

UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
ESCUELA DE POSGRADO



Modelo de gestión de riesgos de TI que contribuye a la operación de procesos core en empresas de telecomunicaciones

**TESIS PARA OPTAR EL GRADO ACADÉMICO DE
MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN
EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN**

AUTOR

Daniel Alonso Romero Garcia

ASESOR

Gregorio Manuel Leon Tenorio

<https://orcid.org/0000-0002-9650-4427>

Chiclayo, 2023

**Modelo de Gestión de riesgos de TI que contribuye a la operación de
procesos core en empresas de telecomunicaciones**

PRESENTADA POR

Daniel Alonso Romero Garcia

A la Escuela de Posgrado de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el grado académico de

**MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN
EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN**

APROBADA POR

Maria Ysabel Aranguri Garcia

PRESIDENTE

Ricardo David Iman Espinoza

SECRETARIO

Gregorio Manuel Leon Tenorio

VOCAL

Dedicatoria

Dedico el siguiente trabajo de investigación a la memoria de mi madre, que desde el cielo me guía e ilumina, de la misma forma agradezco a mi padre y hermano que siempre me brindan una palabra de apoyo y aliento para seguir cumpliendo mis metas y colaboran con mi desarrollo, tanto personal como profesional.

Agradecimientos

Agradezco a mis compañeros y colegas que tuvieron participación en el siguiente trabajo de investigación, en primer lugar, a mi asesor que en todo momento brindo apoyo y sirvió como guía, a mi jefe inmediato y compañeros de labores que colaboraron en el desarrollo inicial del trabajo de investigación y modelo, a los expertos que brindaron su tiempo y disposición para revisión y evaluación del modelo propuesto.

InformeTesis artículo Final - Posgrado - DromeroG v5

INFORME DE ORIGINALIDAD

20%	20%	5%	%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	tesis.usat.edu.pe Fuente de Internet	6%
2	hdl.handle.net Fuente de Internet	5%
3	repositorio.ucv.edu.pe Fuente de Internet	1%
4	1library.co Fuente de Internet	1%
5	www.gob.pe Fuente de Internet	1%
6	mundoplanilla.com Fuente de Internet	<1%
7	repositorio.unal.edu.co Fuente de Internet	<1%
8	www.coursehero.com Fuente de Internet	<1%
9	www.slideshare.net Fuente de Internet	<1%

10	ddigital.umss.edu.bo:8080 Fuente de Internet	<1 %
11	es.scribd.com Fuente de Internet	<1 %
12	www.revistaespacios.com Fuente de Internet	<1 %
13	mail.ues.edu.sv Fuente de Internet	<1 %
14	www.scribd.com Fuente de Internet	<1 %
15	informatica.upla.edu.pe Fuente de Internet	<1 %
16	repositorio.uladech.edu.pe Fuente de Internet	<1 %
17	repositorio.unach.edu.pe Fuente de Internet	<1 %
18	repository.usta.edu.co Fuente de Internet	<1 %
19	core.ac.uk Fuente de Internet	<1 %
20	repository.unipiloto.edu.co Fuente de Internet	<1 %
21	www.ecci.edu.co Fuente de Internet	<1 %

22	dspace.ucuenca.edu.ec Fuente de Internet	<1 %
23	kupdf.net Fuente de Internet	<1 %
24	repositorio.utc.edu.ec Fuente de Internet	<1 %
25	www.elhuerequeque.com Fuente de Internet	<1 %
26	dspace.udla.edu.ec Fuente de Internet	<1 %
27	repositorio.uts.edu.co:8080 Fuente de Internet	<1 %
28	xdoc.mx Fuente de Internet	<1 %
29	Daiane Chioli, Luana Luiz, Marcelo Donin, Jean Tybuszeusky. "PROPOSTA DE MELHORIA BASEADA NA METODOLOGIA DMAIC EM UMA UNIDADE DE PRONTO ATENDIMENTO DE SAÚDE", The Journal of Engineering and Exact Sciences, 2020 Publicación	<1 %
30	administracion.uexternado.edu.co Fuente de Internet	<1 %
31	moam.info Fuente de Internet	<1 %

32 repositorio.osiptel.gob.pe <1 %
Fuente de Internet

33 José Joaquín Pinto Bernal. "Trasformaciones en el cargo de la caja real de Santafé, 1739-1808. Un análisis cualitativo de su impacto administrativo", Anuario del Instituto de Historia Argentina, 2018 <1 %
Publicación

34 María Palacios Guillem. "Propuesta de un nuevo procedimiento basado en la norma ISO 9001 para la gestión conjunta de la norma ISO 31000, la filosofía Kaizen y la herramienta Lean Manufacturing en pymes industriales de la Comunidad Valenciana.", Universitat Politecnica de Valencia, 2021 <1 %
Publicación

35 calidadgestion.wordpress.com <1 %
Fuente de Internet

Excluir citas Activo Excluir coincidencias < 4 words
Excluir bibliografía Activo

Índice

Resumen	10
Abstract	11
1.- Introducción	12
1.1. Justificación	13
1.2. Objetivos	14
2.- Revisión de literatura	14
2.1. Antecedentes	14
2.2. Bases teóricas	16
2.2.1. Gestión de riesgos	16
2.2.2. Armonización.....	16
2.2.3. Estándares internacionales de gestión de riesgos.....	18
2.2.4. Marcos de referencia.....	20
3.- Materiales y métodos	21
3.1. Tipo de estudio.....	21
3.2. Población.....	21
3.3. Métodos, Técnicas e Instrumentos.....	21
4.- Resultados y discusión	22
4.1 Diagnóstico del sector	22
4.2 Análisis de estándares	22
4.3 Propuesta de solución	24
ETAPA 1 : ANALISIS DEL CONTEXTO	25
ETAPA 2: EVALUACION DEL RIESGO	27
ETAPA 3: TRATAMIENTO DEL RIESGO.....	35
ETAPA 4: MONITOREO.....	36

4.4 Discusion	37
5.- Conclusiones	38
6.- Recomendaciones	38
7.- Referencias.....	40
8.- Anexos	43
Anexo 01 Encuesta de Gestión de Riesgos de tecnologías de información.....	43
Anexo 02 : Matriz de consistencia	54
Anexo 03: Plantilla de juicio de expertos.	55
Anexo 04: Respuesta de juicio de expertos.	59
Anexo 05: Implementación parcial del modelo.	62
Anexo 06: Autorización de la empresa.....	81
Anexo 07: Armonización de estándares y modelos.	83
Anexo 08: Alfa de Cronbach y concordancia de Kendall.....	92

Resumen

La investigación objeto del siguiente documento propone un modelo de gestión de riesgos de TI que contribuye a la operación de los procesos core en las empresas de telecomunicaciones, el sector de telecomunicaciones es un sector que constantemente enfrenta desafíos y los últimos años no fue la excepción, tanto ante nuevas ofertas del mercado y cambios en los hábitos de consumo como amenazas de seguridad, protección de usuarios al acceso a internet y aceleración para una correcta transformación digital.

Para el desarrollo del modelo, se ejecutó el proceso de armonización, bajo la metodología de Pardo[1], el proceso tiene como finalidad establecer algunos elementos comunes respecto a diversos modelos propuestos se cumplió con el desarrollo de las fases de la metodología y, finalmente el modelo fue validado mediante juicio de expertos y para medir la confiabilidad de este se empleó Alfa de Cronbach.

El objetivo general de la presente investigación fue determinar el impacto de un modelo de gestión de riesgos de TI en la operación de los procesos core en empresas de telecomunicaciones, que luego se reflejaría mediante la implementación parcial del modelo en una empresa del sector.

Finalmente se realizó la implementación parcial de nuestro modelo en el servicio de Telefonía Fija de una empresa, donde se identificaron 13 activos críticos que soportan la operación, donde se logró identificar 40 escenarios de riesgos, siendo 09 con criticidad alta; con lo cual se pudo proponer proyectos que ayuden a mitigar los riesgos detectados.

Palabras clave: Gestión de riesgos de TI, armonización, empresas de Telecomunicaciones.

Abstract

The research object of the following document proposes an IT risk management model that contributes to the operation of core processes in telecommunications companies, the telecommunications sector is a sector that constantly faces challenges and recent years was no exception. both in the face of new market offers and changes in consumer habits as well as security threats, protection of users to access the Internet and acceleration for a correct digital transformation.

For the development of the model, the harmonization process was carried out, under the Pardo methodology [1], the purpose of the process is to establish some common elements with respect to various proposed models, the development of the methodology phases was fulfilled and, finally, The model was validated through expert judgment and Cronbach's Alpha was used to measure its reliability.

The general objective of this research was to determine the impact of an IT risk management model on the operation of core processes in telecommunications companies, which would later be reflected through the partial implementation of the model in a company in the sector.

Finally, the partial implementation of our model was carried out in the Fixed Telephony service of a company, where 13 critical assets that support the operation were identified, where 40 risk scenarios were identified, 09 being highly critical; with which it was possible to propose projects that help mitigate the risks detected.

Keywords: IT risk management, harmonization, Telecommunications Companies.

1.- Introducción

Las empresas y los sistemas de información se enfrentan, frecuentemente, a ciertos riesgos e inseguridades ocasionados por diversas causas, entre las que podemos encontrar al espionaje, sabotaje, a fraudes basados en informática, entre otros. Es preciso señalar que estas fuentes, en la actualidad se tornan cada vez más comunes y sofisticados, como lo son los ataques de intrusión o los virus informáticos.[2]. Es, a partir de esta situación, que la gestión de riesgos de una empresa, así como sus controles en los sistemas de información cobran especial relevancia, por cuanto el objetivo principal trazado por estas organizaciones resulta ser salvaguardar sus procesos comerciales, como también la capacidad para poder cumplir con sus objetivos trazados.[3]

Ahora bien, si nos remitimos al campo organizacional, para cualquier compañía, la gestión de riesgos es calificada como un aspecto sensible y crítico para el cumplimiento de las metas o expectativas establecidas. Concretamente, si nos remitimos a las empresas de telecomunicaciones, este tipo de procesos no les resulta ajeno, por el contrario, el papel que cumplen en conjunto, hoy por hoy, determina la competitividad para cualquier país.[4, p. 1]. Sumado a lo antes señalado de conformidad con el marco de referencia ETOM (Enhanced Telecommunications Operations Map) el cual es constituye una guía para actividades de redes y servicios dentro de una empresa de telecomunicaciones nos indica como nivel 0 o procesos core a los procesos de operaciones y gestión de la empresa.[4]

A continuación, se presentarán algunos de los casos más sonados relacionados a fallos de seguridad, interrupción de servicios de los últimos años, empezaremos por el año 2011, donde la compañía canadiense Research In Motion (RIM), dedicada a la fabricación de teléfonos móviles BlackBerry, sufrió una contingencia mundial producto de la caída de sus servicios debido al "fallo de un interruptor central", siendo que los servicios afectados fueron el de correo electrónico y mensajería. [5]. En el plano local, en junio del año 2020, se produjo un incendio en un tablero de telefonía de una conocida empresa de telecomunicaciones, lo cual provocó que en varios sectores de la región Lambayeque se quedaran sin servicio de internet[6]. El año 2021 no fue la excepción para el fallo en los servicios de telecomunicaciones, y es que en el mes de junio se suscitó un nuevo incidente global que afectó el servicio de internet de diversas plataformas del rubro bursátil, bancario,

así como de diversas aerolíneas. Entre las empresas afectadas se tienen a la bolsa de valores de la ciudad de Hong Kong, el banco australiano Commonwealth Bank of Australia, así como de las aerolíneas United Airlines y Southwest Airlines, también la aerolínea Virgin Australia. En todos estos casos, la hipótesis que se manejó como la causa de este problema, se originó en la empresa Akamai, con sede en Massachusetts (EE. UU.), que resulta ser una compañía proveedora del servicio de internet.[7]

Aunado a lo antes señalado, el organismo estatal regulador de las telecomunicaciones en el país (Osiptel), dentro de sus informes publicados precisó que, en el año 2018, en el país se registraron un total de 13.419 interrupciones o caídas en el servicio de telecomunicaciones, suponiendo esta cifra un porcentaje del 96 % más en comparación al año 2017, en el que se registraron 6.853 interrupciones.[5].

1.1.Justificación

En el mundo empresarial, y, en general para toda entidad público o privada, la gestión de riesgos, así como los controles en los sistemas de información resulta ser un aspecto muy sensible, pero, a la vez, relevante, por cuanto su finalidad está enmarcada en proteger los procedimientos internos del negocio o giro empresarial, y así, tenga la capacidad de cumplir con los objetivos, y, por qué no ser una Compañía o Institución competitiva en el mercado.

La justificación de la presente investigación en el ámbito social será porque permitirá a los miembros de la organización desarrollar una efectiva gestión de riesgos de TI, impactando de forma positiva en la continuidad de los procesos de la empresa, generando nuevos retos propios del negocio y del sector como es el de telecomunicaciones, a su vez ayudara a la imagen y satisfacción de sus clientes.

Desde el punto de vista económico se justifica en que una correcta gestión de riesgos de TI tiene como consecuencia continuidad de servicios a empresas, y procesos de negocio que a su vez ayudaran al cumplimiento de sus objetivos estratégicos, logrando evitar las pérdidas económicas en caso de que llegue a materializarse un riesgo o amenaza.

En este sentido, resulta relevante y de gran apoyo para las empresas de este sector conocer el producto final de esta investigación, porque la misma, les permitirá mejorar sus procedimientos, minimizar o mitigar las fallas o errores y, de esta forma, ser competitivos en el mercado.

1.2.Objetivos

El objetivo general del proyecto determinar el impacto de un modelo de gestión de riesgos de TI en la operación de los procesos core en empresas de telecomunicaciones.

Adicionalmente, los objetivos específicos son: i) armonizar los estándares y metodologías de la Gestión de Riesgos de TI; ii) Incrementar la capacidad para la detección y tratamiento de los riesgos.; iii) Validar el modelo de Gestión de Riesgos de TI propuesto para mejorar los procesos core en empresas de servicio de telecomunicaciones.; y iv) Realizar la implementación de un piloto en una empresa del sector.

Para el presente proyecto se propone la Hipótesis: Elaboración de un modelo de gestión de riesgos de TI que contribuye de forma positiva con la operación de los procesos core para las empresas de telecomunicaciones.

Por ello, el problema planteado resulta ser el siguiente: ¿De qué manera un modelo de gestión de riesgos de TI impactará en la operación de los procesos core en empresas de telecomunicaciones?

2.- Revisión de literatura

2.1. Antecedentes

Se describirán en adelante antecedentes que guardan estrecha relación con el tema de investigación que ayudarán a fundamentar el tema:

En el año 2018 Santa Cruz, Roberto[9] describe las características de un modelo de gestión de riesgos de tecnologías de información para así asegurar la eficiencia y continuidad del negocio en el sector micro financiero de la ciudad de Chiclayo. La investigación tuvo como

finalidad mejorar la gestión de riesgos de TI en empresas microfinancieras de la región, a través de la propuesta de un modelo de Gestión de Riesgos de TI. Esta investigación también demostró que dicho modelo propuesto cumple con las normas de la Superintendencia de Banca y Seguro.

También en el año 2018, Peña, Moscoso y Soto [10] proponen un modelo de gestión de riesgos de TI para empresas del sector de saneamiento del Perú, se plantearon como objetivo general contribuir a la operación de los procesos de la gestión comercial por medio del desarrollo de un modelo, el tipo de estudio fue observacional, transversal y se realizó un pre test y post test, en dicho estudio se logró identificar que dicha entidad objeto del estudio no implementa o si lo hacen no de forma correcta, la gestión de riesgos de tecnologías de información, mediante el hallazgo de 165 riesgos que podrían afectar la operación del proceso comercial de la compañía, 52 de los riesgos encontrados fueron categorizados como de alta prioridad, este trabajo aporta a la investigación en la propuesta de un modelo de gestión de riesgos de TI.

En el 2019, la tesis de Huaura, Miguel[11] nos brinda la información referida a la manera en cómo la gestión de riesgos de seguridad de la información, amparada en la NTP ISO/IEC 31000 interviene directamente en el control de riesgos en las empresas dedicadas al rubro de las Telecomunicaciones. Adicionalmente, se logra establecer ciertas normas que permiten facilitar indicadores, analizar coherentemente los riesgos, y, establecer métricas de gestión que determinen un diagnóstico de la empresa, la cual deberá ser apoyada por la Alta Dirección. Es por lo que, para lograr este objetivo el autor involucra a las áreas de Alta dirección respecto a la toma de decisiones y el valor que ofrece la Gestión de Riesgos de TI.

En el año 2022, la tesis de Villegas, Cesar [12] nos propone un modelo de gestión de riesgos de TI para la protección de activos en organizaciones del sector salud, para la obtención de dicho modelo el autor se propuso realizar un análisis comparativo de estándares y metodologías relacionadas a la gestión de riesgos. El diseño de la investigación fue de tipo preexperimental, contando con una población de 07 hospitales de la región Amazonas, para

la validación el modelo el autor realiza juicio de expertos y propone fichas y formatos adecuados para empresas del sector y protección de los activos de información.

