UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

Análisis y Gestión de Riesgos de los Sistemas de Información en el proceso de georeferenciado y empadronamiento de conexiones eléctricas en tiempos de pandemia en una empresa eléctrica del Perú

Tesis para obtener el Título Profesional de Ingeniero de Sistemas

Por:

Noemí Elizabeth Colquehuanca Cabana

Asesor:

Mg. Nilton Omar Santillan Aching

Juliaca, julio de 2022

DECLARACIÓN JURADA DE AUTORÍA DEL INFORME DE TESIS

Nilton Omar Santillan Aching, de la Facultad de Ingeniería y Arquitectura, Escuela Profesional de Ingeniería de Sistemas, de la Universidad Peruana Unión.

DECLARO:

Que el presente informe de investigación titulado: *"***ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN EN EL PROCESO DE GEOREFERENCIADO Y EMPADRONAMIENTO DE CONEXIONES ELÉCTRICAS EN TIEMPOS DE PANDEMIA EN UNA EMPRESA ELÉCTRICA DEL PERÚ***"* constituye la memoria que presenta la Bachiller **Noemí Elizabeth Colquehuanca Cabana** para obtener el título de Profesional de Ingeniero de Sistemas, cuya tesis ha sido realizada en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente declaración en Juliaca, a los 12 días del mes de julio del año 2022

Mg. Nilton Omar Santillan Aching
Asesor

162

ACTA DE SUSTENTACIÓN DE TESIS

En Puno, Juliaca, Villa Chullunquiani, a 04 día(s) del mes de Julio del año 2022 siendo las 15:00 horas, se reunieron en el Salón de Grados y Títulos de la Universidad Peruana Unión, Filial Juliaca, bajo la dirección del Señor Presidente del jurado: Msc. Fredy Abel Huanca Torres, el secretario: Mtro. Roel Dante Gomez Apaza y los demás miembros: Msc. Benazir Francis Herrera Yucra Mg. Abel Angel Sullon Macalupu y el asesor Mg. Nilton Omar Santillan Aching con el propósito de administrar el acto académico de sustentación de la tesis titulada: Análisis y Gestion de Riesgos de los Sistemas de Información en el proceso de georeferenciado y empadronamiento de conexiones eléctricas en tiempos de pandemia en una empresa eléctrica del Perú de el(los)/la(las) bachiller/es: a) Noemi Elizabeth Colquehuanca Cabana b) conducente a la obtención del título profesional de Ingeniero de Sistemas

(Nombre del Título Profesional)

con mención en

El Presidente inició el acto académico de sustentación invitando al (los)/a(la)(las) candidato(a)/s hacer uso del tiempo determinado para su exposición. Concluida la exposición, el Presidente invitó a los demás miembros del jurado a efectuar las preguntas, y aclaraciones pertinentes, las cuales fueron absueltas por el(los)/la(las) candidato(a)/s. Luego, se produjo un receso para las deliberaciones y la emisión del dictamen del jurado.

Posteriormente, el jurado procedió a dejar constancia escrita sobre la evaluación en la presente acta, con el dictamen siguiente:

Candidato (a): Noemi Elizabeth Colquehuanca Cabana

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	
Aprobado	16	B	Bueno	Muy Bueno

Candidato (b):

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	

(*) Ver parte posterior

Finalmente, el Presidente del jurado invitó al(los)/a(la)(las) candidato(a)/s a ponerse de pie, para recibir la evaluación final y concluir el acto académico de sustentación procediéndose a registrar las firmas respectivas.

Presidente

Secretario

Asesor

Miembro

Miembro

Candidato/a (a)

Candidato/a (b)

AGRADECIMIENTOS

A Dios por permitirme cumplir mis metas, a la Universidad Peruana Unión, alma máter, a los Ingenieros, Magísteres que siempre tuvieron disposición de ayudarme con su asesoramiento y compartir sus conocimientos conmigo y finalmente al personal de la contratista gracias por su apoyo y compromiso para desarrollar este proyecto.

DEDICATORIA

A Dios, que siempre está junto a mi iluminando mi camino. A mis padres, Gregorio Colquehuanca y Sofia Cabana, lo más preciado que tengo y quienes han sido un apoyo incondicional a seguir adelante en cada etapa de mi vida, a mis hermanos, padrinos y amistades por respaldarme con su apoyo.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

Análisis y Gestión de Riesgos de los Sistemas de Información en el proceso de georeferenciado y empadronamiento de conexiones eléctricas en tiempos de pandemia en una empresa eléctrica del Perú

RESUMEN:

