - Funcional - Múltiples usuarios de Red - Ser único / sin red	Necesita usar tecnología de maneras específicas.

- Restricción de Funcionalidades	
OPERACIONAL / AMBIENTAL - Movilidad - Sitio Arreglado - Semi móvil - Basado en tierra, aerotransportado, basado en el mar, basado en el espacio - Móvil - Población acceso físico o lógico a los componentes de los sistemas de información. - Tamaño de Población - Investigación de antecedentes de la población	Capacidad para confiar en los controles físicos, de procedimiento y de personal proporcionados por el entorno operativo.

Tabla 24. Taxonomía de Condiciones predispuestas.

Valores Cualitativos	**Descripción**
Muy Alta	Aplica a todos los módulos del sistema de información.
Alta	Aplica a casi todos los módulos del sistema de información.
Moderado	Aplica a varios de los módulos del sistema de información.
Baja	Aplica a algunos de los módulos del sistema de información.
Muy baja	Aplica a pocos de los módulos del sistema de información.

Tabla 25. Omnipresencia de Condiciones Predispuestas Fuente: [4]

Identificador	**Fuente de información sobre condiciones predispuestas.**	**La Omnipresencia de la condición.**
CP01	Cambio en las Políticas de Acceso a la información a nivel del gobierno.	Alta
CP02	Migración tecnológica.	Alta
CP03	Cambio de personal fundamental de TI para el funcionamiento de los sistemas de información.	Moderado
CP04	Mala configuración de un Firewall.	Baja

Tabla 26. Identificación de Condiciones Predispuestas. Fuente: [4]

5.2.5 Determinación de probabilidades.

Para la determinación de probabilidades, la Metodología NIST SP 800-30 nos propone la definición de una probabilidad de inicio de acuerdo a la vulnerabilidad identificada en concordancia con del evento de la amenaza como se puede observar en la tabla 27.

Evento de Amenaza	**Vulnerabilidad Identificada**	**Probabilidad de Inicio**
Realiza tácticas de suplantación en línea	Divulgación de información.	Alta
Creación de una página web falsa.	Perdida de Información	Alta
Elaborar certificados adulterados.	Falta de sistemas para comprobar la integridad.	Baja
Comprometer la integridad al realizar acciones como la creación, eliminación o modificación de datos en sistemas de información de acceso público.	Falta de métodos para gestionar la información	Baja
Comprometer la integridad al contaminar o dañar datos esenciales.	Falta de registro de las entradas de acceso a los archivos en modo lectura.	Baja
Llevar a cabo acciones de captura de comunicaciones.	Comunicaciones desprotegidas	Baja
Acceder de manera no autorizada.	Falta de una normativa para la gestión de acceso.	Baja
Adquirir datos confidenciales mediante la monitorización de redes externas.	Falta de sistemas de seguridad en el perímetro y en las redes.	Baja
Explotar VPNs.	Falta de encriptación.	Baja

Distribuir software malicioso previamente identificado en los sistemas de información internos de la organización, como, por ejemplo, a través de correos electrónicos con virus.	Falta de procesos de regulación para la obtención de licencias de software.	Baja
Aprovechar las vulnerabilidades presentes en los sistemas de información internos de la organización.	Ausencia de manejo y administración de vulnerabilidades en los activos de tecnología de la información.	Moderado
Revelar la vulnerabilidad del software de los sistemas de información esenciales de la organización.	Información insuficiente, incorrecta o no registrada para los desarrolladores.	Baja
Realizar intentos de inicio de sesión por fuerza bruta / ataques de adivinación de contraseñas	Contraseñas inseguras	Moderado
Falla en recursos tecnológicos.	Deficiencia o carencia de mantenimiento, así como la falta de un programa para reemplazar componentes.	Moderado
Degradación o eliminación de elementos tecnológicos.	Falta de un protocolo para la eliminación de medios de almacenamiento.	Moderado
Perdida de equipos.	Extracción no autorizada de medios.	Moderado
Falla de energía eléctrica.	Falta de una UPS o su funcionamiento inadecuado.	Moderado
Sobrecalentamiento de componentes.	Deficiencias en el mantenimiento de la infraestructura eléctrica que respalda una UPS.	Moderado
Incidente en la prestación del servicio de internet.	Falta de una vía de internet alternativa.	Moderado
La falta de disponibilidad de servicios críticos (por ejemplo, correo electrónico o sitio web)	Falta de protocolos y prácticas de contingencia para (infraestructura física, hardware, software, personal y proveedores).	Moderado

Alteración de la integridad de los datos.	Falta de copias de seguridad.	Baja
Ineficiencia en las aplicaciones debido a problemas de funcionamiento del software.	Ausencia de planes de contingencia.	Baja
Terremoto en localización en el Cuarto de Telecomunicaciones.	Ausencia de planes de contingencia.	Baja
Incendio en localización en el Cuarto de Telecomunicaciones.	Ausencia de planes de contingencia.	Baja

Tabla 27. Determinación del Impacto.