2.2. Bases teóricas

2.2.1. Gestión de riesgos

En la norma de calidad ISO 31000 [13] se conceptualiza este tema como todas aquellas actividades que se encuentran coordinadas controlar y dirigir la organización de una empresa en concordancia al riesgo, siendo esta situación un efecto derivado de la incertidumbre sobre los objetivos.

Adicionalmente, de acuerdo con lo señalado por Ortiz [4] , señala que resulta ser un proceso elemental para cualquier modelo de gestión empresarial, siendo considerado también como aquel proceso crítico, el cual tiene por finalidad lograr los objetivos de cualquier entidad.

Para Casares y Lizarzaburu [14] se considera que resulta ser una etapa fundamental en relación con la evaluación que se realiza a los aspectos económico y financiero. Sumado a ello, se trata de un enfoque documentado y riguroso en aquellos niveles de desarrollo de las situaciones evaluadas, requiriéndose así de información de las áreas involucradas, como aquellas internas y externas.

2.2.2. Armonización

Para el autor Valencia Duque[15] la figura de la armonización de modelos tiene como finalidad el establecer algunos elementos comunes respecto a diversos modelos propuestos, ello en aras de efectuar una aproximación a un modelo que contenga aquellos elementos generalmente implementados de cada uno de los otros modelos.

Este término cobra principal relevancia en el presente trabajo de investigación debido a uno de los objetivos está orientado a buscar, comparar y analizar las concordancias y similitudes de las metodologías y estándares revisados en el proyecto.

Para la elaboración del modelo de comparación y posterior armonización de los modelos el autor utilizó una metodología que consta de 04 etapas; las cuales se muestran a continuación:

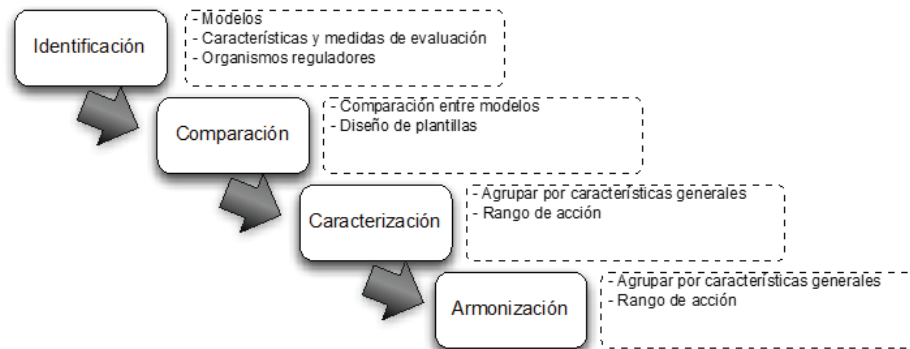


Figura 1 Etapas de la metodología propuesta - armonización de modelos [16]

Posterior a la evaluación y armonización de modelos se logró identificar relación entre los mismos, así como porcentaje de cubrimiento, los autores nos presentan su propuesta metodológica que está basada en la organización de actividades y se muestra a continuación:

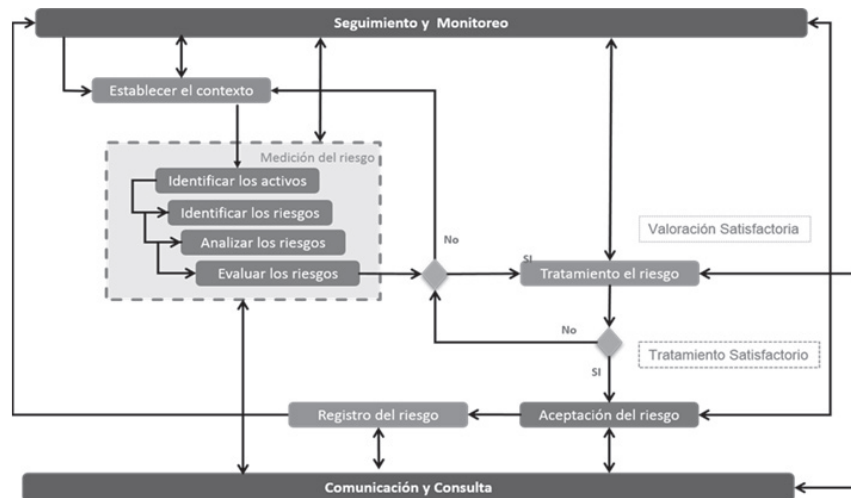


Figura 2 Propuesta Metodológica en la gestión de riesgos en TI [16]

Vanegas, G. & Pardo, C. [16] concluyen en que la metodología se encuentra soportada por aquellas actividades que se encuentran descritas en los procesos de gestión de riesgos, los cuales están determinados en las normas, así como en los estándares certificados, siendo que la aplicación de esta permitirá de alguna manera cumplir con atributos de calidad. La importancia de esta investigación como antecedente radica en que se pone de manifiesto una manera de cómo se tendría

que abordar la armonización de estándares como las metodologías relacionadas con la gestión de riesgos que se viene desarrollando.

2.2.3. Estándares internacionales de gestión de riesgos

2.2.3.1 Norma Internacional ISO 31000:2018-02

La Organización Internacional de Normalización, en su última actualización de la norma ISO 31000:2018:02 denominada “Gestión del riesgo - Directrices”

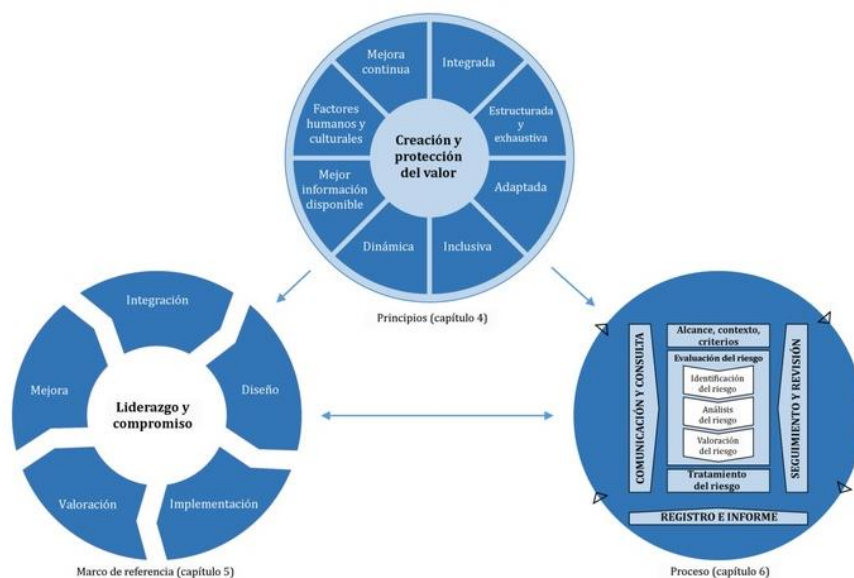


Figura 3 ISO 31000 Principios, marco de referencia y proceso

Esta norma, de acuerdo con Casares y Lizarzaburu [14] resultaría ser una guía de implementación que coadyuva a las Empresas en el desarrollo de su modelo de gestión del riesgo. Adicionalmente, se establece que, de implementarse esta norma, las compañías podrán comparar y evaluar las prácticas de esta gestión desde un parámetro internacional, consiguiendo de esta forma un buen gobierno corporativo, así como una eficaz gestión de los riesgos.



Figura 4 Principios Norma ISO 31000 [13]

La norma, adicionalmente, cuenta con un marco de referencia de la gestión en cuestión cuya finalidad es asistir en la integración de este proceso a todas las actividades de la organización. Este desarrollo implica diseñar, implementar, integrar, mejorar y valorar esta gestión a lo largo de toda la compañía.



Figura 5 Marco de referencia[13]

Finalmente, cuenta con un proceso que implica una aplicación sistemática de prácticas, procedimientos, así como políticas referidas a las actividades de

consulta y comunicación. Sumado a ello, las referidas a la evaluación y establecimiento del contexto, al seguimiento, tratamiento, registro, revisión e informe del riesgo.

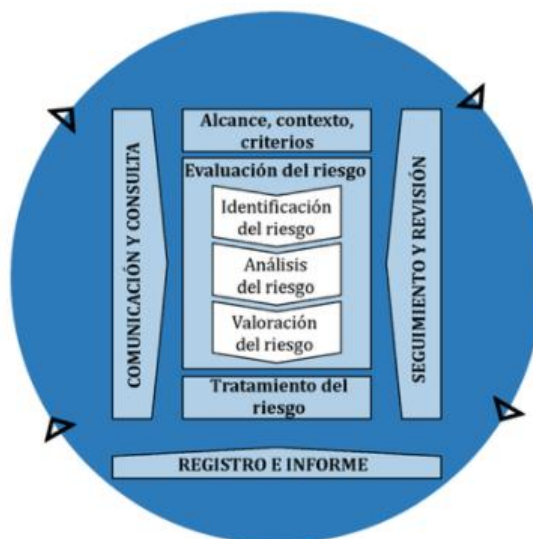


Figura 6 ISO 31000 Proceso[13]

2.2.4. Marcos de referencia

2.2.4.1 COBIT

Desarrollado por ISACA[17] quien señala que COBIT es aquel “*marco para el gobierno y la gestión de las tecnologías de la información de la empresa, dirigido a toda la empresa.*”

Su marco de referencia diferencia de manera objetiva al gobierno y su gestión. Adicionalmente, es necesario precisar que ambas disciplinas abarcan distintos tipos de actividades, las cuales necesitan de diversas estructuras organizativas que permitirán diferentes propósitos.

2.2.4.2. MAGERIT V 3.0

Esta metodología fue elaborada por el gobierno español, específicamente por el Ministerio de Hacienda y Administraciones Públicas [18] quien ha establecido que el MAGERIT efectúa el proceso de gestión de riesgos

basado en situaciones reales de trabajo, ello con la finalidad que sus órganos de gobierno adopten decisiones basadas en aquellos riesgos derivados del uso de las TI.

3.- Materiales y métodos

3.1. Tipo de estudio

La metodología del presente trabajo de investigación será Investigación Aplicada bajo el diseño preexperimental.

Se busca evaluar el efecto de elaborar un modelo de gestión de riesgos de TI que impacta de forma positiva en la operación de procesos core en empresas de telecomunicaciones, empleando un modelo pretest/posttest con un solo grupo:

G A1 X A2

Dónde:

G = Grupo de estudio seleccionado.

A1 = Encuesta Pre-Test a personal de TI, para identificar el estado actual de la gestión de riesgos de TI.

X = modelo de gestión de riesgos de Tecnologías de la Información (TI)

A2 = Encuesta Post Test al mismo personal para conocer la contribución del modelo a los procesos core seleccionados (ventas y operaciones).

3.2. Población

Formaron como población el jefe de operaciones y jefe de TI responsables de las áreas que brindan soporte a los procesos de negocio de ventas y operaciones en la empresa.

3.3. Métodos, Técnicas e Instrumentos

Para este punto, forma parte del presente proyecto la matriz de consistencia que podrá ser visualizado como [anexo 02](#).

4.- Resultados y discusión

4.1 Diagnóstico del sector

Motivo del presente trabajo fue el análisis de resultados a encuestas (ver [anexo 01](#)) aplicadas a empresas del sector de telecomunicaciones que tuvo como finalidad en identificar el nivel de gestión de riesgos de tecnologías de información aplicado en la organización.

Antes debemos recalcar que las encuestas fueron resueltas por personal de las empresas con cocimiento y se encuentran laborando activamente en el área de sistemas.

La conclusión del análisis de las encuestas fueron las siguientes:

- Un 75% de las empresas encuestadas no cuenta con un historial de eventos y su impacto en el negocio, así como una clasificación de los factores causantes de riesgos.
- El 50% de las empresas encuestadas no cuenta con un análisis del impacto de los riesgos de TI asociados a la tolerancia y planes que excedan a la misma.
- El 50% de las empresas no cuentan con una evaluación del impacto a pérdidas de TI.
- El 50% de las empresas encuestadas no cuentan con auditorías y/o consultorías de empresas especializadas para evaluación de gestión de riesgos de Tecnologías de información.
- El 75 % de las empresas encuestadas realizan análisis de riesgos y cuentan con una clasificación y métodos de riesgos de TI.
- El 75% de las empresas encuestadas no cuenta con evaluación y/o auditorías de empresas especializadas gestión de riesgos de TI.

4.2 Análisis de estándares

Para realizar la propuesta de un modelo de gestión de riesgos para empresas de telecomunicaciones, se han considerado los siguientes estándares internacionales y

marcos de referencia asociados a la gestión de riesgos de tecnologías de información.

Para mayor detalle, presentamos la siguiente tabla resumen:

Tabla I: Resumen normas y estándares.

Norma / Estándar	Organización	País
ISO 31000:2018[13]	Organización de estándares internacionales – ISO.	Suiza
COBIT 2019[17]	ISACA	Estados Unidos
ETOM	TM FORUM	Estados Unidos

Fuente: Elaboración Propia

Para la elaboración de nuestra propuesta de modelo de gestión de riesgos de tecnologías de información, hemos contemplado como etapa inicial el proceso de armonización, para el autor Valencia Duque[15] la figura de la armonización de modelos tiene como finalidad el establecer algunos elementos comunes respecto a diversos modelos propuestos, ello en aras de efectuar una aproximación a un modelo que contenga aquellos elementos generalmente implementados de cada uno de los otros modelos.

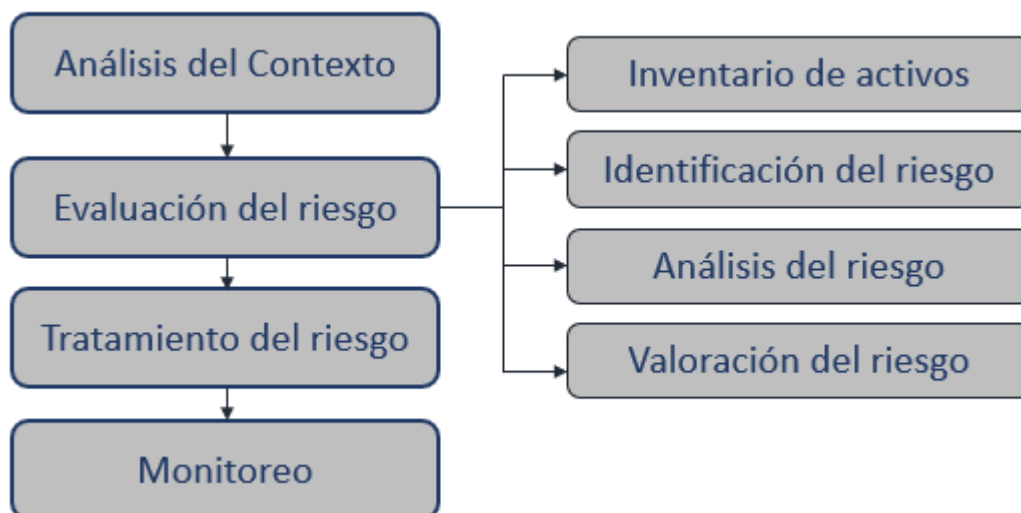
Para la propuesta del nuestro modelo hemos considerado el modelo de Pardo [1], proceso de armonización que consta de 04 etapas, las cuáles son, homogenización, comparación, análisis porcentual y análisis de resultados.

Más información se podrá visualizar en el Anexo 05.

4.3 Propuesta de solución

El siguiente modelo, responde al proceso de armonización de diferentes estándares y metodologías como COBIT 2019, ISO 31000:2018 y el framework ETOM, este último corresponde a una guía para el sector de telecomunicaciones. Adicionalmente se consideró información de la metodología MAGERIT para algunas etapas del modelo propuesto.

Ilustración 1 : Modelo de Gestión de riesgos de TI propuesto



Fuente: Elaboración Propia

ETAPA 1 : ANALISIS DEL CONTEXTO

En la etapa inicial del modelo propuesto, la definición del alcance permitirá conocer a la organización y su entorno con relación al riesgo de TI, así también los principales procedimientos legales y regulatorios asociados a las empresas de telecomunicaciones.

A.1. Revisión Sid Sunarp: La constitución de empresa es un procedimiento a través del cual una persona registra su empresa ante el Estado para que obtengan los beneficios de ser formal. En el siguiente acceso (Sistema de intermediación digital) se podrá registrar, completar los datos necesario para inscripción de la empresa:

Toda la información se podrá validar en el siguiente enlace :

<https://www.sunarp.gob.pe/w-sid/index.html>

A.2. Mantenimiento PDT Plame: (Programa de Declaración Telemática, PDT).

La planilla electrónica es un documento que las empresas con más de tres trabajadores deben presentar todos los meses a la Superintendencia Nacional de Aduanas y de Administración Tributaria SUNAT y el Min. del Trabajo (MTPE).

Esta cuenta permite a toda empresa realizar diversas operaciones con la finalidad de mantener formalizada su empresa, cumpliendo la normativa legal vigente.