La investigación consiste en desarrollar el análisis y gestión de riesgos de los sistemas de información que permite el proceso de georeferenciado y empadronamiento de conexiones eléctricas de una de las empresas vinculadas al sector eléctrico. Debido a la pandemia, surgió la inmovilización de actividades, pero que también excluían a los servicios básicos y públicos, generando el teletrabajo y surgieron muchas dificultades en los sistemas de información, conllevando algunos problemas en garantizar cumplimientos de contratos como la falta de acceso y disponibilidad a los sistemas. Teniendo preeminencia, porque las empresas terciarias del sector eléctrico han optado por implementar la gestión de riesgos, al ser dependiente de una concesionaria eléctrica del sector peruano para brindar continuidad del servicio, lo que conlleva a comprender la exposición de los activos que afecta los procesos para mitigar los riesgos. Metodológicamente se aplicó en 3 fases según Magerit en: i) Identificación y valorización de los activos críticos, lo que permite conocer la situación del problema, ii) Evaluación de las amenazas y mitigación con las salvaguardas, el cual gestiona el problema dando una solución al daño, iii) Estimación del impacto y del riesgo, quien ejecuta la gestión de la fase 2, donde el impacto muestra el daño posible, mientras que el riesgo muestra el daño probable. Determinando los siguientes resultados: i) Realización del análisis para identificar a los 17 activos críticos con un status de alto nivel, ii) Se analizó las amenazas de acuerdo a los activos críticos dando solución con las salvaguardas generando un bajo nivel dentro de las amenazas identificadas, iii) Se estimó el nivel de impacto obteniendo como resultado un nivel medio y también se estimó el riesgo con un status bajo. Siendo aceptado por la concesionaria y contratista. De esta forma, se garantiza el desarrollo de las actividades planificadas de forma eficiente.

Palabras clave: análisis, gestión de riesgos, sistemas de información, magerit, pandemia, georeferenciado y empadronamiento.

Analysis and Risk Management of Information Systems in the process of geo-referencing and registration of electrical connections in times of pandemic in an electric company in Peru

ABSTRACT:

The research consists of developing the analysis and risk management of the information systems that allow the process of geo-referencing and registration of electrical connections of one of the companies linked to the electricity sector. Due to the pandemic, the immobilization of activities arose, but also excluded basic and public services, generating telework and many difficulties arose in the information systems, leading to some problems in ensuring compliance with contracts such as lack of access and availability to the systems. Having preeminence, because tertiary companies in the electricity sector have chosen to implement risk management, being dependent on an electricity concessionaire in the Peruvian sector to provide continuity of service, which leads to understanding the exposure of assets that affect the processes to mitigate risks. Methodologically it was applied in 3 phases according to Magerit en: i) Identification and valuation of critical assets, which allows us to know the situation of the problem, ii) Threat assessment and mitigation with safeguards, which manages the problem by providing a solution to the damage, iii) Impact and risk estimation, who performs phase 2 management, where the impact shows the possible damage, while the risk shows the probable damage. The following results were obtained: i) Analysis was performed to identify the 17 critical assets with a high level status ii) Threats were analyzed according to critical assets, providing a solution with the safeguards, generating a low level within the identified threats, iii) The level of impact was estimated, resulting in a medium level, and the risk was also estimated with a low status. Being accepted by the concessionaire and contractor. This ensures that the planned activities are carried out efficiently.

Keywords: analysis, risk management, information systems, magerit, pandemic, georeferenced and registration.

1 INTRODUCCIÓN

Para el éxito y continuidad de los servicios que brindan las grandes organizaciones requieren del uso de las tecnologías convirtiéndose así la información en un activo vital [1] [2]. Cabe precisar, el aseguramiento de la información y los sistemas que la procesan son objetivos primordiales de una organización, por lo tanto, la evaluación y gestión del riesgo se convierte así en una prioridad; más aún, cuando la empresa comercializadora y distribuidora de energía eléctrica, a quien en adelante se le denominara la concesionaria, terciariza el desarrollo de sus actividades para brindar de forma adecuada los servicios de energía eléctrica.

Se debe comprender que la crisis sanitaria por el contagio del Covid-19 afectó a muchas industrias teniendo que paralizar sus actividades, pero las empresas de servicios básicos y públicos tuvieron que continuar con sus actividades [3], por lo que se pasó al teletrabajo [4]. Es importante indicar que, estos cambios ocasionaron dificultades en la continuidad de los contratos de muchos servicios ya que se tenían que cumplir con los protocolos de seguridad impuestos por el gobierno, lo que generó mayores costos y riesgos en la salud de los trabajadores. Para las empresas de servicios eléctricos, es vital que sus sistemas de información se mantengan operativos [5], porque la falta de acceso y disponibilidad a los sistemas dificulta la entrega normal los servicios tercerizados [6] que proveen informa-ción actualizada para que dichos procedimientos operen a un nivel adecuado [7] [8] [9]. En los sistemas de informa-ción Sielse y Gos [10] brindados por la Concesionaria [11] que afecta la idoneidad y oportunidad de la entrega de in-formación en la cadena de los servicios que presentaron inconvenientes antes mencionados para la continuidad del contrato encargado a la empresa Contratista. Internamente se desarrolló un aplicativo e implementación de equipa-miento, pero aún con la información la contratista se veía afectada por la falta de conectividad, accesos y falta de apoyo de los encargados de la concesionaria que afectaban el cumplimiento del con-trato [12], cuyas actividades realizadas por terceros inicia desde la prestación de diferentes servicios y componentes necesarios para la producción. Según estudios realizados, el porcentaje de con-fianza ronda el 95% que aporta las diligencias de tercerización [13] [14]. En este sentido, [15] recomienda implementar un gobierno de TI como base para implementar la gestión de seguridad y el riesgo de seguridad en un ambiente de TI. Así mismo, [16] sugiere a la gestión de riesgos estrategias esenciales para el cumplimiento de objetivos.