5.2.6 Análisis de impacto.

Esta Metodología de NIST SP 800-30 para el análisis del impacto plantea el parámetro de Tipo de Impacto, este a su vez emparejado con el activo al que es afectado se determina un impacto máximo para cada activo, como se ve en la tabla 28.

Tipo de Impacto	**Activo Afectado por Impacto**	**Evento de Amenaza**	**Impacto Máximo**
Daño a los Activos	Daño o perdida de Activos de información	Realiza tácticas de suplantación en línea.	Alto
	Daño o perdida de Activos de información	Creación de una página web falsa.	Alto
	Daño o perdida de Activos de información	Elaborar certificados adulterados.	Bajo
	Daño o perdida de Activos de información	Comprometer la integridad al realizar acciones como la creación, eliminación o modificación de datos en sistemas	Bajo

		de información de acceso público.	
	Daño o perdida de Activos de información	Comprometer la integridad al contaminar o dañar datos esenciales.	Bajo
	Daño o perdida de Activos de información	Llevar a cabo acciones de captura de comunicaciones.	Moderado
	Daño o perdida de Activos de información	Adquirir datos confidenciales mediante la monitorización de redes externas.	Bajo
	Daño o perdida de Activos de información	Explotar VPNs.	Bajo
	Daño o perdida de Activos de información.	Distribuir software malicioso previamente identificado en los sistemas de información internos de la organización, como, por ejemplo, a través de correos electrónicos con virus.	Moderado
	Daño o perdida de Activos de información.	Aprovechar las vulnerabilidades presentes en los sistemas de información internos de la organización.	Moderado

	Daño o perdida de Activos de información.	Revelar la vulnerabilidad del software de los sistemas de información esenciales de la organización.	Baja
	Daño o perdida de Activos de información	Realizar intentos de inicio de sesión por fuerza bruta / ataques de adivinación de contraseñas.	Moderado
	Daño o perdida de Activos de información	Falla en recursos tecnológicos	Moderado
	Daño o perdida de Activos de información	Degradación o eliminación de elementos tecnológicos.	Bajo
	Daño o perdida de Activos de información	Perdida de equipos.	Moderado
	Daño o perdida de Activos de información	Falla de energía eléctrica.	Moderado
	Daño o perdida de Activos de información	Sobrecalentamiento de componentes.	Moderado
	Daño o perdida de Activos de información	Incidente en la prestación del servicio de internet.	Moderado
	Daño o perdida de Activos de información	La falta de disponibilidad de servicios críticos (por ejemplo, correo electrónico o sitio web)	Moderado
	Daño o perdida de Activos de información	Alteración de la integridad de los datos.	Moderado

	Daño o perdida de Activos de información	Ineficiencia en las aplicaciones debido a problemas de funcionamiento del software.	Moderado
	Daño o perdida en instalaciones físicas de la empresa Activos de información	Terremoto en localización en el Cuarto de Telecomunicaciones.	Bajo
	Daño o perdida en instalaciones físicas de la empresa.	Incendio en localización en el Cuarto de Telecomunicaciones.	Bajo
Daño a Otras Organización o Individuo	Daño a la confiabilidad en las relaciones.	Obtener acceso no autorizado.	Moderado

Tabla 28. Análisis del Impacto. Fuente: [4]

5.2.7 Determinación del riesgo.

Para la determinación de la inseguridad se ha considerado los eventos de las amenazas y su nivel de riesgo como se determina en la tabla 29.