Entre las principales funcionalidades se tiene:

- Dar de Alta a todo trabajador.
- Dar de Baja al trabajador que culmina su vínculo laboral.
- Declarar en la Planilla de la Empresa a los trabajadores, así como sus remuneraciones y todo ingreso percibido.

Es deber de la empresa registrar a sus colaboradores en la planilla electrónica antes del cumplimiento de las 72 horas de iniciar el vínculo laboral caso contrario quedaran expuestos a una multa por la entidad del estado.

Mayor detalle se podría visualizar en el siguiente enlace:

<https://www.youtube.com/watch?v=DPMdNurElw4>

Esta actividad corresponde al registro con los datos de todos los colaboradores de la empresa, como se visualiza a continuación:

Plantilla 1: Mantenimiento cuadro planilla – PDT Plame

FECHA DE INGRESO	CÓDIGO	TIPO DE DOC DE IDENT	NÚMERO DEL DOC DE IDENT	APELLIDO PATERNO	APELLIDO MATERNO	PRIMER NOMBRE	SEGUNDO NOMBRE	NACIONALIDAD	FEC NACIMIENTO	SEXO ("M" o "F")	ESTADO CIVIL
		(TABLA: T1)						(TABLA: T2)			(TABLA: T3)
19/04/2021	44249924	01-DNI	44249924	ROMERO	GARCIA	DANIEL	ALONSO	PERU	12/10/1986	M	SOLTERO

A.3. Validación de concesión y permisos MTC (Min. de Transportes y Comunicaciones)

Para una empresa del sector Telecomunicaciones es necesario revisar y tener actualizado los permisos y concesiones proporcionados por el estado, esta información es de acceso público y actualizada por el gobierno.

En el siguiente enlace web <https://www.gob.pe/institucion/mtc/informes-publicaciones/322450-directorio-de-concesionarios-publicos> podemos visualizar los contratos de asociación público privadas y otros de similar naturaleza suscritos por el Ministerio de Transportes y Comunicaciones.

Adicionalmente en caso se desea registrar como proveedor de servicio de telecomunicaciones, se podrá realizar el trámite desde el siguiente acceso <https://www.gob.pe/8063>

ETAPA 2: EVALUACION DEL RIESGO

La segunda etapa del modelo propuesto consta de la evaluación del riesgo como proceso integral de la gestión del riesgo, teniendo las tareas de enumerar, clasificar, analizar y valorar el riesgo.

En la siguiente etapa consideramos las siguientes actividades:

B.1. Inventario de Activos

En esta actividad debemos identificar los activos primordiales para la organización, su relación y su valor para conocer a que amenazas se encuentran expuestas y poder estimar el impacto y riesgo en caso de algún daño.

B.1.1. Identificación de activos

En esta etapa debemos conocer todos los activos con los que cuenta la empresa, con la finalidad de poder gestionarlos de la mejor manera:

Plantilla 2: Registro de identificación de Activos

CODIGO	NOMBRE	DESCRIPCION	PROPIETARIO	RESPONSABLE
COD001	SERVTFIJA	Servicio telefonía Fija	EMPRESA ABC	OPERACIONES
COD002	PROVENTAS	Proceso de ventas	EMPRESA ABC	VENTAS
COD003	PROOPERACIONES	Proceso de Operaciones	EMPRESA ABC	OPERACIONES
COD004	GSXLIMPE01 (GSX SONUS)	Media Gateway de Voz	OPERACIONES	OPERACIONES
COD005	LimCat01 (Catalyst 3750)	SW core voz Mpls	OPERACIONES	OPERACIONES
COD019	PC_SOPORTETECNICO	PC de Soportetecnico	SOPORTETECNICO	SOPORTETECNICO
COD020	PC_CONTABILIDAD	PC de Contabilidad	CONTABILIDAD	CONTABILIDAD
COD021	PC_RRHH	PC de Rrhh	RRHH	RRHH
COD022	IMP_OPERACIONES	Impresora del área de operaciones	OPERACIONES	OPERACIONES

B.1.2. Clasificación de activos

De acuerdo con la metodología MAGERIT[19]: La clasificación corresponde a la asignación de un código o epígrafe y este reflejara su posición jerárquica mediante una breve descripción.

Primero debemos completar la tabla de descripción de registros que se visualiza a continuación:

Plantilla 3: Formato registro de descripción de activos

ITEM	DESCRIPCION	ETIQUETA
1	[SW] Software	[SW]
2	[S] Servicios	[S]
3	[HW] Hardware - Equipamiento	[HW]
4	[COM] Redes de comunicaciones	[COM]
5	[P] Personal	[P]

Plantilla 4: Formato de Clasificación de activos

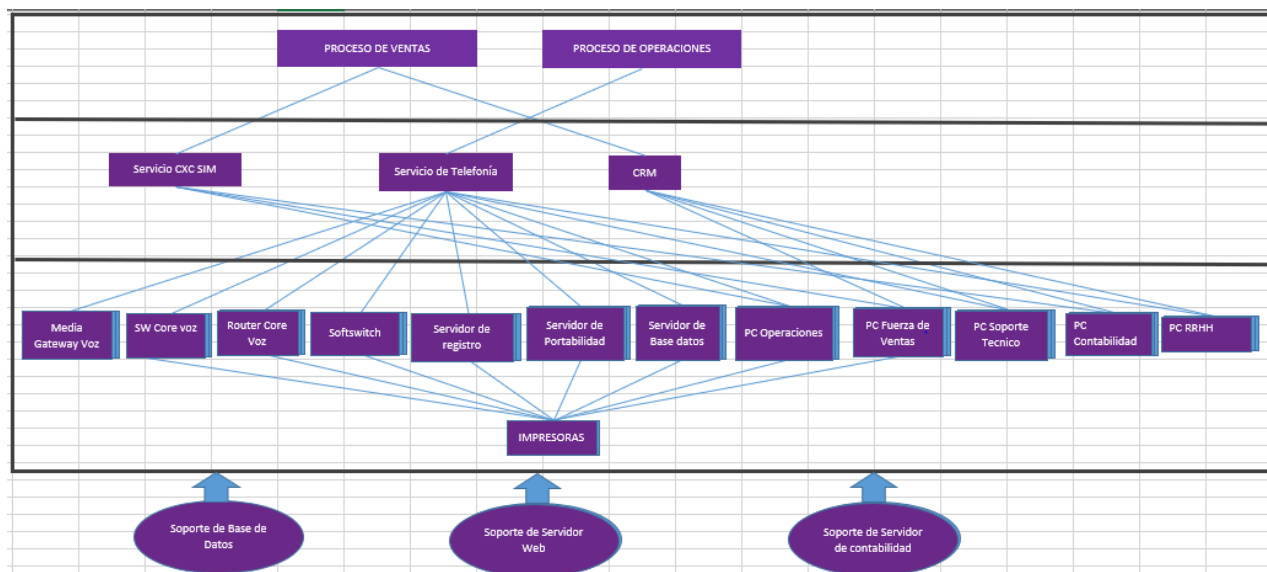
ITEM	NOMBRE DEL ACTIVO	DESCRIPCION	DESCRIPCION ACTIVO	ETIQUETA
1	GSXLIMPE01 (GSX SONUS)	Media Gateway de Voz	[SW]	[SW - GSXLIMPE01 (GSX SONUS)]
2	LimCat01	SW_core_voz_Mpls	[HW]	[HW - LimCat01]
3	LimCat02	SW_core_voz_Mpls	[HW]	[HW - LimCat02]
4	LimRtr01	Router_Core_Voz_Mpls	[HW]	[HW - LimRtr01]
5	PSXLIMPE01	Softswitch	[SW]	[SW - PSXLIMPE01]

B.1.3. Dependencia de activos

En esta sección debemos identificar los activos y su dependencia, esto con la finalidad de identificar correctamente el activo y su riesgo en la organización.

Paso inicial es el registro de la plantilla de dependencia de activos.

Ilustración 2: Registro de dependencia de activos



Fuente: MAGERIT 3.0 [18]

B.1.4. Valoración de activos

La valoración del activo en esta tarea corresponde al reconocimiento del activo en caso verse afectado o dañado y el reconocimiento del impacto real en la organización.

[D] Disponibilidad: Tener acceso al activo cuando se requiera o necesite.

[I] Integridad: El activo no haya sido alterado o modificado.

[C] Confidencialidad: No disponible a personas no autorizadas.

Ilustración 3: Criterios de valoración Confidencialidad - Disponibilidad e Integridad

Criterios de la Valoración	Valor	Clase	Descripción
Confidencialidad	3	Alta	Activo que solo puede ser de conocimiento estrictamente por algunas personas en particular.
	2	Media	Activo disponible dentro de la organización con restricciones variadas para ciertas áreas.
	1	Baja	Activo que puede ser publicado a cualquier persona de la compañía.
	0	No relevante	Activo que puede ser publicado al público en general
Disponibilidad	3	Alta	El activo debe estar disponible en todo momento.
	2	Media	El activo puede no estar disponible por menos de un día.
	1	Baja	El activo puede no estar disponible por más de un día.
	0	No relevante	El activo puede no estar disponible.
Integridad	3	Alta	El daño o alteración generará un fuerte impacto en la empresa y podría conllevar a consecuencias críticas.
	2	Media	El daño o alteración generará un impacto significativo en la empresa.
	1	Baja	El daño o alteración generará un impacto insignificante o menor en la empresa.
	0	No relevante	El daño o alteración no generará un impacto negativo en la empresa.

B.2. Identificación del Riesgo

El fin de esta tarea corresponde a describir, enumerar los riesgos que impiden el cumplimiento de los objetivos de la organización, para este es necesario tener información adecuada y actualizada.

Plantilla 5 : Registro de amenazas

Ítem	DESCRIPCION	ETIQUETA	CONCATENADO
1	Desastres Naturales	[DN]	[DN] Desastres Naturales
2	Desastres Naturales Fuego	[DNF]	[DNF] Desastres Naturales Fuego
3	Desastres Naturales Agua	[DNA]	[DNA] Desastres Naturales Agua
4	Desastres Naturales Terremoto	[DNT]	[DNT] Desastres Naturales Terremoto

B.3. Análisis del Riesgo

La siguiente tarea consta de entender las características y naturaleza del riesgo, debemos detallar fuentes de riesgo, consecuencias, escenarios y controles

- Debemos definir criterios de probabilidad en base a ocurrencia de incidencias en nuestra organización.

Tabla de niveles:

Criterios de probabilidad

Que tan probable es que ocurra un evento, para este paso debemos completar el registro de criterios de probabilidad:

Plantilla 6: Criterios de probabilidad

TIPOLOGIA	RARO	IMPROBABLE	POSIBLE	PROBABLE	CASI SEGURO
NIVEL	1	2	3	4	5
PROBABILIDAD	<2%	2%-15%	16%-50%	51%-80%	>80%

ESCENARIO DESCRIPTIVO	El evento es posible, y ha ocurrido criterios de probabilidad organización.	El evento ocurrió ciertas veces en la organización	Un evento así ha ocurrido en nuestra organización	Un evento así ha ocurrido en varias ocasiones en la organización.	El evento ocurre frecuentemente en la organización.
-----------------------	---	--	---	---	---

Criterios de impacto

Para lo cual debemos identificar 03 aspectos asociados a la empresa, **Apetito**, **tolerancia** y **capacidad**, esta con la finalidad de tener mayor detalle del impacto de la organización.

APETITO: El nivel de riesgo que una empresa está dispuesta a aceptar expresado en Soles.

TOLERANCIA: Variación aceptable relativa al apetito de riesgo expresado en Soles.

CAPACIDAD: Nivel máximo que una empresa puede soportar expresado en Soles.

Plantilla 7: Registro criterios de impacto

TIPOLOGIA	INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTROFICO
NIVEL	1	2	3	4	5
UMBRAL EMPRESA	<S/ 3 K	S/ 3 K- S/ 100 K	S/ 100 K - S/ 500 K	S/ 500 K - S/ 1 MM	> S/ 1 MM
ESCENARIO	El daño no es significativo para la empresa	El daño puede ser asumido por el área responsable	Se deben presentar acciones ante el daño presentado	El daño tiene efectos mayores en la empresa	Perdida catastrófica que pone en riesgo la rentabilidad de la empresa

Plantilla 8: Análisis del riesgo

ACTIVOS			CRITERIOS								RIESGO		
Nº	Código	Activo	C	I	D	TOTAL	AMENAZA	VULNERABILIDAD	IMPACTO	PROBAB	CÓDIGO	CÓDIGO	NIVEL
1	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	[ERU] Error de Usuario	Escaso conocimiento por parte de los usuarios	1	5	R1	5	BAJO
	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	[ER] Errores y Fallos	Falta de gestión de procesos	2	4	R2	8	BAJO
	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	[FSI] Falla servicio de Internet	No contar con un proveedor externo de internet	2	3	R3	6	BAJO
	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	Errores de Mantenimiento SW	Falta de Planificación	2	4	R6	8	BAJO

B.4. Valoración del Riesgo

Esta tarea comprende al proceso de comparar los resultados del análisis del riesgo agrupándolos en base a su magnitud y definiendo si son aceptables o tolerables.

Posterior a la agrupación tendremos un mapa de calor de riesgos que nos permitirá trabajar en proyectos que ayuden a priorizarlos.

Ilustración 4: Valoración del riesgo

PROBABILIDAD/ FRECUENCIA	5 Frecuente	R1				
	4 Probable		R2, R6	R5, R7, R10	R9, R13, R14, R15, R16, R17, R24, R27, R30	
	3 Ocasional		R3, R4, R8, R32, R34, R36, R38, R40	R11, R12, R31, R33, R35, R37, R39	R18, R19, R20, R21, R22, R23, R25, R26, R28, R29	
	2 Posible					
	1 Improbable					
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5

ETAPA 3: TRATAMIENTO DEL RIESGO

Es el resultado que define las acciones a tomar como empresa ante los riesgos encontrados, para ello debemos definir las estrategias que tomara la organización y establecer controles para el tratamiento de estos.

El resultado puede ser una plantilla o documento.

Ilustración 5: Descripción de criterios de Tratamiento del riesgo

Estrategia	Descripción Criterio
Reducir	Se deben evaluar y establecer controles que permitan mitigar el riesgo asociado.
Transferir	La responsabilidad es transferida a un área diferente o, en última instancia, a un tercero.
Aceptar	En este caso, el líder usuario o propietario de la información, acepta el riesgo de seguridad de la información.
Mitigar	En caso sea factible, se identifica la causa del riesgo para establecer medidas que lo eviten e impidan su materialización absoluta.

Plantilla 9: Tratamiento del riesgo

Nombre del Proyecto	Implementación de plan de Teletrabajo
Estrategia	Mitigar
Riesgo que trata	R7, R3, R14
Nivel de riesgo	Medio, Alto
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]
Objetivo	Mitigar riesgo de plan de teletrabajo, solicitado por el estado post pandemia COVID.

ETAPA 4: MONITOREO

Esta tarea consiste en la revisión constante de todas las fases anteriores, para esta etapa debemos definir responsables y asignar tareas, estas tareas deben ser de coordinadas y sinceras de acuerdo con la organización.

En esta etapa nos respondemos si lo que estamos cumpliendo con lo comprometido.

Nombre del Proyecto	Compra de equipo de respaldo eléctrico.
Estrategia	Mitigar
Riesgo que trata	R10, R16, R19
Nivel de riesgo	Medio, Alto
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]
Objetivo	Mitigar problema en los procesos ante Corte de suministro Eléctrico
Responsables	KP (Gerente de Operaciones)
Recursos requeridos	06 UPS
Presupuesto	1,500.00 X 6 = S/9,000.00 soles
Tiempo de ejecución	03 meses.

4.4 Discussion

En este ítem realizaremos el análisis de los resultados obtenidos de nuestro trabajo de investigación frente a los antecedentes presentados en la investigación:

- El modelo de gestión de riesgos de ti propuesto en el siguiente trabajo de investigación propone en una de sus etapas, para ser más específicos en la etapa de Análisis del contexto, verificación de permisos y concesiones del estado y documentación en regla en relación con el vínculo laboral con los trabajadores, esto con la finalidad de seguir las normas de entidades regulatorias del sector tal como lo propone Santa Cruz, Roberto [9] en su modelo orientado al sector micro financiero.
- Asimismo, tal como concluye Peña, Moscoso y Soto[10] en su trabajo de investigación entidades del estado no cuentan y si cuentan no de la manera correcta, un plan de gestión de riesgos de ti que colabore con los procesos de la organización, dentro de nuestra investigación y raíz del diagnóstico del sector identificamos que la organización cuenta con procedimientos para la gestión de riesgos sin embargo no cuentan con un plan resultado de un proceso y metodología.
- Por otra parte, la investigación de Huaura, Miguel [11] quien propone como modelo de gestión de riesgos de seguridad de la información basado en ISO/IEC 31000, concluye en que una correcta y eficiente gestión de riesgos influye en la correcta toma de decisiones de la alta dirección para la continuidad del negocio, este proyecto recomienda que es necesaria una participación mayor de la alta dirección en las fases del modelo.
- En general el modelo propuesto consta de 4 etapas para la gestión de riesgos de tecnologías de información, cada etapa presenta plantillas para identificación, clasificación y análisis de los riesgos de la misma manera en que Villegas, Cesar [12] propone de manera ordenada en su trabajo de investigación.