Para minimizar el riesgo del uso de las tecnologías de información (TI), [17] aplicó el método Magerit para valores precisos en diferentes escalas, ya que [18] expone el análisis y gestión de riesgos ser fundamental, enfatizando Magerit para un mejor desempeño en el gobierno de TI. [19] también aplicó métodos con características propias entre sí, teniendo como limitante su valides teórica. [20] Aborda el análisis de riesgo de las necesidades del negocio, de manera estructurada, coherente y apoyada en matemáticas para que los resultados sean más efectivos, permitiendo establecer procesos de mejora continua. [21] Desarrolló un plan de gestión de riesgos para garantizar la resiliencia. Para asegurar suministros de agua en los hospitales, se puede utilizar el mismo método para desarrollar planes sólidos de gestión de riesgos para garantizar que se construya y mantenga la resiliencia en otras industrias. [22] propuso un modelo de gestión de riesgos con base a la efectividad de los controles propuestos por la ISO 27004 la metodología Magerit, en una PYME farmacéutica en Lima, Perú, disminuyendo el riesgo en un 71%. Sin embargo, no se encontraron estudios sobre el análisis y gestión de riesgo de los Sistemas de Información (SI) en el pro-ceso de georeferenciado y empadrona-miento de conexiones eléctricas durante la pandemia de una empresa eléctrica peruana.

Así pues, resultó pertinente desarrollar el análisis y gestión de los riesgos de los SI para de esta forma mitigar o disminuir los riesgos y asegurar el cumplimiento del servicio de georeferenciado y empadronamiento de conexiones eléctricas y no generar pérdidas económicas, penalizaciones o afectaciones en la reputación de la empresa.

A continuación, se describen los principales conceptos que deben entenderse para el estudio:

1.1 Análisis y gestión de riesgos

El análisis de riesgos, es desarrollar el entendimiento del riesgo. Suministra una entrada para las decisiones, si es necesario tratar los riesgos y las estrategias de trata-miento del riesgo más adecuadas y eficaces en términos de costo. El análisis implica la consideración de las fuentes de riesgo, sus consecuencias positivas y negativas y la posibilidad de que puedan ocurrir [23]. También, establece claramente que es un paso que incluye dos aspectos esenciales: identificar las amenazas que enfrenta una entidad y evaluar su capacidad de materialización [24]. Por otro lado, forman un sistema para definir el nivel de vulnerabilidad y el impacto de un ataque que causaría; esto le ayudara a elegir las medidas más apropiadas [25].

Es así que, la gestión de riesgos se define como una parte integral del proceso de gestión. Es un proceso multifacético, cuyos aspectos apropiados los realiza con frecuencia un equipo multi-disciplinario. Es un proceso iterativo de mejora continua [26]. También se define como parte fundamental de la continuidad de negocios, es la gestión de incidentes y a su vez está se relaciona con la gestión de riesgos. La adecuada gestión de incidentes evita que sean activados los planes de continuidad de negocios, por ello es importante que las respuestas a incidentes sean efectivas y se tengan claros los riesgos que pue-den estar asociados [27]. Para ello existen métodos como: COSO, CRAMM, Octave, Mehari, Magerit entre otros.

Es así que Magerit (Fig.1) se diferencia de otros métodos en sus objetivos como concientizar a los responsables de los sistemas de in-formación sobre la existencia de riesgos y la necesidad de gestionar-los, proporciona un enfoque sistemático para analizar dichos riesgos, ayuda a identificar y planificar las medidas adecuadas para controlarlos [28]. Aparte de proporcionar una guía completa sobre como realizar el análisis de riesgos paso a paso y gestionarlos, ya que consta de tres guías: método, catálogo de elementos y guía de técnicas.