EVENTOS DE AMENAZAS	NIVEL DEL RIESGO
Realiza tácticas de suplantación en línea	Bajo
Creación de una página web falsa.	Bajo
Elaborar certificados adulterados.	Muy Bajo
Comprometer la integridad al realizar acciones como la creación, eliminación o modificación de datos en sistemas de información de acceso público.	Bajo
Comprometer la integridad al contaminar o dañar datos esenciales.	Bajo
Llevar a cabo acciones de captura de comunicaciones.	Bajo
Acceder de manera no autorizada.	Bajo
Adquirir datos confidenciales mediante la monitorización de redes externas.	Bajo
Explotar VPNs.	Bajo
Distribuir software malicioso previamente identificado en los sistemas de información internos de la organización, como, por ejemplo, a través de correos electrónicos con virus.	Bajo

Aprovechar las vulnerabilidades presentes en los sistemas de información internos de la organización.	Moderado
Revelar la vulnerabilidad del software de los sistemas de información esenciales de la organización.	Bajo
Inducir la difusión de información importante y/o confidencial por parte de usuarios con autorización	Bajo
Logre acceso no autorizado.	Bajo
Obtener datos o información confidencial de sistemas de información de acceso público.	Moderado
Incorpore software malicioso específico en los sistemas de información de la organización y en sus componentes.	Bajo
Poner en riesgo los sistemas de información cruciales mediante la obtención de acceso físico.	Bajo
Realizar tácticas de ingeniería social que involucran a individuos externos con el fin de obtener información.	Moderado
Provocar la revelación de información crucial y/o confidencial por parte de usuarios con autorización.	Bajo
Inyectar software malicioso personalizado en los sistemas de información de la organización de acuerdo con las configuraciones del sistema.	Bajo
Aprovechar sistemas de información que están expuestos a Internet y que tienen configuraciones incorrectas o no autorizadas.	Bajo
Realizar intentos de inicio de sesión por fuerza bruta / ataques de adivinación de contraseñas.	Moderado
Realizar ingeniería social basada en información privilegiada para obtener información.	Bajo
Explotar las debilidades presentes en los sistemas de información internos de la organización.	Bajo
Causar la divulgación no autorizada y/o la indisponibilidad al exponer información confidencial.	Moderado
Falla en recursos tecnológicos	Moderado
Degradación o eliminación de elementos tecnológicos.	Moderado
Perdida de equipos.	Moderado
Falla de energía eléctrica.	Moderado
Sobrecalentamiento de componentes.	Moderado
Incidente en la prestación del servicio de internet.	Moderado
La falta de disponibilidad de servicios críticos (por ejemplo, correo electrónico o sitio web)	Bajo
Alteración de la integridad de los datos	Moderado
Ineficiencia en las aplicaciones debido a problemas de funcionamiento del software.	Bajo
Terremoto en localización del Cuarto de Telecomunicaciones.	Bajo
Incendio en localización del Cuarto de Telecomunicaciones.	Bajo

Tabla 29. Valoración del Nivel de Riesgo.

5.2.8 Documentación de resultados

Para la evaluación de la inseguridad como primer paso se realizó la recolección de información con el propósito de detectar posibles vulnerabilidades. Una vez completada la recopilación de la información, se identificó las fuentes de amenaza que la metodología NIST SP 800-30 provee. Como tercer paso se identificaron las vulnerabilidades usando la metodología de NIST SP 800-30, además se consideraron los niveles para medir los resultados :Muy Alto, Alto, Moderado, Bajo, Muy Bajo, y para seguir desarrollando la metodología NIST SP 800-30 se tuvieron presentes los eventos de amenaza con la vulnerabilidad identificada y las condiciones predispuestas, cada acontecimiento de amenaza posee una posibilidad de inicio de ataque , impacto, vulnerabilidades y su riesgo como se puede observar en la tabla 30.

1	2	3	4	5	6	7	8	9	10	11	12	13
EVENTOS DE AMENAZAS	FUENTES DE AMENAZAS	FUENTE CARACTERITICAS DE LAS FUENTES DE AMANEZAS			RELEVANCIA	PROBABILIDAD DE INICIACIÓN DEL ATAQUE	VULNERABILIDAD Y CONDICIONES PREDISPUESTAS	SEVERIDAD Y OMNIPRESENCIA	PROBABILIDAD DEL ATAQUE EXISTOSO	PROBABILIDAD GENERAL	NIVEL DE IMPACTO	RIESGO
		CAPACIDAD	INTENCION	OBJETIVO								
Realiza tácticas de suplantación en línea.	Agente Externo	Muy Baja	Alto	Alto	Posible	Alto	V01, CP01	Moderado	Muy Bajo	Muy Bajo	Alto	Bajo
Creación de una página web falsa.					Posible	Alto	V02, CP04	Moderado	Muy Bajo	Muy Bajo	Alto	Bajo
Elaborar certificados adulterados.					Posible	Bajo	V03, CP04	Bajo	Muy Bajo	Muy Bajo	Bajo	Muy Bajo