5.- Conclusiones

1.- Para el desarrollo de la siguiente investigación, se realizó el proceso de armonización de estándares internacionales y marcos de trabajo fundados en la gestión de riesgos de tecnologías de información, esto con la finalidad de proponer un modelo acorde a una empresa de telecomunicaciones. Para el desarrollo del proceso se cumplieron las fases de la metodología como homogenización de modelos, comparación entre modelos, análisis entre modelos y análisis de resultados. Mayor detalle visualizar en el anexo 06

2.- El modelo de gestión de riesgos de TI fue propuesto con el objetivo de determinar el impacto de un modelo de gestión de riesgos de TI en la operación de procesos Core en las empresas de telecomunicaciones. En consecuencia, después del diagnóstico del sector y el proceso de armonización, el modelo como producto consta de 04 etapas las cuales servirán de base para cumplir con el objetivo general; dichas fases son las siguientes: Definir el Alcance, Evaluación del Riesgo, Tratamiento del Riesgo y por último el monitoreo.

3.- El modelo de gestión de riesgos de TI propuesto, fue validado por 03 expertos. Por medio de Alfa de Cronbach se determinó el nivel de confiabilidad, obteniendo un resultado de 0.93, catalogando con “Excelente confiabilidad”; luego se analizó la concordancia de los resultados por medio del Coeficiente de Concordancia W de Kendall; como resultado el valor de significancia obtenido se situó por debajo de 0.05; ergo, el modelo es apropiado para las empresas del sector de telecomunicaciones.

4.- Se implementó de manera parcial el modelo de gestión de riesgos de TI, en una empresa de telecomunicaciones, como resultado se identificaron 40 riesgos, 09 de ellos fueron categorizados con prioridad alta, y se plantearon proyectos para tratar estos riesgos, colaborando así con la operación del proceso de operaciones en la empresa.

6.- Recomendaciones

- En la implementación parcial del modelo pudimos identificar que en la primera etapa del modelo (alcance del entorno) se pudo involucrar a otras áreas directivas de la organización, con la finalidad de tener una mayor visualización de toda empresa y los

riesgos que estas enfrentas, por lo que se recomienda profundizar en el alcance del entorno.

- Se recomienda que el modelo propuesto pueda extenderse hacia otras áreas de la empresa, sabemos que hoy en día enfrentan amenazas y vulnerabilidades que pueden extenderse a través de otras áreas dada la integración de estas, cubriendo mayores áreas y en consecuencia teniendo mayor cobertura, conoceremos mejor todos los riesgos y desarrollar más proyectos y tomar mayores acciones preventivas.
- Se recomienda que el proceso y la gestión de riesgos de tecnologías de información se convierta en una actividad diaria de todas las áreas de la organización, partiendo de un plan de gestión de riesgos.

7.- Referencias

- [1] C. Pardo, M. Cuellar, y M. Correa Valencia, «Armonización de Múltiples Modelos para el Gobierno de TI y el Desarrollo de Software», 2014. [En línea]. Available: <https://www.researchgate.net/publication/283546897>
- [2] Comisión de Reglamentos Técnicos y Comerciales - INDECOPI, *NORMA TÉCNICA NTP-ISO/IEC 17799 PERUANA 2007*, vol. 2. 2007, pp. 1-173.
- [3] M. Lucila Guerrero Julio y L. Carlos Gómez Flórez, «Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional», pp. 87-95, 2012, [En línea]. Available: www.elsevier.es/estudios_gerenciales
- [4] L. Ortiz y F. J. Valencia, «Gestión de riesgos en eTOM. Un análisis comparativo con los estándares de riesgo corporativo», *Revista Logos, Ciencia & Tecnología*, vol. 9, n.º 1, jul. 2017, doi: 10.22335/rlct.v9i1.334.
- [5] EFE News Service, «BlackBerry dice que el fallo de un interruptor provocó la caída de servicios: CANADÁ BLACKBERRY (Actualización) - ProQuest», oct. 11, 2011. <https://www.proquest.com/docview/897115225/ACEDEEC5D24F4566PQ/1?accountid=45277> (accedido dic. 07, 2021).
- [6] H. D. Barrios, «En Vivo | Chiclayo | reportan incendio en el centro de la ciudad | Irnd | Sociedad | La República», jun. 2020. Accedido: dic. 06, 2021. [En línea]. Available: <https://larepublica.pe/sociedad/2020/06/19/en-vivo-chiclayo-reportan-incendio-en-el-centro-de-la-ciudad-lrnd/>
- [7] EFE News Service, «Nuevo apagón de internet paraliza brevemente servicios de bancos y aerolíneas: FALLO INTERNET - ProQuest», jun. 17, 2021. <https://www.proquest.com/docview/2541730487/93F0EDD6DBDC4F45PQ/8?accountid=45277> (accedido dic. 07, 2021).
- [8] EFE News Service, «Caídas en telecomunicaciones de Perú se duplicaron en 2018 con 13.419 casos: PERÚ TELECOMUNICACIONES», Madrid, may 2019. [En línea]. Available: http://fresno.ulima.edu.pe/ss_bd00102.nsf/RecursoReferido?OpenForm
- [9] R. Santa Cruz, «MODELO DE GESTIÓN DE RIESGOS DE TI PARA EL CUMPLIMIENTO DE LAS EXIGENCIAS DE LA SBS EN SECTOR MICROFINANCIERO DE CHICLAYO», UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO, CHICLAYO, 2018. Accedido: ene. 18, 2022. [En línea]. Available:

- <https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/6116/BC-1957%20SANTA%20CRUZ%20ACOSTA.pdf?sequence=1&isAllowed=y>
- [10] L. Moscoso, E. Peña, y M. Soto, «MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE A LA OPERACIÓN DE LOS PROCESOS DE GESTIÓN COMERCIAL DE LAS EMPRESAS DEL SECTOR DE SANEAMIENTO DEL NORTE DEL PERÚ», UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO, CHICLAYO, 2018.
- [11] M. Huaura Mere, «Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones», Universidad Nacional Mayor de San Marcos, Lima, 2019.
- [12] C. Villegas, «MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE EN LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN EN HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS», 2022. [En línea]. Available: <https://orcid.org/0000-0003-0409-8773>
- [13] ISO.ORG, «ISO 31000:2018(es), Gestión del riesgo — Directrices», 2018. <https://www.iso.org/obp/ui/es/#iso:std:iso:31000:ed-2:v1:es> (accedido dic. 21, 2021).
- [14] I. Casares y E. Lizarzaburu, «INTRODUCCIÓN A LA GESTIÓN INTEGRAL DE RIESGOS EMPRESARIALES ENFOQUE ISO 3100», may 2016.
- [15] F. J. Valencia Duque, «La Auditoría Continua, una herramienta para la modernización de la función de auditoría en las organizaciones y su aplicación en el Control Fiscal Colombiano», 2015, Accedido: dic. 30, 2021. [En línea]. Available: <https://repositorio.unal.edu.co/handle/unal/55045>
- [16] G. Vanegas Devia y C. Pardo, «Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT», Colombia, 2014. [En línea]. Available: http://www.icesi.edu.co/revistas/index.php/sistemas_telematica
- [17] ISACA, *Marco de referencia COBIT® 2019: Introducción y metodología*. 2018. [En línea]. Available: www.isaca.org/COBITuse.
- [18] Dirección General de Modernización Administrativa, «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método», ESPAÑA, 2012. [En línea]. Available: <http://administracionelectronica.gob.es/>
- [19] Dirección General de Modernización Administrativa, «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de elementos», 2012. [En línea]. Available: <http://administracionelectronica.gob.es/>
- [20] «Directorio de concesionarios públicos - Informes y publicaciones - Ministerio de Transportes y Comunicaciones - Gobierno del Perú».

<https://www.gob.pe/institucion/mtc/informes-publicaciones/322450-directorio-de-concesionarios-publicos> (accedido ago. 05, 2022).

- [21] F. J. Pino, F. Garcia, y M. Piattini, «Homogenization of Models to Support Multi-model Processes in Improvement Environments», 2009. [En línea]. Available: <https://www.researchgate.net/publication/220738576>
- [22] J. Escobar-Pérez y Á. Cuervo-Martínez, «VALIDEZ DE CONTENIDO Y JUICIO DE EXPERTOS: UNA APROXIMACIÓN A SU UTILIZACIÓN», 2008.

8.- Anexos

Anexo 01 Encuesta de Gestión de Riesgos de tecnologías de información.

Encuesta de Gestión de Riesgos de Tecnologías de Información

Objetivo: El objetivo de la presente encuesta es identificar el nivel de gestión de riesgos de tecnologías de información aplicado en la institución.

Instrucciones: Favor marque con un aspa (X), la respuesta que se ajuste mejor a la realidad de su empresa.

NÚMERO	PREGUNTA	SI	NO
1	¿Realizan en su empresa un análisis de la gestión de riesgos de TI?		
2	¿Cuentan con un método para la búsqueda y clasificación de los riesgos de TI?		
3	¿Cuentan con un método para el análisis de los riesgos de TI?		
4	¿Cuentan con un registro de datos relevantes relacionados con los riesgos de TI?		
5	¿Cuentan con un registro/ historial de los eventos de riesgo y su impacto en el negocio?		
6	¿Cuentan con una clasificación de factores causantes de riesgos?		
7	¿Tienen conocimiento del momento en el que debe realizar análisis de riesgos existentes o nuevos?		
8	¿Cuentan con un plan de gestión de riesgos de TI, definiendo la criticidad de sus activos?		
9	¿Cuentan con un análisis de impacto de riesgos de TI relacionado tolerancias al riesgo?		
10	¿Cuentan con un plan para gestión de riesgos de TI que excedan la tolerancia?		
11	¿Cuentan con una aprobación o validación del impacto de riesgos de TI?		
12	¿Cuentan con un análisis de costo/beneficio frente a la respuesta al riesgo de TI?		

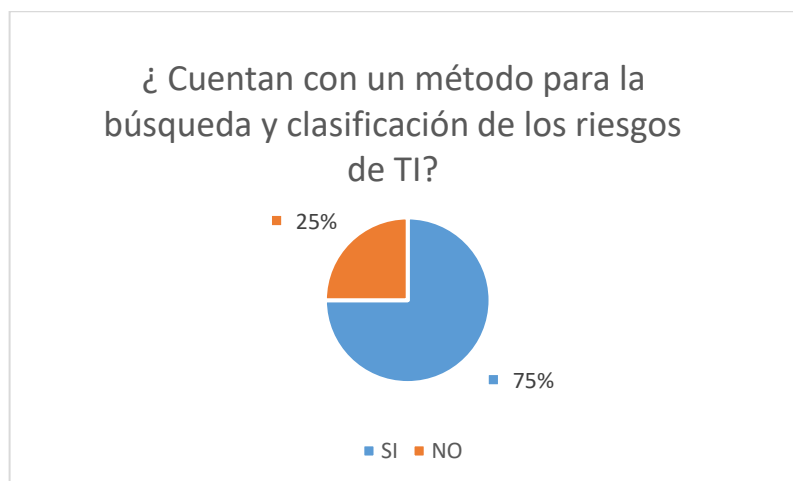
13	¿Cuentan con un inventario de los procesos de negocio y su dependencia con los servicios de TI (personal, infraestructura)?		
14	¿Cuentan con un inventario de los procesos de negocio y su dependencia con los servicios externos (partners)?		
15	¿Cuentan con un plan de comunicación del análisis de riesgos de TI a las áreas involucradas de la empresa?		
16	¿Cuentan con una evaluación del impacto a pérdidas de TI, con relación a consideraciones de reputación, legal y/o regulatorias?		
17	¿Cuentan con evaluación y/o auditorías de riesgos de TI por empresas especializadas?		
18	¿Cuentan con un inventario de actividades de control para mitigar el riesgo (procedimientos)? (plan de contingencia)		
19	¿Cuentan con un plan de proyectos para reducir el riesgo considerando costos, beneficios, perfil de riesgo?		

Resultados de encuestas aplicadas

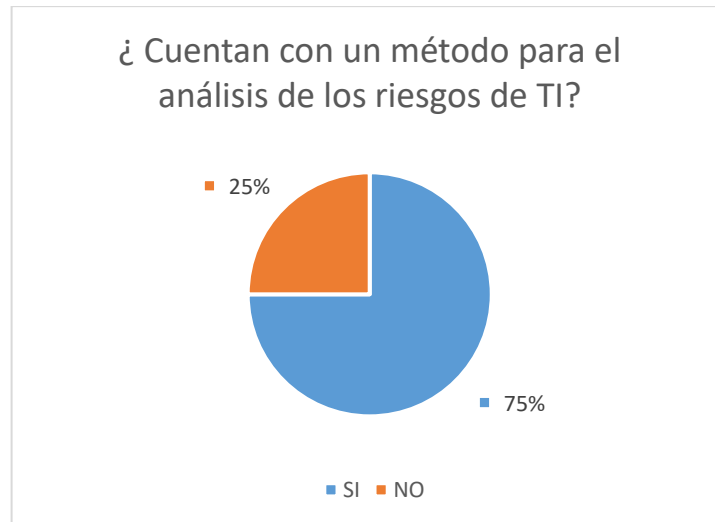
PREGUNTA 1 ¿Hacen un análisis de la gestión de riesgos?



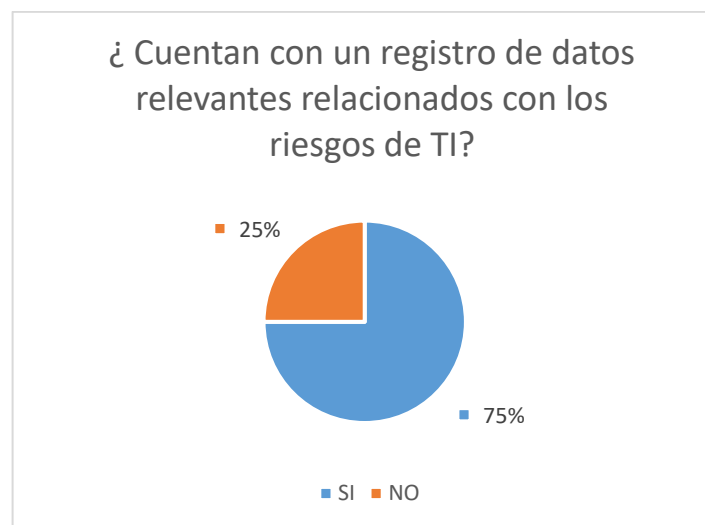
Pregunta 2 ¿Cuentan con un método para la búsqueda y clasificación de los riesgos de TI?



Pregunta 3 ¿Cuentan con un método para el análisis de los riesgos de TI?

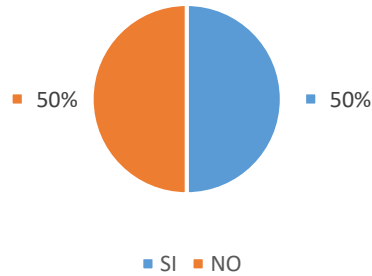


Pregunta 4 ¿ Cuentan con un registro de datos relevantes relacionados con los riesgos de TI?



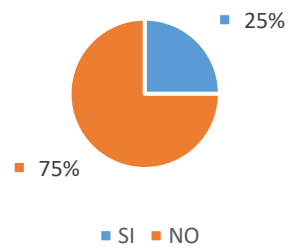
Pregunta 5 ¿Cuentan con un registro/ historial de los eventos de riesgo y su impacto en el negocio?

¿ Cuentan con un registro/ historial de los eventos de riesgo y su impacto en el negocio?



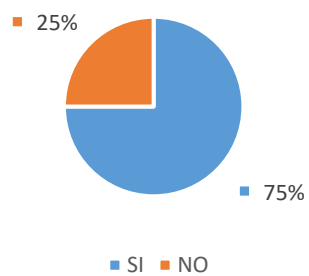
Pregunta 6 ¿Cuentan con una clasificación de factores causantes de riesgos?

¿ Cuentan con una clasificación de factores causantes de riesgos?

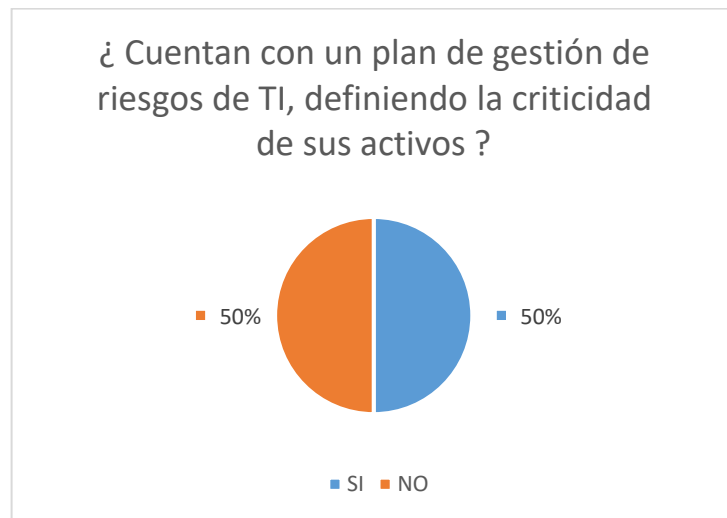


Pregunta 7 ¿Tienen conocimiento del momento en el que debe realizar análisis de riesgos existentes o nuevos?