En relación con este tema, en un estudio donde las empresas requieren altos niveles de disponibilidad de información y algunos incluso requieren niveles ininterrumpidos, donde el análisis de riesgo con Magerit es esencial para garantizar la seguridad de la información, desarrollando un plan de contingencia en equipos y sistemas informáticos, logrando desarrollar medidas preventivas y correctivas apropiadas [29]. En otro estudio, resalta el uso de Magerit en empresas e instituciones desde pequeñas a grandes, lo que facilita su integración en la gestión técnica de riesgos. También adopta las mejores prácticas de la ISO 27001, 15408, 17799 y 13335. Sin embargo, para la gestión de riesgos se alinea correctamente con los requerimientos de la ISO 27005 e ISO 31000. Desarrolla procesos para su implementación dentro de la planificación y lanzamiento de un proyecto, que resulte en una ganancia o pérdida financiera [30].

Figura 1. Magerit

1.2 Georeferenciado y empadronamiento de conexiones eléctricas

El georeferenciado permite la ubicación exacta en sistema de coordenadas UTM (Universal Transverse Mercator) de una conexión eléctrica.

El empadronamiento registra las características propias como número de contrato, medidor, marca, modelo, serie, evidenciado con fotos de cada conexión eléctrica.

2 METODOLOGÍA

El estudio se basa en el método Magerit, por sus siglas metodología de análisis y gestión de riesgos de los sistemas de información [31], donde se implementa un proceso de 3 fases (Fig.2) para el análisis y gestión de riesgos de los SI en el marco de la organización de gestión para asegurar el cumplimiento del servicio de georeferenciado y empadrona-miento de conexiones eléctricas de la contratista.

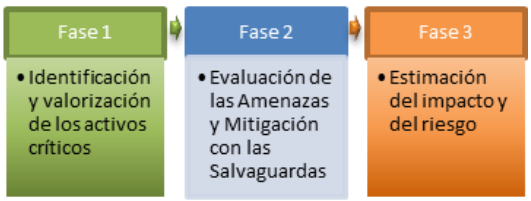

Figura 2. Adaptado de la metodología Magerit

El proceso inicia con la fase 1 donde se identificaron los activos críticos, para lo cual se realizó reuniones con responsables de la contratista, por lo que también se procedió a reunirse con otras contratistas dependientes de la concesionaria del sector eléctrico, apoyados a las técnicas y procedimientos de scamper el cual se define como una lluvia de ideas en equipo, el análisis de premisas, la revisión, el análisis documental y entrevistas no estructuradas, aplicado de manera presencial con inferencia de datos subjetivamente.

Se realizó un inventario determinando los activos en función a la clasificación publica, interna y restringida. Las categorías en función de los activos de información, software, hardware, personal y servicios, como se describe e identifica en la siguiente tabla:

Tabla 1.
Categorización de activos.

Tipo	Código	Categoría	Especificación
Activos de Información	AI1	Inf. Escrita	Estatutos, Informes, Fichas
	AI2	Inf. Electrónica	Factura Electrónica, Correos, BD
	AI3	Inf. Hablada	Llamadas, Video conferencias
Activos de Software	AS1	Sw. para Administración de BD	PosgresSql, Mysql
	AS2	Sw. Herramientas y Utilitarios	Microsoft Office, Access
	AS3	Sw. Internamente desarrollado	Aplicativo
	AS4	Sw. desarrollado por terceros	Oracle, SAP
	AS5	Sw. por Otros servicios	GOS, SIELSE
Activos de Hardware	AH1	Hw. de Procesamiento	Servidores, Laptop, Pc's
	AH2	Hw. de Comunicaciones	Telefonía, switch
	AH3	Hw. de Almacenamiento	External Hard Drive, USB
	AH4	Equipamiento y Mobiliario	GPS, Cargadores, UPS, Carpetas
Personal	AP1	Empleados	Personal Interno
Servicios	AS1	Servicio Público	Energía Eléctrica

La valorización de activo, en una escala desde muy bajo a muy alto es dependiente del estudio de dimensiones (D) de: confidencialidad (información en privado), integridad (información incompleta) y disponibilidad (información no útil). De acuerdo a la información (D) que podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio en la reputación de la empresa y/o afectar dentro de la organización, en la tabla 2 se muestra los valores de las dimensiones para su evaluación generando el valor de activo siendo el promedio de las dimensiones. Por consiguiente, es determinada en una escala de apreciación del activo: bajo = 1 - 1.5, medio = 1.5 - 3.5 y alto = 3.5 - 5. Estos se evalúan en base a los criterios técnicos y de valoración de la contratista.

Tabla 2.
Cuadro de dimensiones.