Comprometer la integridad al realizar acciones como la creación, eliminación o modificación de datos en sistemas de información de acceso público.					Posible	Bajo	V04, CP03	Bajo	Bajo	Bajo	Bajo	Bajo
Comprometer la integridad al contaminar o dañar datos esenciales.					Posible	Bajo	V05	Bajo	Bajo	Bajo	Bajo	Bajo
Llevar a cabo acciones de captura de comunicaciones.					Posible	Baja	V06	Moderado	Bajo	Bajo	Moderado	Bajo
Acceder de manera no autorizada.					Posible	Baja	V07, CP03	Moderado	Bajo	Moderado	Bajo	Bajo
Adquirir datos confidenciales mediante la monitorización de redes externas.					Posible	Baja	V08	Bajo	Bajo	Bajo	Bajo	Bajo

Explotar VPNs.					Posible	Baja	V09,CP01	Bajo	Bajo	Bajo	Moderado	Bajo
Distribuir software malicioso previamente identificado en los sistemas de información internos de la organización, como, por ejemplo, a través de correos electrónicos con virus.	Agente Interno				Predicho	Baja	V10	Baja	Bajo	Bajo	Moderado	Bajo
Aprovechar las vulnerabilidades presentes en los sistemas de información internos de la organización.	Agente Externo	Moderado	Muy Bajo	Muy Bajo	Posible	Moderado	V11	Moderado	Bajo	Moderado	Moderado	Moderado

Revelar la vulnerabilidad del software de los sistemas de información esenciales de la organización.					Posible	Baja	V12, CP02	Bajo	Bajo	Bajo	Moderado	Bajo
Inducir la difusión de información importante y/o confidencial por parte de usuarios con autorización					N/A	Moderado	-	Bajo	Bajo	Bajo	Moderado	Bajo
Logre acceso no autorizado.					N/A	Moderado	-	Bajo	Bajo	Bajo	Bajo	Bajo
Obtener datos o información confidencial de sistemas de información de acceso público.					N/A	Moderado	--	Bajo	Bajo	Moderado	Moderado	Moderado

Incorpore software malicioso específico en los sistemas de información de la organización y en sus componentes.					N/A	Moderado	-	Bajo	Bajo	Bajo	Moderado	Bajo
Poner en riesgo los sistemas de información cruciales mediante la obtención de acceso físico.					N/A	Moderado	-	Bajo	Bajo	Bajo	Moderado	Bajo
Realizar tácticas de ingeniería social que involucran a individuos externos con el fin de obtener información.					N/A	Moderado	-	Bajo	Bajo	Moderado	Moderado	Moderado

Provocar la revelación de información crucial y/o confidencial por parte de usuarios con autorización.					N/A	Moderado	-	Bajo	Bajo	Bajo	Moderado	Bajo
Inyectar software malicioso personalizado en los sistemas de información de la organización de acuerdo con las configuraciones del sistema.	Administrador	Bajo	Bajo	Bajo	N/A	Moderado	-	Bajo	Bajo	Bajo	Moderado	Bajo
Aprovechar sistemas de información que están expuestos a Internet y que tienen configuraciones incorrectas o no autorizadas.		Bajo	Bajo	Bajo	N/A	Bajo	-	Bajo	Bajo	Bajo	Moderado	Bajo

Realizar intentos de inicio de sesión por fuerza bruta / ataques de adivinación de contraseñas.		Bajo	Bajo	Bajo	Posible	Bajo	V13, CP04	Moderado	Bajo	Moderado	Moderado	Moderado
Realizar ingeniería social basada en información privilegiada para obtener información.		Bajo	Bajo	Bajo	N/A	Bajo	-	Bajo	Bajo	Bajo	Moderado	Bajo
Explotar las debilidades presentes en los sistemas de información internos de la organización.		Bajo	Bajo	Bajo	N/A	Bajo	-	Bajo	Bajo	Bajo	Bajo	Bajo
Causar la divulgación no autorizada y/o la indisponibilidad al exponer información confidencial.		Bajo	Bajo	Bajo	N/A	-	-	Bajo	Bajo	Moderado	Moderado	Moderado