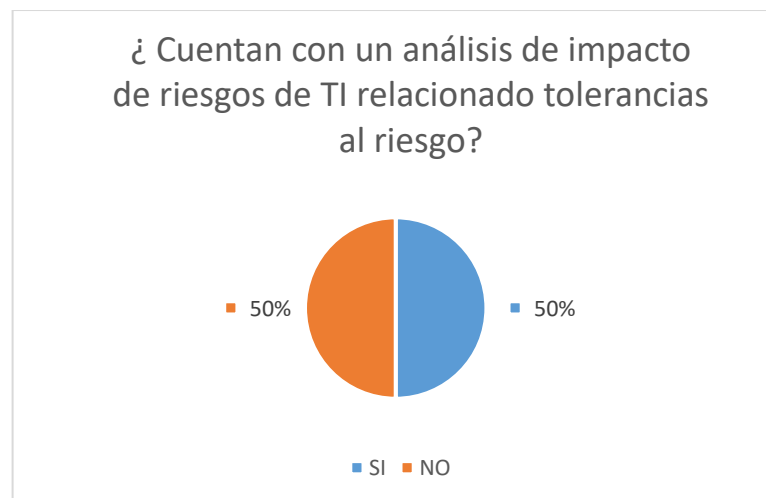
¿ Tienen conocimiento del momento en el que debe realizar análisis de riesgos existentes o nuevos?



Pregunta 8 ¿Cuentan con un plan de gestión de riesgos de TI, definiendo la criticidad de sus activos?



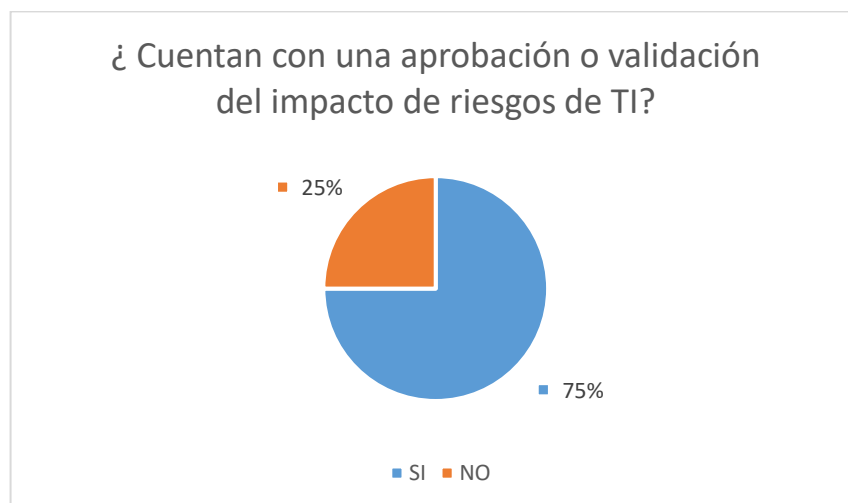
Pregunta 9 ¿Cuentan con un análisis de impacto de riesgos de TI relacionado tolerancias al riesgo?



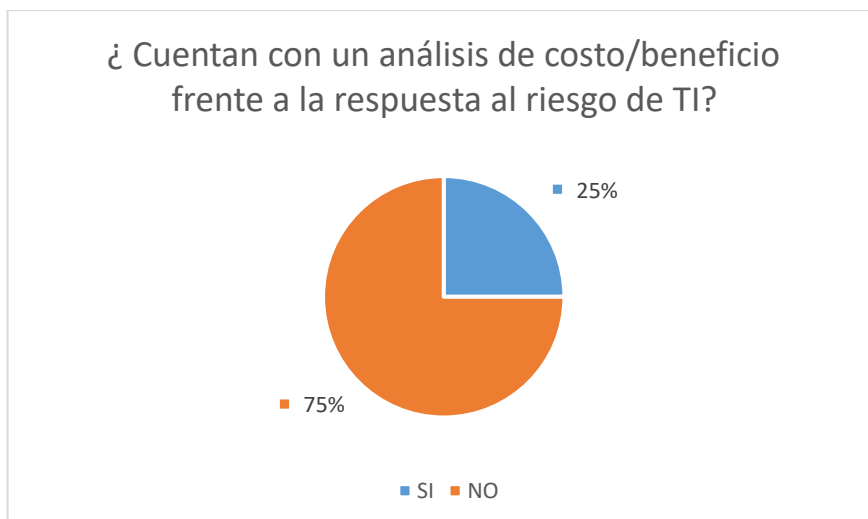
Pregunta 10 ¿Cuentan con un plan para riesgos que excedan la tolerancia?



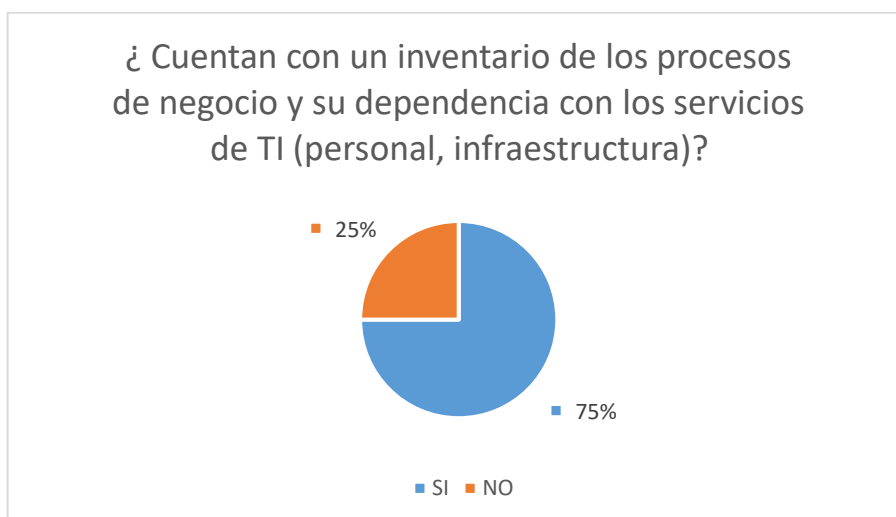
Pregunta 11 ¿Cuentan con una aprobación o validación del impacto de riesgos de TI?



Pregunta 12 ¿Cuentan con un análisis de costo/beneficio frente a la respuesta al riesgo de TI?

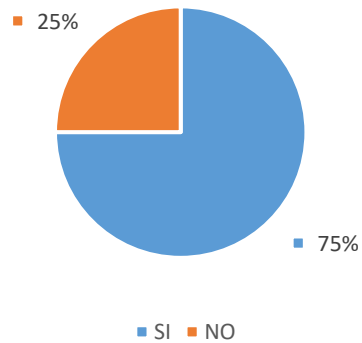


Pregunta 13 ¿ Cuentan con un inventario de los procesos de negocio y su dependencia con los servicios de TI (personal, infraestructura)?



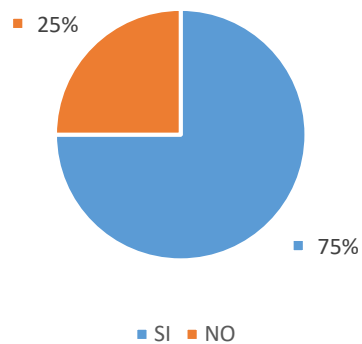
Pregunta 14 ¿Cuentan con un inventario de los procesos de negocio y su dependencia con los servicios externos (partners)?

¿ Cuentan con un inventario de los procesos de negocio y su dependencia con los servicios externos (partners)?



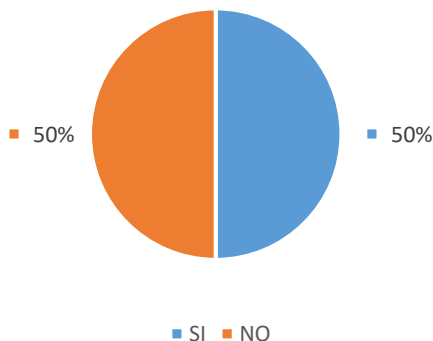
Pregunta 15 ¿Cuentan con un plan de comunicación del análisis de riesgos de TI a las áreas involucradas de la empresa?

¿ Cuentan con un plan de comunicación del análisis de riesgos de TI a las áreas involucradas de la empresa?



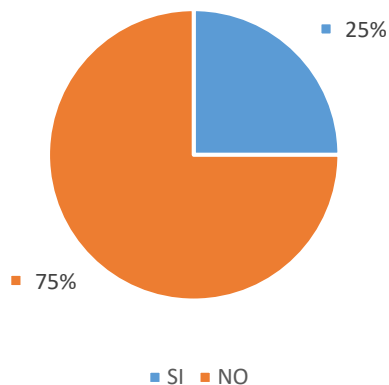
Pregunta 16 ¿Cuentan con una evaluación del impacto a pérdidas de TI, con relación a consideraciones de reputación, legal y/o regulatorias?

¿ Cuentan con una evaluación del impacto a pérdidas de TI, en relación a consideraciones de reputación, legal y/o regulatorias?



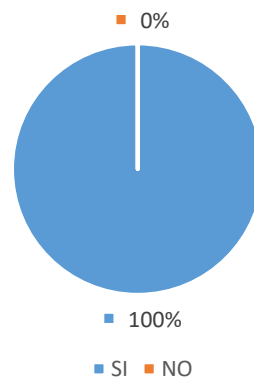
Pregunta 17 ¿Cuentan con evaluación y/o auditorías de riesgos de TI por empresas especializadas?

¿ Cuentan con evaluación y/o auditorías de riesgos de TI por empresas especializadas?



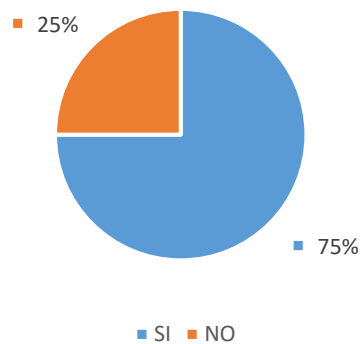
Pregunta 18 ¿Cuentan con un inventario de actividades de control para mitigar el riesgo (procedimientos)? (plan de contingencia)

¿ Cuentan con un inventario de actividades de control para mitigar el riesgo (procedimientos)?
(plan de contingencia)



Pregunta 19 ¿ Cuentan con un plan de proyectos para reducir el riesgo considerando costos, beneficios, perfil de riesgo?

¿ Cuentan con un plan de proyectos para reducir el riesgo considerando costos, beneficios, perfil de riesgo?



Anexo 02 : Matriz de consistencia

MATRIZ DE CONSISTENCIA						
Modelo de gestión de riesgos de TI que contribuye la operación de procesos Core en empresas de telecomunicaciones						
<u>FORMULACIÓN DEL PROBLEMA</u>			<u>METODOLOGIA DE LA INVESTIGACION</u>			
¿De qué manera un modelo de gestión de riesgos de TI impactará en la operación de los procesos core en empresas de telecomunicaciones?			TIPO DE INVESTIGACION			
			APLICADA - PRE EXPERIMENTAL			
<u>OBJETIVO GENERAL</u>		<u>METODO</u>		<u>DESCRIPCION</u>		
<p>El objetivo general del proyecto determinar el impacto de un modelo de gestión de riesgos de ti en la operación de los procesos core en empresas de telecomunicaciones.</p> <p>HIPOTESIS: la elaboración de un modelo de gestión de riesgos de TI impacta de forma positiva en la operación de los procesos core en empresas de telecomunicaciones.</p> <p>Variable independiente Modelo de gestión de riesgos de TI</p> <p>Variable dependiente nivel de operación de procesos core en empresas de telecomunicaciones</p>		analítico		Estudio y análisis de plan de Gestión de Riesgos		
		deductivo		Estrategia para el desarrollo de un modelo de gestión de riesgos de TI		
		implementación				
		<u>TÉCNICAS</u>		<u>INSTRUMENTOS</u>		<u>ELEMENTOS DE LA POBLACION</u>
		<u>PROPÓSITO</u>				
		Análisis bibliográfico		Fichas bibliográficas	-	
		Encuesta		Cuestionario	Directores de TI	Conocer el nivel de operación de los procesos core
Observación		Ficha de observación				
<u>OBJETIVOS ESPECIFICOS</u>		<u>DESCRIPCION DEL LOGRO DE LOS OBJETIVOS ESPECIFICOS</u>		<u>INDICADORES</u>		
1. Armonizar los estándares y metodologías de la Gestión de Riesgos de Tecnologías de la Información (TI).		Listar y comparar estándares y metodologías				
2. Incrementar la capacidad para la detección y tratamiento de los riesgos.		modelo propuesto		Numero de riesgos detectados en piloto		
3. Validar el modelo de Gestión de Riesgos de TI propuesto para mejorar los procesos Core en empresas de servicio de telecomunicaciones		validación		Valor confiabilidad Alfa de Cronbach Valor Concordancia de expertos - Kendall		
4. Realizar la implementación de un piloto en una empresa del sector.		Confirmación de encargado		Documento de aceptación de parte de encargado del área		

Anexo 03: Plantilla de juicio de expertos.

FORMATO PARA VALIDACION DE EXPERTO DE MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitarle su apoyo en la validación de la propuesta realizada en la investigación que lleva como título **Modelo de gestión de riesgos de TI que contribuye a la operación de procesos Core en empresas de telecomunicaciones.**

Para tal fin, se anexa la matriz de consistencia para validación.

1.- DATOS PERSONALES

NOMBRES Y APELLIDOS: _____

FORMACIÓN ACADÉMICA : _____

AREAS DE EXPERIENCIA PROFESIONAL: _____

TIEMPO : _____

CARGO ACTUAL : _____

INSTITUCIÓN : _____

2.- OBJETIVOS

Objetivo de la investigación: Determinar el impacto de un modelo de gestión de riesgos de ti en la operación de los procesos Core en empresas de telecomunicaciones.

Objetivo del juicio de expertos: Verificar la validez del modelo en relación con la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba: Determinar la utilidad del modelo propuesto para la empresa ABC PERU.

De acuerdo son los siguientes indicadores califique cada uno de los ítems según corresponda.

CATEGORIA	CALIFICACIÓN	INDICADOR
SUFICIENCIA	1 no cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.

	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes
CLARIDAD	1 No cumple con el criterio	El ítem no es claro.
El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
	COHERENCIA	1 No cumple con el criterio
El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA	1 No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
El ítem es esencial o importante, es decir debe ser incluido.	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado Nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy importante y debe ser incluido.

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE A LA OPERACIÓN DE PROCESOS CORE EN EMPRESAS DE TELECOMUNICACIONES

ETAPA I: DEFINICION DEL ALCANCE						
PROCESO	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Proceso 1: Revisión SID SUNARP	Identificar los procedimientos legales asociados a las empresas de telecomunicaciones.					
Proceso 2: Mantenimiento PDT PLAME	Identificar los procedimientos laborales asociados a empresas del sector telecomunicaciones.					
Proceso 3: Validación de Concesión y permisos MTC	Identificar los procedimientos regulatorios asociados a las empresas de telecomunicaciones.					
ETAPA II: EVALUACION DEL RIESGO						
Proceso 1: Inventario de Activos	Identificación de activos : conocer todos los activos con los que cuenta la empresa					
	Clasificación de activos					
	Dependencia de activos: identificar los activos y su dependencia					
	Valoración de activos					

Proceso 2: Identificación del riesgo.	Encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. (En base a metodología MAGERIT)					
Proceso 3: Análisis del riesgo.	Comprender la naturaleza del riesgo y sus características					
Proceso 4: Valoración del riesgo.	Comparación de los resultados del análisis del riesgo con sus criterios					
ETAPA III: TRATAMIENTO DEL RIESGO						
Proceso 1: Tratamiento del Riesgo.	Definición de acciones para reducir, prevenir, transferir o asumir los riesgos					
ETAPA IV: MONITOREO						
Proceso 1: Monitoreo del riesgo	El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo					

ACEPTACION	
OBSERVADO	
DISCONFORMIDAD	


NOMBRE :

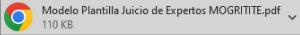
DNI:

Anexo 04: Respuesta de juicio de expertos.

JURADO 1:

Re: Consulta evaluación Juicio de expertos - Tesis USAT

 Romulo Lomparte <romulo.lomparte@yahoo.com>
 Para Daniel Alonso Romero Garcia



Hola Ing. Rómulo

Buenas tardes.

Quiso saludarlo, lleve el curso de Gobierno de TI dentro de la maestría de ingeniería de sistemas en la USAT, ahora me encuentro en el desarrollo de la tesis para esta etapa es necesaria la evaluación de mi modelo por expertos, quería consultarle si podría compartirme mi modelo, evaluarlo y brindar feedback del mismo.