Valor	Confidencialidad	Integridad	Disponibilidad
5 MUY ALTO	Si la información no se conserva en privado podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio irreversible en la reputación de la empresa	Si la información falta o está incompleta podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio irreversible en la reputación de la empresa	Si la información no es útil podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio irreversible en la reputación de la empresa
4 ALTO	Si la información no se conserva en privado podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio grave en la reputación de la empresa	Si la información falta o está incompleta podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio grave en la reputación de la empresa	Si la información no es útil podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio grave en la reputación de la empresa
3 MEDIO	Si la información no se conserva en privado podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio considerable en la reputación de la empresa	Si la información falta o está incompleta podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio considerable en la reputación de la empresa	Si la información no es útil podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio considerable en la reputación de la empresa
2 BAJO	Si la información no se conserva en privado podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio parcial en la reputación de la empresa	Si la información falta o está incompleta podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio parcial en la reputación de la empresa	Si la información no es útil podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio parcial en la reputación de la empresa
1 MUY BAJO	Si la información no se conserva en privado podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio no impactando en la reputación de la empresa. Aunque podría afectar dentro de la organización.	Si la información falta o está incompleta podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio no impactando en la reputación de la empresa. Aunque podría afectar dentro de la organización	Si la información no es útil podría permitir causar efectos negativos; factores como procesos administrativos o penalidades originando perjuicio no impactando en la reputación de la empresa. Aunque podría afectar dentro de la organización.

Continuando con el proceso, la fase 2, se procedió a identificar las amenazas para cada activo de información, se dividen en 4 tipos de amenazas (tabla 6), de naturaleza (N) lluvias y temblores, de humanos (H) carencia de profesionales y personal clave, en instalaciones (I) ausencia de energía y desperfecto de suministros, en tecnología (T) internet o perdida de información. Su nivel de impacto es su valoración respecto al daño donde:1= no impactando, 2= parcial, 3= considerable, 4= grave y 5= irreversible, en relación a las dimensiones como se aprecia en la tabla 2 y su frecuencia en los valores: 5= una vez al día, 4= una vez a la semana, 3= una vez a la quincena, 2= una vez al mes y 1= una vez al mes y medio. Determinando por fórmula: Nivel de Amenaza= (N. de Impacto+ Frecuencia de amenazas) /2

Asimismo, las salvaguardas o contra medidas de las amenazas, permitió medir los impactos y riesgos que están expuestos los activos a gestionarlos. Se evaluó e identifico el nivel de capacidad de controlamientos de protección existentes siendo Preventivos, Detectivos y Correctivos como se muestra en la tabla 3, en relación a las dimensiones respectivamente, para así determinar el nivel de vulnerabilidad: N. Vulnerabilidad = (NC(Preventivo)+ NC(Detectivo)+ NC(Correctivo)/D)

Tabla 3.
Nivel de capacidad.

Valor		Descripción
5	Inconclusos	Controles no cumplen el propósito
4	Ejecutados	Controles determinados cumple su finalidad(indocumentado)
3	Gestionados	Controles se ejecuta
2	Específicos	Controles definidos por la empresa
1	Predecibles	monitorear, controlar y corregir con medidas establecidas

Finalmente, en la fase 3 la estimación del impacto, proviene de la probabilidad de ocurrencia (PO) de los activos que se obtiene del promedio del nivel de amenazas y nivel de vulnerabilidad reflejando el daño que probablemente ocurra. En la determinación se evaluó e identifico en base a criterios financieros y operativos como principales riesgos del servicio como se muestra en la tabla 4. Seguidamente la estimación del riesgo es el producto de PO y del impacto. Siendo determinado en escala, bajo del 1 al 10, medio del 10 al 17 y alto del 17 al 25.

Tabla 4.
Escala del riesgo financiero y operativo.

Valor	Financiero	Operativo
5	Perjuicio igual o mayor que 2500	Daño de forma irreversible la operatividad de procedimientos de la empresa
4	Perjuicio igual o mayor que 2000 y menor que 2500	Daño de forma grave la operatividad de procedimientos de la empresa
3	Perjuicio igual o mayor que 1500 y menor que 2000	Daño de forma considerable la operatividad de procedimientos de la empresa
2	Perjuicio igual o mayor que 1000 y menor que 1500	Daño parcial en la operatividad de procedimientos de la empresa
1	Perjuicio menor que 1000	No impacta en los procedimientos de la empresa

3 RESULTADOS

3.1 Referidos a los activos críticos

Se efectuó la lista de información esencial a ejecutar por parte de la contratista de acuerdo a las bases con la concesionaria para la culminación del servicio sin afectar la garantía de la buena pro.

Como se muestra en la tabla 5, de acuerdo a la categorización, clasificación y dimensiones definidas de confidencialidad, integridad y disponibilidad, se identificó a 17 activos críticos en un 100% calificado en un nivel de apreciación alto del riesgo, describiendo las dificultades y generando el análisis del riesgo en la realidad de la situación del avance del proceso, para el cumplimiento del contrato en el tiempo de la pandemia.