Falla en recursos tecnológicos.	Comunicaciones	Moderado	Moderado	Moderado	Posible	-	V14, CP02	Moderado	Moderado	Alto	Moderado	Moderado
Degradación o eliminación de elementos tecnológicos.		Moderado	Moderado	Moderado	Posible	-	V15	Moderado	Moderado	Moderado	Moderado	Moderado
Perdida de equipos.		Moderado	Moderado	Moderado	Posible	-	V16, CP02	Moderado	Moderado	Moderado	Moderado	Moderado
Falla de energía eléctrica.	Fuente de energía.	Moderado	Moderado	Moderado	Posible	-	V17	Moderado	Moderado	Alto	Moderado	Moderado
Sobrecalentamiento de componentes.		Moderado	Moderado	Moderado	Posible	-	V18	Moderado	Moderado	Moderado	Moderado	Moderado
Incidente en la prestación del servicio de internet.	Red	Moderado	Moderado	Moderado	Posible	-	V19	Moderado	Moderado	Alto	Moderado	Moderado

La falta de disponibilidad de servicios críticos (por ejemplo, correo electrónico o sitio web)		Moderado	Moderado	Moderado	Posible	-	V20, CP01	Moderado	Bajo	Bajo	Moderado	Bajo
Alteración de la integridad de los datos		Bajo	Moderado	Moderado	Posible	-	V21	Bajo	Moderado	Moderado	Moderado	Moderado
Ineficiencia en las aplicaciones debido a problemas de funcionamiento del software.	Aplicativo de uso General.	Bajo	Moderado	Bajo	Posible	-	V22	Bajo	Moderado	Bajo	Moderado	Bajo
Terremoto en localización en el Cuarto de Telecomunicaciones.	Terremoto	Alto	Bajo	Bajo	Esperado	-	V23	Bajo	Bajo	Bajo	Bajo	Bajo
Incendio en localización en el Cuarto de Telecomunicaciones.	Incendio	Alto	Bajo	Bajo	Esperado	-	V24	Bajo	Bajo	Bajo	Bajo	Bajo

Tabla 30. Resumen de Riesgos. Fuente: [4]

6. Conclusiones

La implementación de una metodología de análisis de riesgos en la Dirección Distrital 14D01 se erige como una herramienta esencial para el establecimiento de políticas de seguridad de la información.

Mediante el desarrollo de dos metodologías de gestión de riesgos, hemos llegado a las siguientes conclusiones:

La metodología Magerit se inició con valoración de los activos y la parametrización de la evaluación, lo que nos permitió identificar las amenazas a las que se exponen dichos activos. A través del tratamiento de riesgos y una valoración cuantitativa, obtuvimos los niveles de riesgo asociados a cada activo. Esto, a su vez, proporciona una base sólida para que la Dirección Distrital pueda implementar normas y procedimientos destinados a proteger los recursos y la información institucional.

Por su parte, la metodología NIST SP 800-30 ofrece un conjunto completo de herramientas para identificar riesgos basados en eventos de amenazas. Además, en cada etapa de su metodología, se presentan tablas guía que permiten vincular eventos de amenazas con una valoración cualitativa de los riesgos que conllevan.

Luego de un exhaustivo estudio de ambas metodologías, hemos determinado que la que mejor se acopla a los requisitos de la institución es la metodología Magerit. Su enfoque en costos la hace más accesible y comprensible para la toma de decisiones tanto por parte del Director Distrital como del equipo técnico, en lo que se refiere a la gestión de riesgos en la seguridad de la información.

Referencias

[1] Incibe, (2015). “Gestión de Riesgos :una guía de aproximación para el usuario”, pag.8

[2] Ministerio de la hacienda y Administración Pública, (2012, Octubre 20) [Online].Available: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i- metodo/file.html

[3] Enisa, (2022,Junio). Ompendium Of Risk Management Frameworks With Potential Interoperability,pag .9-11

[4] National Institute of Standars and Tecnology, (2012, septiembre), “Guía de gestión de riesgos de los sistemas de tecnología de la información”, NIST, Publicación Especial 800-30 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy /SP/nistspecial publication800-30.pdf

[5] A.Mogollón, (2016). “Análisis Comparativo: Metodologías de análisis de Riesgos”.Universidad Centroccidental Lisandro Alvarado. [Online] Available :https://dsi.face.ubiobio.cl/sbravo/1-AUDINF/Comp%20Met%20An-Riesg.pdf

[6] O. Silva (2019, Junio) “Auditoría Informática aplicando la metodología OCTAVE de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado (GAD) de San Pedro de Pelileo” , Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos. [Online]. Available :https://repositorio.uta.edu.ec/jspui/bitstream/123456789 /30111/1/Tesis_ t1639si.pdf