Alguna duda, podría comunicarme con usted y brindar mayor detalle de lo solicitado.


Gracias de antemano por su gentil respuesta.

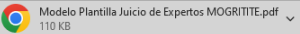
Saludos cordiales

Daniel Romero Garcia

+51 948 445 007

Re: Consulta evaluación Juicio de expertos - Tesis USAT

 Romulo Lomparte <romulo.lomparte@yahoo.com>
 Para Daniel Alonso Romero Garcia



Disculpe:

Adjunto el archivo solicitado.

Saludos cordiales,

Rómulo Lomparte A.
 MBA, PMP, CISA, COBIT, CRISC, CISM, CDPSE, CSX, QMSLA, IRCA, IATCA, ISO 27002, CRMA, RWPC, COBIT Foundation, Coach, APMG Trainer, Scrum SFPC, BIFPC

El domingo, 15 de enero de 2023, 22:47:51 PET, Daniel Alonso Romero Garcia <daniel.comeron@outlook.com> escribió:

Hola Ing. Romulo

Buenas noches.

Agradezco el tiempo brindado, como conversamos adjunto plantilla de juicio de expertos para evaluación.

Alguna duda o consulta, favor comunicar.

JURADO2:

Re: Juicio de expertos - Validación Modelo Gestión de Riesgos - Daniel Romero - USAT

PM PAUL MARTIN VILLACORTA CHAVEZ <ingpaulvillacorta@gmail.com>
Para Daniel Alonso Romero Garcia

Modelo Plantilla Juicio de Expertos MOGRITTEV2.docx
89 KB

Iniciar la respuesta a todos con: Muchas gracias. Excelente, gracias. Muchas gracias, así será. Comentarios

Hola Ing. Paul

Buenos días,

Gusto saludarlo, como le comente agradeceré su apoyo para validación del siguiente modelo de gestión de riesgos de tecnologías de información para el sector de telecomunicaciones.

Adjunto implementación parcial y plantilla de juicio de expertos.

Alguna duda o consulta, favor comunicar.

Re: Juicio de expertos - Validación Modelo Gestión de Riesgos - Daniel Romero - USAT

PM PAUL MARTIN VILLACORTA CHAVEZ <ingpaulvillacorta@gmail.com>
Para Daniel Alonso Romero Garcia

Modelo Plantilla Juicio de Expertos MOGRITTEV2.docx
89 KB

Iniciar la respuesta a todos con: Muchas gracias. Excelente, gracias. Muchas gracias, así será. Comentarios

Servido mi estimado.

Sigue adelante hasta alcanzar el objetivo del grado y luego sigue la certificación PMI.

Saludos cordiales,

Paul Villacorta

JURADO 3:

Juicio de expertos - Validación Modelo Gestión de Riesgos - Daniel Romero - USAT

 Daniel Alonso Romero García
Para epena@usat.edu.pe
CC daniel.romerog@outlook.com

Responder Responder a todos Reenviar

viernes 13/01/2023 11:39

Hola Ing. Edgard

Buenos días,

Gusto saludarlo, como le comente agradeceré su apoyo para validación del siguiente modelo de gestión de riesgos de tecnologías de información para el sector telecomunicaciones.

Adjunto implementación parcial y plantilla de juicio de expertos.

Alguna duda o consulta, favor comunicar.

Agradezco de antemano su apoyo y predisposición.


Modelo Gestion de Riesgos de T... Plantilla Juicio de Expertos M...

Saludos cordiales

Daniel Romero García

+51 948 445 007
daniel.romerog@outlook.com


RV: Juicio de expertos - Validación Modelo Gestión de Riesgos - Daniel Romero - USAT

 Peña Nuñez Edgard Esau <epena@usat.edu.pe>
Para daniel.romerog@outlook.com

Responder Responder a todos Reenviar

domingo 15/01/2023 11:38

Se han quitado los saltos de línea adicionales de este mensaje.

 Plantilla Juicio de Expertos MOGRITITE Daniel Romero FIRMADA.pdf
1 MB

Estimado Daniel, un cordial saludo

Envío el documento de Juicio de expertos realizado por mi persona, tambien he sugerido algunas mejoras, despues me parece todo correcto en tu modelo.

Que te vaya super bien.

Saludos

Mtro. Edgard Peña Nuñez
Coordinador de Desarrollo de Sistemas
Av. San Josemaría Escrivá 855. Chiclayo - Perú
T: (074) 606200 - Anexo 4051
<https://na01.safelinks.protection.outlook.com/?url=http%3A%2Fwww.usat.edu.pe%2F&data=05%7C01%7C7C22454f306ad64502826808daf7171af2%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C638093976064231229%7CUnknown%7CTWFpbGZsb3d8eyJWljiOiMC4wLjAwMDA1CjQjoiV2luMzIiLCBIIi6iK1haWwIiLCJXVCi6Mn0%3D%7C3000%7C%7C&sdata=LyqnH2%28SD3DFRBLrNJzaEL66cOggTln%2FY5owGtn%2Fr4Y%3D&reserved=0>
https://na01.safelinks.protection.outlook.com/?url=http%3A%2Fwww.facebook.com%2Fusat_peru&data=05%7C01%7C7C22454f306ad64502826808daf7171af2%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C638093976064231229%7CUnknown%7CTWFpbGZsb3d8eyJWljiOiMC4wLjAwMDA1CjQjoiV2luMzIiLCBIIi6iK1haWwIiLCJXVCi6Mn0%3D%7C3000%7C%7C&sdata=bfr99%2FclERWnBJ8esenuX45iacS8kyS57DMebWElUfP%3D&reserved=0

Anexo 05: Implementación parcial del modelo.

La presente simulación hace referencia al servicio de telefonía fija de la empresa ABC PERU.

ETAPA 1: DEFINICION DEL ALCANCE

En la etapa inicial del modelo propuesto, la definición del alcance permitirá conocer a la organización ABC PERU y su entorno con relación al riesgo de TI, así también los principales procedimientos legales y regulatorios asociados a las empresas de telecomunicaciones.

1.1 Revisión Sid Sunarp:

La constitución de empresa es un procedimiento a través del cual una persona o grupo de personas registran su empresa ante el Estado para que este les ofrezca los beneficios de ser formales. En el siguiente acceso (Sistema de intermediación digital) se podrá registrar, completar los datos necesario para inscripción de la empresa:

Toda la información se podrá validar en el siguiente enlace:

<https://www.sunarp.gob.pe/w-sid/index.html>

1.2 Mantenimiento PDT Plame: (Programa de Declaración Telemática, PDT).

La planilla electrónica es un documento que las empresas o personas naturales con más de tres trabajadores deben presentar todos los meses a la Superintendencia Nacional de Aduanas y de Administración Tributaria SUNAT y el Ministerio del Trabajo (MTPE). Esta cuenta permite a toda empresa realizar diversas operaciones con la finalidad de mantener formalizada su empresa, cumpliendo la normativa legal vigente.

Entre las principales funcionalidades se tiene:

- Dar de Alta a todo trabajador.
- Dar de Baja al trabajador que culmina su vínculo laboral.

- Declarar en la Planilla de la Empresa a los trabajadores, así como sus remuneraciones y todo ingreso percibido.

Las empresas deben incluir a los trabajadores en la planilla electrónica antes de que cumplan las 72 horas de haber iniciado sus actividades laborales. Cuando estas no cumplen con lo establecido se exponen a ser multadas por el Ministerio de Trabajo.

El monto de la multa se encuentra entre 1 Unidad Impositiva Tributaria (UIT) y 20 Unidades Impositivas Tributarias (UIT).

Mayor detalle se podría visualizar en el siguiente enlace:

<https://www.youtube.com/watch?v=DPMdNurElw4>

Esta actividad corresponde al llenado con los datos de todos los colaboradores de la empresa, como se visualiza a continuación:

FECHA DE INGRESO	CÓDIGO	TIPO DE DOC DE IDENT	NÚMERO DEL DOC DE IDENT	APELLIDO PATERNO	APELLIDO MATERNO	PRIMERO NOMBRE	SEGUNDO NOMBRE	NACIONALIDAD	FEC NACIMIENTO	SEXO ("M" o "F")	ESTADO CIVIL
		(TABLA: T1)						(TABLA: T2)			(TABLA: T3)
19/04/2021	44249924	01-DNI	44249924	ROMERO	GARCIA	DANIEL	ALONSO	PERU	12/10/1986	M	SOLTERO
19/05/2020	46075257	01-DNI	46075257	JULCA	ROJAS	ROBERTO	ALBERTO	PERU	18/08/1989	M	SOLTERO

Ilustración 6: Ejemplo alta trabajador - SUNAT


T-Registro: Registro de Prestadores

CONSTANCIA DE ALTA DEL TRABAJADOR Formulario 1604-1 Comprobante de Información Registrada

Con el número de orden 116175983 se realizó satisfactoriamente el registro del trabajador el 18/05/2021 a las 17:13:35, según el siguiente detalle:

EMPLEADOR

Número de RUC:	20262207774	Nombre o razón social:	CONVERGIA PERU S.A.
-----------------------	-------------	-------------------------------	---------------------

TRABAJADOR - Datos de identificación

Tipo y número de documento:	LE / DNI - 44249924	Fecha de nacimiento:	12/10/1986
Pais emisor del documento:	PERÚ	Apellidos y nombres:	ROMERO GARCIA DANIEL ALONSO
Sexo:	Masculino	Estado civil:	SOLTERO
Nacionalidad:	PERU		
Teléfono:	948445007	Correo electrónico:	daniel.romerog@outlook.com
Primera dirección:	AV. BRIGIDA SILVA DE OCHOA 165 TORRE 24 INT. 1101 LIMA-LIMA-SAN MIGUEL		
Segunda dirección:	-		
Referente para Centro Asistencial EsSalud:	AV. BRIGIDA SILVA DE OCHOA 165 TORRE 24 INT. 1101 LIMA-LIMA-SAN MIGUEL		

TRABAJADOR - Datos laborales

Periodos laborales:

Fecha de inicio	Fecha de fin	Motivo de baja

1.3. Validación de concesión y permisos Ministerio de Transportes y Comunicaciones (MTC)

Para una empresa del sector Telecomunicaciones es necesario revisar los datos de los concesionarios de servicios públicos de Telecomunicaciones.

En el siguiente enlace web <https://www.gob.pe/institucion/mtc/informes-publicaciones/322450-directorio-de-concesionarios-publicos> podemos visualizar los contratos de asociación público privadas y otros de similar naturaleza suscritos por el Ministerio de Transportes y Comunicaciones.

Adicionalmente en caso se desea registrar como proveedor de servicio de telecomunicaciones, se podrá realizar el trámite desde el siguiente acceso <https://www.gob.pe/8063>

Ilustración 7: Ejemplo de validación Concesión del MTC

15	CONVERGIA PERÚ S.A.	AV. LOS LIBERTADORES N° 155 PISO 2	SAN ISIDRO	LIMA	LIMA	CARLOS GUSTAVO MENDOZA CARRASCO
16	EMPRESA NACIONAL DE TELECOMUNICACIONES BOLIVIA S.A.C.	AV. NICOLAS DE RIBERA 885 DPTO. 101	SAN ISIDRO	LIMA	LIMA	JUAN ALFONSO JOSE PEREYRA SARMIENTO
17	ENTEL PERÚ S.A.	AV. REPUBLICA DE COLOMBIA N° 791	SAN ISIDRO	LIMA	LIMA	SEBASTIAN VILLEGAS BACIGALUPO

CARLOS GUSTAVO MENDOZA CARRASCO	RM 0411-99-MTC/15.03 (iii)	20/10/1999	S/N	02/12/1999
	RM 0411-99-MTC/15.03 (iii)	20/10/1999	S/N	02/12/1999
JUAN ALFONSO JOSE PEREYRA SARMIENTO	RM 0081-2019-MTC/01.03	08/02/2019	018-2019-MTC/27	08/05/2019
	RM 0081-2019-MTC/01.03	08/02/2019	018-2019-MTC/27	08/05/2019
SEBASTIAN VILLEGAS BACIGALUPO	RM 0183-2002-MTC/15.03	03/04/2002	S/N	24/05/2002
	RM 0183-2002-MTC/15.03	03/04/2002	S/N	24/05/2002
	RM 0437-2003-MTC/03	09/06/2003	S/N	20/08/2003
	RM 0310-2007-MTC/03	27/06/2007	S/N	27/09/2007
	RM 0683-2004-MTC/03	10/09/2004	S/N	23/09/2004

Fuente: Directorio de concesionarios públicos - MTC [20]

ETAPA 2: EVALUACION DEL RIESGO

La segunda etapa del modelo propuesto consta de la evaluación del riesgo como proceso global de identificación, análisis y valoración del riesgo.

2.1. Inventario de Activos

En esta actividad debemos identificar los activos relevantes para la empresa, su relación y su valor para conocer a que amenazas se encuentran expuestas y poder estimar el impacto y riesgo en caso de algún daño.

2.1.1. Identificación de activos

En esta etapa debemos conocer todos los activos con los que cuenta la empresa, con la finalidad de poder gestionarlos de la mejor manera:

CODIGO	NOMBRE	DESCRIPCION	PROPIETARIO	RESPONSABLE
COD001	SERVTFIJA	Servicio telefonía Fija	EMPRESA ABC	OPERACIONES
COD002	PROVENTAS	Proceso de ventas	EMPRESA ABC	VENTAS
COD003	PROOPERACIONES	Proceso de Operaciones	EMPRESA ABC	OPERACIONES
COD004	GSXLIMPE01 (GSX SONUS)	Media Gateway de Voz	OPERACIONES	OPERACIONES
COD005	LimCat01 (Catalyst 3750)	SW core voz Mpls	OPERACIONES	OPERACIONES
COD006	LimCat02 (Catalyst 3750)	SW core voz Mpls	OPERACIONES	OPERACIONES
COD007	LimRtr01 (Router 7604)	Router Core Voz Mpls	OPERACIONES	OPERACIONES
COD008	PSXLIMPE01 (HP DL380p)	Softswitch	OPERACIONES	OPERACIONES
COD009	DSILIMPE03 (HP DL380p)	Servidor de registro	OPERACIONES	OPERACIONES
COD010	DSILIMPE04 (HP DL380p)	Servidor de registro	OPERACIONES	OPERACIONES
COD011	NGNLIMPE01 (HP DL380p)	Servidor de portabilidad	OPERACIONES	OPERACIONES
COD012	ASX 1 (HP DL380p)	Servidor de registro	OPERACIONES	OPERACIONES
COD013	ASX 2 (HP DL380p)	Servidor de registro	OPERACIONES	OPERACIONES
COD014	ADS (HP DL380p)	Servidor de base de datos	OPERACIONES	OPERACIONES
COD015	NGNLIMPE03 (Dell Power Edge 1850)	Servidor de portabilidad	OPERACIONES	OPERACIONES
COD016	NGNLIMPE02 (Dell Power Edge 730)	Servidor de portabilidad	OPERACIONES	OPERACIONES
COD017	PC_OPERACIONES	PC de Operaciones	OPERACIONES	OPERACIONES
COD018	PC_VENTAS	PC de Ventas	VENTAS	VENTAS
COD019	PC_SOPORTETECNICO	PC de Sopotetecnico	SOPORTETECNICO	SOPORTETECNICO
COD020	PC_CONTABILIDAD	PC de Contabilidad	CONTABILIDAD	CONTABILIDAD
COD021	PC_RRHH	PC de Rrhh	RRHH	RRHH
COD022	IMP_OPERACIONES	Impresora del área de operaciones	OPERACIONES	OPERACIONES

2.1.2. Clasificación de activos

De acuerdo con la metodología MAGERIT[19]: “La relación que sigue clasifica los activos dentro de una jerarquía, determinando para cada uno un código que refleja su posición jerárquica, un nombre y una breve descripción de las características que recoge el epígrafe.”