Tabla 5.
Activos críticos

Activos Críticos	Datos		Dimensiones			Escala de Apreciación
	CAT.	CLAS.	C	I	D	
Activos de Información						
Fichas de Empadronamiento de los suministros de los clientes	AI1	R	4	3	4	Alto
Fichas de Accesos a Recursos Informáticos a Concesionaria	AI1	I	4	4	3	Alto
Fichas de Notificaciones de Suministros por cliente	AI1	I	4	3	5	Alto
Registro de Credenciales de Empadronadores	AI1	I	3	4	4	Alto
Backup's	AI2	R	4	4	4	Alto
Activos de Software						
Database	AS1	I	4	4	5	Alto

GOS	AS5	R	3	4	5	Alto
SIELSE	AS5	R	4	4	5	Alto
Activos de Hardware						
Database Server	AH1	R	4	4	5	Alto
PC's	AH1	R	4	3	4	Alto
Plotters	AH4	I	3	4	4	Alto
Celulares	AH2	I	4	4	4	Alto
GPS	AH4	I	4	4	5	Alto
Activos de R.R.H.H.						
Analista de Sistemas	AP1	I	4	3	4	Alto
Soporte TI	AP1	I	3	4	4	Alto
Activos de Servicio						
Internet	AS1	I	3	3	5	Alto
Luz	AS1	I	3	4	5	Alto

3.2 Referidos a las amenazas y salvaguardas

Teniendo definidos los 17 activos críticos se determinó y evaluó las amenazas de acuerdo a su tipo de amenaza, la descripción de la amenaza en afinidad a los activos críticos para establecer su impacto y frecuencia, siendo gestionados los peligros con las salvaguardas en relación a las dimensiones de confidencialidad, integridad y disponibilidad con los controlamientos de protección preventivo, detectivo y correctivo definidos.

Por lo tanto, a través de la gestión de riesgos se logra un 100% de valor agregado de los activos críticos clave, como se muestra en la tabla 6, permitiendo definir las soluciones inmediatas a la situación real del avance y cierre del proceso para el cumplimiento del contrato.

Tabla 6.

Amenazas y salvaguardas.

Activos Críticos	**Tipo Amen.**	**DETALLE**	**Impacto**	**Frecuencia**	**Salvaguardas C I D**	**Control: P D C**	**Escala de Apreciación.**
1	H	Retraso en la entrega de fichas por Sub Estación de Transformación.	5	5	Acceso a validar suministros en el sistema	1	Bajo
					Suministros registrados con fotos	2	
					Entregable por SET Y SED	1	
2	T	No accesos a recursos del software y falta de órdenes de servicio y trabajo.	5	5	Acceso a órdenes	1	Bajo
					Información en servidor	1	
					Continuidad del servicio	1	

3	H	No lograr ingresar al suministro.	4	5	Autorización del supervisor y/o coordinador de Concesionaria	1	Bajo
					Planificación	2	
					Acceso por suministro	1	
4	H	Sin acceso de usuario y sin credencial.	3	5	Acceso y autorización a empadronador	1	Bajo
					Capacitado	2	
					9 horas por 6 días	1	
5	T	No tener copias de seguridad.	4	4	Acceso a datos	1	Bajo
					Filtración de datos	1	
					Observaciones	1	
6	H	Datos del suministros empadronados	4	5	Acceso a consulta de base de datos no autorizadas	1	Bajo
					Validación de información	1	
					Actualización de información	1	
7	T	Caída de la app móvil.	3	5	Accesos independientes	1	Bajo
					Información de campo	1	
					Recopilación de datos	1	
8	T	Aplicación web no accesible.	4	5	Acceso con superusuario, estabilizar el acceso web	1	Bajo
					Autorización, privilegios	2	
					Trazabilidad de información	1	
9	T	Perdida de datos, productividad de la empresa.	5	4	Acceso limitado, Respaldo de servidor	1	Bajo
					Sin interferencia	1	
					Información accesible	1	
10	H	Ip's inaccesibles	4	5	Acceso a generar ip's	1	Bajo
					Configuración	1	
					Acceso sin fallas	1	
11	H	Sin catastros	3	4	Accesible a personal	1	Bajo
					Buen funcionamiento	1	
					Operativo	1	
12	H	Registrado sin acceso y móvil inoperativo	4	5	App interna de encarpetado	1	Bajo
					Baterías de recarga	1	
					Acceso a apps, móvil encendido	1	
13	T	No obtener la coordenadas	5	4	GPS por la contratista	1	Bajo

		geográficas (sistema en UTM) del suministro en app.			Memoria externa Suministro con coordenadas	1 1	
14	H	Contraste de información.	5	4	Autenticidad Responsabilidad Fiabilidad	1 1 1	Bajo
15	H	Falta de apoyo.	4	5	Asistencia a infraestructura tecnológica Maquinas, herramientas y equipos de ti en buen funcionamiento Asistencia remota	1 1 1	Bajo
16	I	No conectividad.	4	5	Aumentar el ancho de banda Firewall SSL para https	1 1 1	Bajo
17	I	Ausencia de energía.	4	4	Generador eléctrico Protección del equipo dentro de la organización Transferencia automática, Ups	1 1 1	Bajo

3.3 Referidos a la estimación del impacto y riesgos

Se determinó la estimación del impacto (ver tabla 7) en una escala de nivel medio en su totalidad, conforme a la fase 2 que permite precisar la probabilidad, manifestando el avance de los activos críticos del nivel alto a un nivel bajo al gestionarlos.