[7] D.Espinosa, J.Martínez y S.Amador(2022,Junio). “Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S.” Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC. Ingenierías USBMed,5(2), 33-43.[Online]. Available: http://www.revistas.usb.edu.co/index.php/IngUSBmed/article/view/309/220

[8] J.Rivera,V.Salazar,V. Herrera,X. Ruiz y C.Guillen, (2019 ,Mayo) “Gestión de Riesgos de TIC en hospitales públicos”, [Online]. Available: https://www.proquest.com/openview/2e45495973142cf41bb3814cfecea9bc/

[9] IBM Corporation (2022). “IBM X-Force Threat Intelligence Índex.” [Online]. Avaible: https://www.ibm.com/downloads/cas/ADLMYLAZ.

[10] C. Torres (2016), "La importancia de realizar un análisis de riesgo en las empresas”, (Bachelor's thesis, Universidad Piloto de Colombia). [Online]. Available:http://repository.unipiloto.edu.co/handle/20.500.12277/2728. López Ramírez,

[11] J. Figueroa, R.Rodríguez, C. Bone y J. Saltos, (2018). “La seguridad informática y la seguridad de la información.”, *Polo del conocimiento*, *2*(12), 145-155, [Online]. Avaible: https://polodelconocimiento.com/ojs/index.php/es/article/view/420

[12]A. Infante, J. Infante y J. Gallardo ,(2022). “Factores claves para concienciar la ciberseguridad en los empleados.” *Revista de Pensamiento Estratégico y Seguridad CISDE*, *7*(1), 69-79. [Online]. Avaible: http://uajournals.com/ojs/index.php/cisdejournal/article/view/1126 .

[13] J. Sánchez and M. Ignoto,(1991), “La seguridad informática ”.[Online] .Avaible: http://www.iesaguadulce.es/gestiona/datos/programaciones/FP_SMR_2/SEGIN_29920697/2021_22/programacion_220388.pdf

[14] T.Jiménez (2018). “Análisis y evaluación de riesgos, de los activos de información de la Dirección Ejecutiva Seccional de Administración Judicial de Tunja - DESAJT, adoptando una metodología de gestión de riesgos de los sistemas de información” ,Monografia, Universidad Nacional Abierta y a Distancia UNAD. [Online]. Avaible: https://repository.unad.edu.co/handle/10596/21575.

[15] J. Rodriguez y I.Peralta (2013). “Gestión de Riesgos Magerit” . [Online].Avaible:https://www.tithink.com/publicacion/MAGERIT.pdf

[16] R.Castillo (2022). “Desarrollo de una aplicación web y móvil para la gestión de riesgos de seguridad de la información aplicado a una empresa de de sistemas.”[Online].Avaible: https://cybertesis.unmsm.edu.pe/handle/20.500.12672/18129

[17] Lopez Luis,(2017),” Analisis de gestión de Riesgos Informáticos”. [Online].Avaible: https://contenidos.areandina.edu.co/repo/modulos/IS/247_Analisis_de_riesgo

s_informaticos/Publicar/referentes/recursos/eje3/pdf/Referente_Pensamiento consultoría _Eje_3.pdf

[18] H. Alemán y C. Rodríguez, (2015) "Metodologías para el análisis de riesgos en los sgsi", Publ. investig., vol. 9, pp. 77 , oct. 2015.[Online]. Available:https: //hemerotecaunad. edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754

[19] [Online]. Available:. https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/ediciones-especiales/item/13006-edicion-especial-no-641

[20] [Online]. Available:https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/17420-quinto-suplemento-al-registro-oficial-no-160.

[21] J.Miranda ,(2021) . " Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos". [Online] Available: https://dspace.ups.edu.ec/handle/123456789/20966.

[22] J.Recalde, (2019), " Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS ",(Bachelor's thesis, Quito, 2019). [Online]. Available:https://bibdigital.epn.edu.ec/bitstream/15000/20530/1/CD%2010022.pdf

[23] A. Vieites, (2011), "Enciclopedia de la seguridad informática", Editorial RA-MA. [Online].Available:https://books.google.es/books?hl=es&lr=&id=Bq8DwAAQBAJ&oi=fnd&pg=PT2&dq=Enciclopedia+de+la+Seguridad+Inform%C3%A1tica.+2%C2%AA+edici%C3%B3n&ots=dxs22hYdhJ&sig=MUu7Pz54PbjwgB8mdAnQoCbr7aU#v=onepage&q&f=false