Primero debemos completar la tabla de descripción de registros que se visualiza a continuación:

Descripción de Activos

ITEM	DESCRIPCION	ETIQUETA
1	[SW] Software	[SW]
2	[S] Servicios	[S]
3	[HW] Equipos informáticos (hardware)	[HW]
4	[COM] Redes de comunicaciones	[COM]
5	[P] Personal	[P]

Clasificación de activos

ITEM	NOMBRE DEL ACTIVO	DESCRIPCION	DESCRIPCION ACTIVO	ETIQUETA
1	GSXLIMPE01 (GSX SONUS)	Media Gateway de Voz	[SW]	[SW - GSXLIMPE01 (GSX SONUS)]
2	LimCat01	SW_core_voz_Mpls	[HW]	[HW - LimCat01]
3	LimCat02	SW_core_voz_Mpls	[HW]	[HW - LimCat02]
4	LimRtr01	Router_Core_Voz_Mpls	[HW]	[HW - LimRtr01]
5	PSXLIMPE01	Softswitch	[SW]	[SW - PSXLIMPE01]
6	DSILIMPE03	Server_Registro	[HW]	[HW - DSILIMPE03]
7	DSILIMPE04	Server_Registro	[HW]	[HW - DSILIMPE04]
8	NGNLIMPE01	Server_Porta	[HW]	[HW - NGNLIMPE01]
9	ASX 1	Server_Registro	[HW]	[HW - ASX 1]
10	ASX 2	Server_Registro	[HW]	[HW - ASX 2]
11	ADS	Server_BD	[HW]	[HW - ADS]
12	NGNLIMPE03	Server_Porta	[HW]	[HW - NGNLIMPE03]
13	NGNLIMPE02	Server_Porta	[HW]	[HW - NGNLIMPE02]
14	SERVTFIJA	Servicio telefonía Fija	[S]	[S - SERVTFIJA]

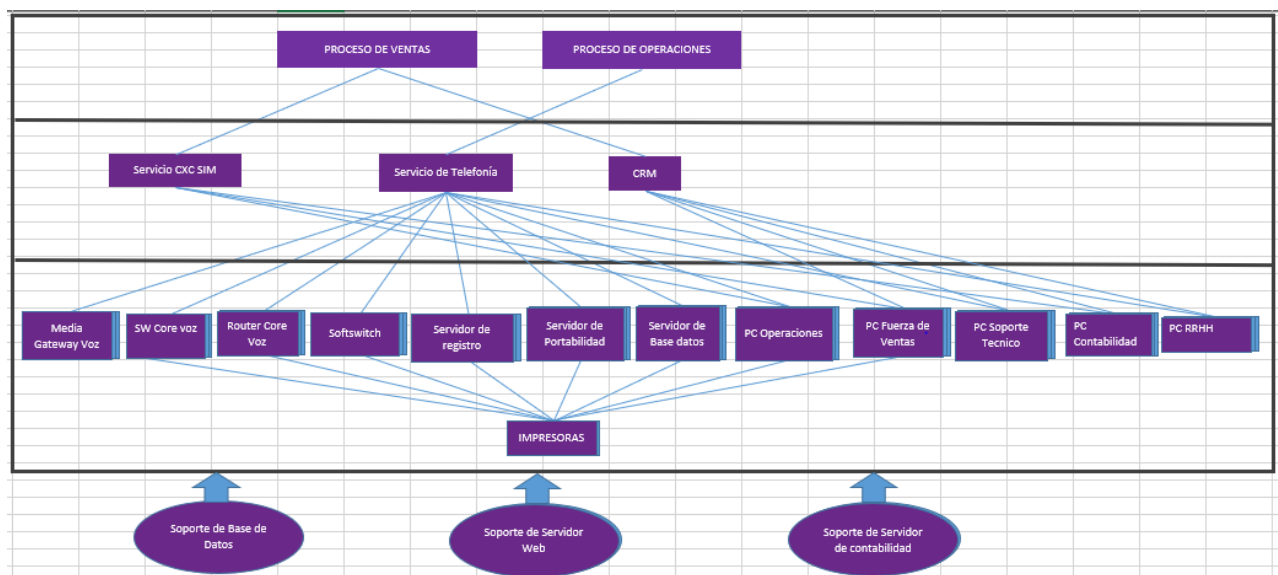
15	PROVENTAS	Proceso de ventas	[S	[S - PROVENTAS]
16	PROOPERACIONES	Proceso de Operaciones	[S	[S - PROOPERACIONES]
17	PC_OPERACIONES	PC_OP	[HW	[HW - PC_OPERACIONES]
18	PC_VENTAS	PC_VEN	[HW	[HW - PC_VENTAS]
19	PC_SOPORTETEC	PC_ST	[HW	[HW - PC_SOPORTETEC]
20	PC_CONT	PC_Cont	[HW	[HW - PC_CONT]
21	PC_RRHH	PC_RRHH	[HW	[HW - PC_RRHH]
22	IMP_OPERACIONES	Impresora de Operaciones	[HW	[HW - IMP_OPERACIONES]

2.1.3. Dependencia de activos

En esta sección debemos identificar los activos y su dependencia, esto con la finalidad de identificar correctamente el activo y su riesgo en la empresa.

Paso inicial es el registro de la plantilla de dependencia de activos.

Dependencia de activos



Fuente: MAGERIT 3.0 [18]

2.1.4. Valoración de activos

La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

Para lo cual debemos considerar lo siguiente:

[D] Disponibilidad

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

[I] Integridad

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

[C] Confidencialidad

Propiedad o característica consistente en que la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Criterios de la Valoración	Valor	Clase	Descripción
Confidencialidad	3	Alta	Activo que solo puede ser de conocimiento estrictamente por algunas personas en particular.
	2	Media	Activo disponible dentro de la organización con restricciones variadas para ciertas áreas.
	1	Baja	Activo que puede ser publicado a cualquier persona de la compañía.
	0	No relevante	Activo que puede ser publicado al público en general
Disponibilidad	3	Alta	El activo debe estar disponible en todo momento.
	2	Media	El activo puede no estar disponible por menos de un día.
	1	Baja	El activo puede no estar disponible por más de un día.
	0	No relevante	El activo puede no estar disponible.

Integridad	3	Alta	El daño o modificación no autorizada generará un fuerte impacto en la empresa y podría conllevar a consecuencias críticas.
	2	Media	El daño o modificación no autorizada generará un impacto significativo en la empresa.
	1	Baja	El daño o modificación no autorizada generará un impacto insignificante o menor en la empresa.
	0	No relevante	El daño o modificación no autorizada no generará un impacto negativo en la empresa.

2.2. Identificación del Riesgo

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.

Para el proceso de identificación de riesgos hemos considerado el catálogo de amenazas proporcionado por MAGERIT[18].

Registro de amenazas

Ítem	DESCRIPCION	ETIQUETA	CONCATENADO
1	Desastres Naturales	[DN]	[DN] Desastres Naturales
2	Desastres Naturales Fuego	[DNF]	[DNF] Desastres Naturales Fuego
3	Desastres Naturales Agua	[DNA]	[DNA] Desastres Naturales Agua
4	Desastres Naturales Terremoto	[DNT]	[DNT] Desastres Naturales Terremoto
5	D Origen Industrial	[DOI]	[DOI] D Origen Industrial
6	D Origen Industrial Avería	[DOIA]	[DOIA] D Origen Industrial Avería
7	D Origen Industrial Corte Suministro	[DOIC]	[DOIC] D Origen Industrial Corte Suministro
8	Errores y Fallos	[ER]	[ER] Errores y Fallos
9	Error de Usuario	[ERU]	[ERU] Error de Usuario
10	Error del Administrador	[ERA]	[ERA] Error del Administrador
11	Ataques	[AT]	[AT] Ataques
12	Ataque robo	[ATR]	[ATR] Ataque robo
13	Virus	[VIR]	[VIR] Virus
14	Ataque manipulación de registros	[ATMR]	[ATMR] Ataque manipulación de registros
15	Ataque destrucción de información	[ATDI]	[ATDI] Ataque destrucción de información
16	Ataque denegación de servicio	[ATDS]	[ATDS] Ataque denegación de servicio

17	Falla servicio de Internet	[FSI]	[FSI] Falla servicio de Internet
18	Falla de comunicaciones	[FCO]	[FCO] Falla de comunicaciones

2.3. Análisis del Riesgo

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia.

Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos.

Tabla de niveles:

Criterios de probabilidad

Que tan probable es que ocurra un evento, para este paso debemos completar el registro de criterios de probabilidad:

TIPOLOGIA	RARO	IMPROBABLE	POSIBLE	PROBABLE	CASI SEGURO
NIVEL	1	2	3	4	5
PROBABILIDAD	<2%	2%-15%	16%-50%	51%-80%	>80%
ESCENARIO DESCRIPTIVO	El evento es posible, y ha ocurrido criterios de probabilidad organización.	El evento ocurrió ciertas veces en la organización	Un evento así ha ocurrido en nuestra organización	Un evento así ha ocurrido en varias ocasiones en la organización.	El evento ocurre frecuentemente en la organización.

Criterios de impacto

Para lo cual debemos identificar 03 aspectos asociados a la empresa. El apetito, el cual es el nivel de riesgo que una empresa está dispuesta a aceptar para alcanzar su misión, la tolerancia, definida por la variación aceptable relativa al apetito de riesgo y por último la capacidad siendo el nivel máximo que una

empresa puede soportar.

APETITO: El nivel de riesgo que una empresa está dispuesta a aceptar expresado en Soles.

TOLERANCIA: Variación aceptable relativa al apetito de riesgo expresado en Soles.

CAPACIDAD : Nivel máximo que una empresa puede soportar expresado en Soles.

TIPOLOGIA	INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTROFICO
NIVEL	1	2	3	4	5
UMBRAL EMPRESA	<S/ 3 K	S/ 3 K- S/ 100 K	S/ 100 K - S/ 500 K	S/ 500 K - S/ 1 MM	> S/ 1 MM
ESCENARIO	El daño no es significativo para la empresa	El daño puede ser asumido por el área responsable	Se deben presentar acciones ante el daño presentado	El daño tiene efectos mayores en la empresa	Perdida catastrófica que pone en riesgo la rentabilidad de la empresa

Análisis del riesgo

ACTIVOS			CRITERIOS				AMENAZA	VULNERABILIDAD	IMPACTO	PROBAB	RIESGO		
Nº	Código	Activo	C	I	D	TOTAL					CÓDIGO	CÓDIGO	NIVEL
1	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	[ERU] Error de Usuario	Escaso conocimiento por parte de los usuarios	1	5	R1	5	BAJO
	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	[ER] Errores y Fallos	Falta de gestión de procesos	2	4	R2	8	BAJO
	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	[FSI] Falla servicio de Internet	No contar con un proveedor externo de internet	2	3	R3	6	BAJO
	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	Abuso de privilegios de acceso	Falta de capacitación y falta de acuerdo de confidencialidad	2	3	R4	6	BAJO
	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	Suplantación de la identidad del usuario	Falta de restricciones y seguridad	3	4	R5	12	MEDIO
	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	Errores de Mantenimiento SW	Falta de Planificación	2	4	R6	8	BAJO
	[S - PROVENTAS]	Proceso de ventas	3	3	3	9	Indisponibilidad del personal	Plan de ejecución de teletrabajo	3	4	R7	12	MEDIO
2	[S - PROOPERACIONES]	Proceso de Operaciones	3	3	3	9	[ERU] Error de Usuario	Escaso conocimiento por parte de los usuarios	2	3	R8	6	BAJO
	[S - PROOPERACIONES]	Proceso de Operaciones	3	3	3	9	[ER] Errores y Fallos	Falta de gestión de procesos	4	4	R9	16	ALTO
	[S - PROOPERACIONES]	Proceso de Operaciones	3	3	3	9	[DOIC] D Origen Industrial Corte Suministro	Falta de equipo de respaldo eléctrico	3	4	R10	12	MEDIO
	[S - PROOPERACIONES]	Proceso de Operaciones	3	3	3	9	Abuso de privilegios de acceso	Falta de capacitación y falta de acuerdo de confidencialidad	3	3	R11	9	BAJO
	[S - PROOPERACIONES]	Proceso de Operaciones	3	3	3	9	Suplantación de la identidad del usuario	Falta de restricciones y seguridad	3	3	R12	9	BAJO
	[S - PROOPERACIONES]	Proceso de Operaciones	3	3	3	9	Indisponibilidad del personal	Falta de contingencia de accesos remotos	4	4	R13	16	ALTO
	[S - PROOPERACIONES]	Proceso de Operaciones	3	3	3	9	Indisponibilidad del personal	Plan de ejecución de teletrabajo	4	4	R14	16	ALTO

	[S - PROOPERACIONES]	Proceso de Operaciones	3	3	3	9	[ERA] Error del Administrador	No contar con permisos adecuados, logs de seguimiento	4	4	R15	16	ALTO
3	[HW - LimCat01]	SW core voz Mpls	3	3	3	9	[DOIC] D Origen Industrial Corte Suministro	Falta de equipos generadores de energia	4	4	R16	16	ALTO
	[HW - LimCat01]	SW core voz Mpls	3	3	3	9	[ER] Errores y Fallos	Falta de personal capacitado	4	4	R17	16	ALTO
	[HW - LimCat01]	SW core voz Mpls	3	3	3	9	[ERA] Error del Administrador	Falta de gestión de procesos	4	3	R18	12	MEDIO
4	[SW - PSXLIMPE01]	Softswitch	3	3	3	9	[DOIC] D Origen Industrial Corte Suministro	Falta de equipo de respaldo eléctrico	4	3	R19	12	MEDIO
	[SW - PSXLIMPE01]	Softswitch	3	3	3	9	[ER] Errores y Fallos	Falta de mantenimiento preventivo	4	3	R20	12	MEDIO
	[SW - PSXLIMPE01]	Softswitch	3	3	3	9	[ERA] Error del Administrador	Falta de gestión de procesos	4	3	R21	12	MEDIO
5	[HW - DSILIMPE03]	Servidor de registro	3	3	3	9	[ER] Errores y Fallos	Falta de mantenimiento preventivo	4	3	R22	12	MEDIO
	[HW - DSILIMPE03]	Servidor de registro	3	3	3	9	[VIR] Virus	Desactualización del antivirus	4	3	R23	12	MEDIO
	[HW - DSILIMPE03]	Servidor de registro	3	3	3	9	[FCO] Falla de comunicaciones	Falta de plan de mantenimiento preventivo	4	4	R24	16	ALTO
6	[HW - NGNLIMPE01]	Servidor de portabilidad	3	3	3	9	[ER] Errores y Fallos	Falta de mantenimiento preventivo	4	3	R25	12	MEDIO
	[HW - NGNLIMPE01]	Servidor de portabilidad	3	3	3	9	[VIR] Virus	Desactualización del antivirus	4	3	R26	12	MEDIO
	[HW - NGNLIMPE01]	Servidor de portabilidad	3	3	3	9	[FCO] Falla de comunicaciones	Falta de plan de mantenimiento preventivo	4	4	R27	16	ALTO
7	[HW - ADS]	Servidor de base de datos	3	3	3	9	[ER] Errores y Fallos	Falta de mantenimiento preventivo	4	3	R28	12	MEDIO
	[HW - ADS]	Servidor de base de datos	3	3	3	9	[VIR] Virus	Desactualización del antivirus	4	3	R29	12	MEDIO
	[HW - ADS]	Servidor de base de datos	3	3	3	9	[FCO] Falla de comunicaciones	Falta de plan de mantenimiento preventivo	4	4	R30	16	ALTO

8	[HW] PC de Ventas - PC_VENTAS	PC de Ventas	2	3	3	8	[VIR] Virus	Desactualización del antivirus	3	3	R31	9	BAJO
	[HW] PC de Ventas - PC_VENTAS	PC de Ventas	2	3	3	8	[ATR] Ataque robo	Falta de seguridad	2	3	R32	6	BAJO
9	[HW - PC_SOPORTE TEC]	PC de Soportetecnico	2	2	2	6	[VIR] Virus	Desactualización del antivirus	3	3	R33	9	BAJO
	[HW - PC_SOPORTE TEC]	PC de Soportetecnico	2	2	2	6	[ATR] Ataque robo	Falta de seguridad	2	3	R34	6	BAJO
10	[HW - PC_CONT]	PC de Contabilidad	2	3	3	8	[VIR] Virus	Desactualización del antivirus	3	3	R35	9	BAJO
	[HW - PC_CONT]	PC de Contabilidad	2	3	3	8	[ATR] Ataque robo	Falta de seguridad	2	3	R36	6	BAJO
11	[HW] PC de Rrhh - PC_RRHH	PC de Rrhh	2	2	3	7	[VIR] Virus	Desactualización del antivirus	3	3	R37	9	BAJO
	[HW] PC de Rrhh - PC_RRHH	PC de Rrhh	2	2	3	7	[ATR] Ataque robo	Falta de seguridad	2	3	R38	6	BAJO
12	[HW - IMP_OPERACIONES]	Impresora de Operaciones	1	2	2	5	[VIR] Virus	Desactualización del antivirus	3	3	R39	9	BAJO
	[HW - IMP_OPERACIONES]	Impresora de Operaciones	1	2	2	5	[ATR] Ataque robo	Falta de seguridad	2	3	R40	6	BAJO

2.4. Valoración del Riesgo

La valoración del riesgo es el proceso de comparación de los resultados del análisis del riesgo con sus criterios para determinar si el riesgo o su magnitud son aceptables o tolerables.

PROBABILIDAD/ FRECUENCIA	5 Frecuente	R1				
	4 Probable		R2, R6	R5, R7, R10	R9, R13, R14, R15, R16, R17, R24, R27, R30	
	3 Ocasional		R3, R4, R8, R32, R34, R36, R38, R40	R11, R12, R31, R33, R35, R37, R39	R18, R19, R20, R21, R22, R23, R25, R26, R28, R29	
	2 Posible					
	1 Improbable					
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5

ETAPA 3: TRATAMIENTO DEL RIESGO

Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Descripción de criterios de Tratamiento del riesgo

Estrategia	Descripción Criterio
Reducir	Se deben evaluar y establecer controles que permitan mitigar el riesgo asociado.
Transferir	La responsabilidad es transferida a un área diferente o, en última instancia, a un tercero.
Aceptar	En este caso, el líder usuario o propietario de la información, acepta el riesgo de seguridad de la información.
Eliminar	En caso sea factible, se identifica la causa del riesgo para establecer medidas que lo eviten e impidan su materialización absoluta.
Escalar	Identificar un riesgo que no afecta a nuestros objetivos, pero que podría afectar a alguna otra parte de la organización.