Por consiguiente, permitió determinar la estimación del riesgo (ver tabla 7), teniendo de importancia los peligros financieros y operativos, el cual genera un acorde a la escala en un status bajo, con excepción de un activo de nivel medio siendo el internet porque se ha convertido en un canal de comunicación indispensable dependiente de un proveedor, resultando aceptable para comprometer a la concesionaria y contratista empresa terciaria del sector eléctrico en la pandemia, a la culminación del servicio de georeferenciado y empadronamiento de conexiones eléctricas.

Tabla 7.
Estimación del impacto y riesgo.

Estimación del Impacto			Estimación del Riesgo			
Activos Críticos	Probabilidad	Escala	Financiero	Operativo	Valor de Riesgo	Nivel de Riesgo
1	3.2	Medio	3	3	9.5	Bajo
2	3	Medio	3	3	9.0	Bajo
3	3	Medio	3	3	8.7	Bajo
4	2.7	Medio	3	4	9.3	Bajo
5	2.5	Medio	4	3	8.8	Bajo
6	2.8	Medio	3	3	8.3	Bajo
7	2.5	Medio	3	2	6.3	Bajo
8	2.9	Medio	3	3	8.7	Bajo
9	2.8	Medio	3	3	8.3	Bajo
10	2.8	Medio	3	4	9.6	Bajo
11	2.3	Medio	3	3	6.8	Bajo
12	2.8	Medio	3	4	9.6	Bajo
13	2.8	Medio	4	3	9.6	Bajo
14	2.8	Medio	3	4	9.6	Bajo
15	2.8	Medio	3	3	8.3	Bajo
16	2.8	Medio	4	4	11.0	Medio
17	3	Medio	3	4	8.8	Bajo

4 CONCLUSIONES

El análisis realizado permitió evidenciar la situación de la contratista como se observó en la tabla 5, respecto al proceso de georeferenciado y empadronamiento de conexiones eléctricas en la pandemia. En la tabla 6, se realizó la gestión de los riesgos garantizando la culminación del contrato como se aprecia en la tabla 7, comprometiendo a ambas partes tanto concesionaria como contratista.

Así, esta metodología propuso el análisis y gestión de riesgos de los sistemas de información en base a estándares de Magerit para el proceso de georeferenciado y empadronamiento de conexiones eléctricas para el suministro de electricidad en tiempos de pandemia. La implementación objetiva determina seguir el estándar que permite el cumplimiento del proceso con eficacia y eficiencia para lograr con éxito la meta de la contratista siendo el proceso más óptimo; por lo que futuros estudios podrían incluir los riesgos de diferentes servicios tercerizados.

REFERENCIAS

[1] J. C. García Vázquez, «Las TIC en la pandemia Covid-19,» *Nuevo Hospital,* vol. XVI, 2020.

[2] G. E. Cano Pita, «Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones,» *Revista Cientifica Dominio de las Ciencias,* vol. 4, nº 1, pp. 499-510, 2018.

[3] Presidencia del Consejo de Ministros, «Decreto Supremo 044-2020-PCM,» *El Peruano,* 15 marzo 2020.

[4] P. d. C. d. Ministros, «Decreto de Urgencia N°026-2020,» *El Peruano,* marzo 2020.

[5] Miniterio de economia y finanzas-MEF, «Sistema Nacional de Programación Multianual y Gestión de inversiones invierte.pe,» 26 setiembre 2019. [En línea]. Available: https://www.gob.pe/852-sistema-nacional-de-programacion-multianual-y-gestion-de-inversiones-invierte-pe.

[6] EL Peruano, «Ley que regula los servicios de tercerización,» *Normas Legales Actualizadas,* 24 junio 2008.

[7] C. E. p. A. L. y. e. C. -. CEPAL, «Sectores y empresas frente al covid-19,» 2 julio 2020. [En línea]. Available: https://www.cepal.org/es/publicaciones/45734-sectores-empresas-frente-al-covid-19-emergencia-reactivacion.

[8] L. E. Díaz Vargas, «Cambio de plataforma corporativa en una entidad financiera,» 2006. [En línea]. Available: http://cybertesis.uni.edu.pe/handle/uni/7202.

[9] Ministerio de Energía y Minas, «MINEM,» 2020. [En línea]. Available: http://minem.gob.pe/minem/archivos/file/OGP/PMI/Diagnostico%20de%20Brechas%20del%20Sector%20EM2.pdf.

[10] ElectroSurEste, «SIELSE,» [En línea]. Available: http://www.else.com.pe/SIELSEAyuda/AspectosGenerales/index.html.

[11] Perú Licitaciones, «Moitoreo y Seguimiento de Contrataciones Públicas de Perú,» [En línea]. Available: https://www.perulicitaciones.com/servicio-georeferenciado-y-de-empadronamiento-de-conexiones-el%EF%BF%BDctricas-para-el-suministro-de-electricidad-lct125334.html.

[12] OSCE, «Organismo Supervisor de las Contrataciones del Estado,» Ministerio de Economía y Finanzas, [En línea]. Available: https://www.gob.pe/osce.

[13] International Business Machines, «Business impact of outsourcing: a fact-based analysis,» *IBM*, january 2010.

[14] Y. Ospitia Medina y O. D. Molina Ospina, «Tercerización Estrategica de Procesos de TI,» Universidad ICESI, 2011. [En línea]. Available: https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/67976/1/tercerizacion_estrategica_procesos.pdf.

[15] K. Romero, «La gestión de la seguridad y el riesgo en TI,» *Universidad Piloto de Colombia*, pp. 1-8, 2015.

[16] D. Díaz Gomez, «Gestión de Riesgos en entornos Empresariales Alineados a la Norma ISO 31000,» *Universidad Piloto de Colombia*, pp. 1-13, 2017.

[17] J. Martín, A. Mateos y E. Vicente, «Risk analysis in information systems: A fuzzification of the MAGERIT methodology,» *Elsevier*, vol. 66, pp. 1-12, August 2014.

[18] J. Alvarado Zabala, J. Pacheco Guzmán y I. Martillo Alchundia, «El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT,» *Contribuciones a las Ciencias Sociales*, noviembre 2018.

[19] F. Y. Holguín García y L. M. Lema Moreta, «Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras,» *Risti*, pp. 1-17, 2019.

[20] C. D. Ocampo, J. Tamayo y H. M. Castaño, «Gestión del Riesgo en la Implementación de Sistemas Fotovoltaicos en Proyectos de Extracción de Oro en Colombia a partir del Proceso de Análisis Jerárquico(AHP),» *Scielo*, pp. 1-10, 2019.

[21] A. Dippenaar y S. Bezuidenhout, «The development of a robust risk management plan for the continuous supply of water to hospitals in the western cape province,» *Scielo*, vol. 30, nº 2, pp. 1-15, August 2019.

[22] D. F. Carnero Garay, M. A. Carbajal Ramos , J. Armas Aguirre y J. M. Madrid Molina, «Modelo de gestión de riesgos de seguridad de información para mitigar el impacto en las PYMEs en Perú,» *CISTI (Iberian Conference on Information Systems & Technologies)*, pp. 1-7, 2020.

[23] Instituto Colombiano de Normas Técnicas y Certificación, «Norma Técnica Colombiana NTC 5254: Gestión de riesgo,» *ICONTEC*, pp. 4-8, 2006.

[24] P. Sikdar, «Alternate approaches to business impact,» *Information Security Journal: Global Perspective*, vol. 20, pp. 128-134, 2011.

[25] P. A. López, Seguridad Informática, Madrid, España: Editex, 2010.

[26] Instituto Colombiano de Normas Técnicas y Certificación (Icontec), «Norma Técnica Colombiana NTC 5254: Gestión del riesgo,» *ICONTEC,* pp. 6-44, 2004.

[27] A. Ramírez Castro y Z. Ortiz Bayona, «Gestión de Riesgos tecnológicos basada,» *INGENIERÍA,* vol. 16, nº 2, pp. 56-66, 2011.

[28] Ministerio de Hacienda y Administraciones Públicas, «Magerit v.3 : Metodología de análisis y gestión de riesgos de los sistemas de información.,» octubre 2012. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WaeCb7LyjIU.

[29] E. Ferruzola Gómez, J. Duchimaza S, J. Ramos Holguín y M. Alejandro Lindao, «Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit,» *Revista Científica y Tecnológica UPSE,* vol. 6, nº 1, pp. 34-41, 2019.

[30] E. Crespo Martínez y G. Cordero-Torres, «Estudio comparativo entre las metodologias CRAMM Y MAGERIT para la gestión de riesgo de TI en las MPYMES,» *UDA AKADEM,* nº 1, pp. 38-47, 2018.

[31] Magerit, «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información versión 3.0,» 2021. [En línea]. Available: https://administracionelectronica.gob.es/ctt/magerit#.YjE8vHpBzIU.

ANEXOS

Anexo A. Formato de entrega de fichas de planos por SET Y SED

Anexo B. Territorio del proyecto