Tratamiento del riesgo

Nombre del Proyecto	Implementación de plan de Teletrabajo
Estrategia	Mitigar
Riesgo que trata	R7, R3, R14
Nivel de riesgo	Medio, Alto
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]
Objetivo	Mitigar riesgo de plan de teletrabajo, solicitado por el estado post pandemia COVID.

Nombre del Proyecto	Compra de equipo de respaldo eléctrico.
Estrategia	Mitigar
Riesgo que trata	R10, R16, R19
Nivel de riesgo	Medio, Alto
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]

Objetivo	Mitigar problema en los procesos ante Corte de Suministro Eléctrico
-----------------	---

Nombre del Proyecto	Capacitación del personal
Estrategia	Mitigar
Riesgo que trata	R1, R8
Nivel de riesgo	Bajo
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]
Objetivo	Mitigar errores de usuario por falta de transferencia de conocimiento

Nombre del Proyecto	Programa de mantenimientos a equipamiento
Estrategia	Mitigar
Riesgo que trata	R24, R27, R30
Nivel de riesgo	Alto
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]
Objetivo	Mitigar problema de exceso de polvo en el ambiente de trabajo, para dar mayor vida útil a los activos.

ETAPA 4: MONITOREO

El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

En esta etapa nos respondemos si lo que estamos cumpliendo con lo comprometido.

Nombre del Proyecto	Compra de equipo de respaldo eléctrico.
Estrategia	Mitigar
Riesgo que trata	R10, R16, R19
Nivel de riesgo	Medio, Alto
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]
Objetivo	Mitigar problema en los procesos ante Corte de suministro Eléctrico
Responsables	KP (Gerente de Operaciones)
Recursos requeridos	06 UPS
Presupuesto	1,500.00 X 6 = S/9,000.00 soles
Tiempo de ejecución	03 meses.

Nombre del Proyecto	Implementación de plan de Teletrabajo
Estrategia	Mitigar
Riesgo que trata	R7, R3, R14
Nivel de riesgo	Medio, Alto
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]
Objetivo	Mitigar riesgo de plan de teletrabajo, solicitado por el estado post pandemia COVID.
Responsables	KP (Gerente de Operaciones)
Recursos requeridos	asesoría legal, RRHH
Presupuesto	S/ 4000.00
Tiempo de ejecución	6 meses

Nombre del Proyecto	Capacitación del personal
Estrategia	Mitigar
Riesgo que trata	R1, R8
Nivel de riesgo	Bajo
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]
Objetivo	Mitigar errores de usuario por falta de transferencia de conocimiento.
Responsables	KP (Gerente de Operaciones), RRHH
Recursos requeridos	01 personal de Operaciones
Presupuesto	09 horas
Tiempo de ejecución	3 meses

Nombre del Proyecto	Programa de mantenimientos a equipamiento
Estrategia	Mitigar
Riesgo que trata	R24, R27, R30
Nivel de riesgo	Alto
Procesos de Negocio afectados	[S - PROVENTAS], [S - PROOPERACIONES]
Objetivo	Mitigar problema de exceso de polvo en el ambiente de trabajo, para dar mayor vida útil a los activos.
Responsables	Operaciones, Soporte Técnico
Recursos requeridos	01 operaciones, 01 Soporte Técnico
Presupuesto	10 horas
Tiempo de ejecución	2 meses

Anexo 06: Autorización de la empresa

Re: Modelo Gestión de Riesgos de TI - Tesis Daniel Romero

KP Kleiber Palomino Gutierrez <kleiber.palomino@convergia.io>
Para Daniel Alonso Romero Garcia

Responder Responder a todos Reenviar


jueves 26/01/2023 17:16

Estimado Daniel, posterior a la revisión y evaluación del modelo propuesto de Gestión de Riesgo de TI aplicado al servicio de telefonía fija, considera que sería un gran aporte a la empresa su implementación y su extensión a otros servicios y áreas de negocio.
Aprovecho la oportunidad para felicitarte por el buen trabajo desarrollado para tu tesis, de seguro que será de gran aporte a la empresa.

Sin otro particular, me despido.

Saludos,
Kleiber Palomino
Gerente de Operaciones
Convergia Perú
T (511) 640 1036 - (51) 983 447 193
E kleiber.palomino@convergia.io | www.convergia.io
D Calle Los Libertadores 155, Piso 2 - San Isidro, Lima

in f t i



Cloud Connectivity Data & Security Voice



The PanAmerican Connectivity Company

Lima, 08 de junio del 2022

Señores.-

Universidad Católica Santo Toribio De Mogrovejo

Presente.-

Referencia: Maestría en Ingeniería de Sistemas y Computación

De nuestra consideración:

Por medio de la presente, tengo el agrado de dirigirme a ustedes, a fin de informarles sobre la solicitud para la recolección y uso de información de mi representada requerida por vuestro alumno **Daniel Alonso Romero García** para la elaboración del proyecto de tesis, en el programa académico de la referencia, correspondiente a la asignatura **"Investigación e Innovación Tecnológica I"**, el mismo que lleva como título **"Modelo de gestión de riesgos de TI que contribuye a la operación de procesos Core en empresas de telecomunicaciones"**.

Al respecto, a través de la presente misiva le pongo de su conocimiento que mi representada ha autorizado la recolección y uso de la información necesaria de la Compañía para la ejecución del proyecto de tesis señalado en el párrafo anterior.

Sin otro particular, me despido de ustedes, expresándole las muestras de mi mayor consideración.

Atentamente,

CARLOS G. MENDOZA CARRASCO

Gerente General

CONVERGIA PERU S.A.

Carlos Mendoza Carrasco

Gerente General

Convergía Perú S.A.

Anexo 07: Armonización de estándares y modelos.

Para la propuesta del nuestro modelo hemos considerado el modelo de Pardo [1], proceso de armonización que consta de 04 etapas, las cuáles son, homogenización, comparación, análisis porcentual y análisis de resultados.

- **Homogenización:** Consiste en la recopilación de información y una primera vista de comparación.

Para el presente proyecto en esta etapa consideramos lo siguiente:

Tabla II: Homogenización de modelos

Sección	Estereotipos y elementos	ETOM	COBIT 2019	ISO 31000
Sección 1: Descripción (SD)	SD1. Categoría de proceso	x	x	x
	SD2. Procesos	x	x	x
	SD3. Actividades	x	x	x
	SD4. Tareas			x
Sección 2: Roles y Recursos (SRR)	SRR1. Roles	x	x	x
	SRR2. Herramientas			x
Sección 3: Control (SC)	SC1. Artefactos		x	
	SC2. Objetivos	x	x	x
	SC3. Métricas		x	x
Sección 4: Información Adicional (SIA)	SIA1. Procesos relacionados		x	x
	SIA2. Métodos			

▪ **Comparación**

En esta etapa podremos identificar la posible relación entre modelos.

Tabla III: Comparación ISO 31000 / COBIT 2019

ISO 31000 \ COBIT 2019		Evaluar, Dirigir y Monitorizar (EDM)			Alinear, Planificar y Organizar (APO)					
		EDM03 Asegurar la optimización del riesgo			APO12 Gestionar el riesgo					
		EDM03.01 Evaluar la gestión de riesgos	EDM03.02 Dirigir la gestión de riesgos.	EDM03.03 Monitorizar la gestión de riesgos.	APO12.01 Recopilar datos.	APO12.02 Analizar el riesgo.	APO12.03 Mantener un perfil de riesgo.	APO12.04 Articular el riesgo.	APO12.05 Definir un portafolio con acciones de gestión de riesgos.	APO12.06 Responder al riesgo.
6.3	Alcance, contexto y criterios	6.3.2 Definición del alcance	X							
		6.3.3 Contextos externo e interno	X							
		6.3.4 Definición de los criterios del riesgo		x						
6.4	Evaluación del riesgo	6.4.2 Identificación del riesgo			X					
		6.4.3 Análisis del riesgo				X				
		6.4.4 Valoración del riesgo					X	X		
6.5	Tratamiento del riesgo	6.5.2 Selección de las opciones para el tratamiento del riesgo							x	
		6.5.3 Preparación e implementación de los planes de tratamiento del riesgo		X						x

6.6 Seguimiento y revisión

X

6.7 Registro e informe

X

A continuación, se presenta la comparación entre el framework ETOM y COBIT 2019.

Tabla IV: Comparación ETOM/ COBIT 2019

ETOM \ COBIT 2019		Alinear, Planificar y Organizar (APO)						
		APO12 Gestionar el riesgo						
		APO12.01 Recopilar datos.	APO12.02 Analizar el riesgo.	APO12.03 Mantener un perfil de riesgo.	APO12.04 Articular el riesgo.	APO12.05 Definir un portafolio con acciones de gestión de riesgos.	APO12.06 Responder al riesgo.	
1.7.2 Auditoría empresarial y gestión de riesgos	1.7.2.1 Gestión de auditoría empresarial	1.7.2.1.1 Definir política de auditoría		X				
		1.7.2.1.2 Definir el mecanismo de auditoría				X		
		1.7.2.1.3 Evaluar las actividades operativas						
		1.7.2.1.4 Evaluar actividades operativas						
		1.7.2.1.5 Informe de auditorías						
		1.7.2.1.6 Aplicar mecanismos de auditoría de manera proactiva		X			X	
	1.7.2.2 Gestión de riesgos empresariales		1.7.2.2.1.1 Coordinar la continuidad del negocio	X		X		
		1.7.2.2.1 Gestión de la Continuidad del Negocio	1.7.2.2.1.2 Planificar la Continuidad del Negocio				X	X
			1.7.2.2.1.3 Plan de Recuperación de Infraestructura					

		1.7.2.2.1.4 Planificar la Gestión de Incidentes Graves		x
		1.7.2.2.1.5 Administrar Metodologías de Continuidad del Negocio		
		1.7.2.2.2.1 Identificar Riesgos Asegurables		
1.7.2.2.2	Gestión de Seguros	1.7.2.2.2.2 Analizar Costo/Beneficios del Seguro	x	
		1.7.2.2.2.3 Brindar asesoramiento sobre seguros	x	
		1.7.2.2.2.4 Administrar Cartera de Seguros		x

- **Análisis Porcentual entre modelos**

En esta sección se detalla en porcentajes las relaciones entre los modelos analizados descritos en los pasos anteriores

Una vez identificadas las similitudes entre los modelos, determinamos porcentualmente el apoyo de un modelo a otro, para el análisis porcentual debemos considerar la siguiente escala de comparación de acuerdo con Pino [21]:

Tabla V : Tabla de Escala de comparación

ACRONIMO	DESCRIPCION	PORCENTAJE
S	Fuertemente relacionado	(86% a 100%)
L	Relacionado en gran medida	(51% a 85%)
P	Parcialmente relacionado	(16% a 50%)
W	Débilmente relacionado	(1% a 15%)
N	No relacionado	0%

6.5.3 Preparación e implementación de los planes de tratamiento del riesgo	P	P
6.6 Seguimiento y revisión	L	
6.7 Registro e informe		S

El presente cuadro corresponde al análisis porcentual entre el framework ETOM y COBIT 2019.

Tabla VII: Análisis porcentual ETOM / COBIT 2019

ETOM \ COBIT 2019		Evaluar, Dirigir y Monitorizar (EDM)			Alinear, Planificar y Organizar (APO)						
		EDM03 Asegurar la optimización del riesgo			APO12 Gestionar el riesgo						
		EDM03.01	EDM03.02	EDM03.03	APO12.01	APO12.02	APO12.03	APO12.04	APO12.05	APO12.06	
		Evaluar la gestión de riesgos	Dirigir la gestión de riesgos.	Monitorizar la gestión de riesgos.	Recopilar datos.	Analizar el riesgo.	Mantener un perfil de riesgo.	Articular el riesgo.	Definir un portafolio de acciones de gestión de riesgos.	Responder de al riesgo.	
1.7.2 Auditoría empresarial y gestión de riesgos	1.7.2.1 Gestión de auditoría empresarial	1.7.2.1.1 Definir política de auditoría				P					
		1.7.2.1.2 Definir el mecanismo de auditoría						P			
		1.7.2.1.3 Evaluar las actividades operativas									
		1.7.2.1.4 Evaluar actividades operativas									
		1.7.2.1.5 Informe de auditorías									
		1.7.2.1.6 Aplicar mecanismos de auditoría de manera proactiva					W			P	
	1.7.2.2 Gestión del Negocio	1.7.2.2.1 Gestión de la Continuidad del Negocio	1.7.2.2.1.1 Coordinar la continuidad del negocio	L		P		L			

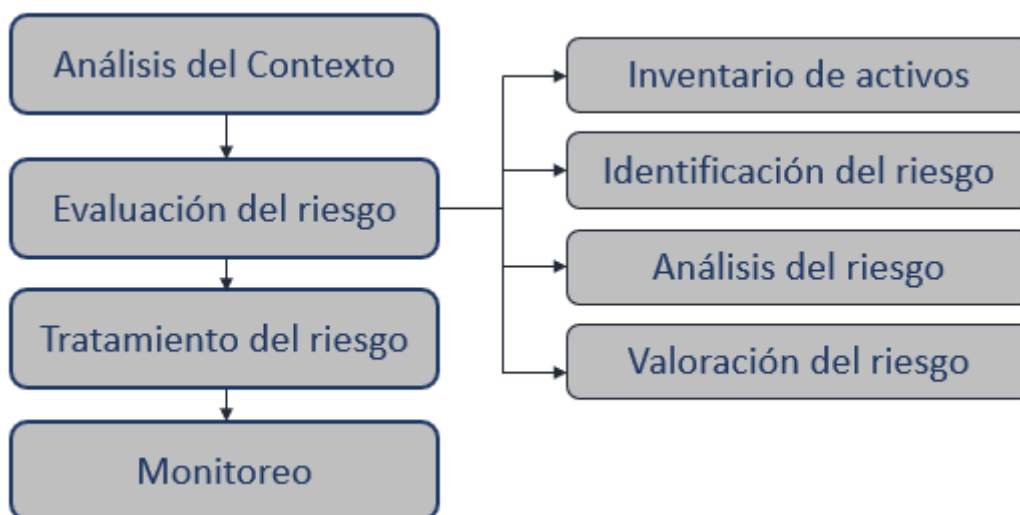
	1.7.2.2.1.2 Planificar la Continuidad del Negocio		P	L
	1.7.2.2.1.3 Plan de Recuperación de Infraestructura			L
	1.7.2.2.1.4 Planificar la Gestión de Incidentes Graves		L	
	1.7.2.2.1.5 Administrar Metodologías de Continuidad del Negocio			
1.7.2.2.2 Gestión de Seguros	1.7.2.2.2.1 Identificar Riesgos Asegurables	L		
	1.7.2.2.2.2 Analizar Costo/Beneficios del Seguro		W	
	1.7.2.2.2.3 Brindar asesoramiento sobre seguros		W	
	1.7.2.2.2.4 Administrar Cartera de Seguros			W

- **Análisis de resultados**

Posterior al cumplimiento de las etapas del proceso de armonización podemos validar que la norma ISO 31000:2018 y COBIT 2019 cuentan con mucha similitud en relación fases y actividades, por lo que consideraremos a la norma ISO 31000:2018 como eje principal de nuestra metodología, apoyado con actividades de COBIT 2019, considerar también que el framework ETOM apoyara con algunos lineamientos asociados a la visión del negocio.

El resultado es el que se muestra a continuación:

Ilustración 8 : Modelo de Gestión de riesgos de TI propuesto



Fuente: Elaboración Propia

Anexo 08: Alfa de Cronbach y concordancia de Kendall

- Para la validación del modelo propuesto se empleó tres instrumentos:

Primero el **juicio de expertos** según Escobar - Cuervo[22], por lo que 3 profesionales expertos analizaron y evaluaron las etapas e ítems del modelo propuesto, obteniendo la aprobación de este. Para más información ver el [anexo 02](#).

Segundo, para medir el nivel de confiabilidad del modelo, se procesaron los resultados proporcionados por los profesionales expertos aplicando **alfa de Cronbach**, obteniendo un nivel de 0.93% de confiabilidad como se detalla a continuación:

Tabla VIII: Estadística de Confiabilidad

Estadística de confiabilidad	
Coficiente de confiabilidad	0.93
Ítems del instrumento	12
Σ de las varianzas de los ítems.	0.944
Varianza total del instrumento.	6.431

Tabla IX: Nivel de Confiabilidad

RANGO	CONFIABILIDAD
0.53 a menos	Confiabilidad nula
0.54 a 0.59	Confiabilidad baja
0.60 a 0.65	Confiable
0.66 a 0.71	Muy confiable
0.72 a 0.99	Excelente confiabilidad

Validando el resultado en nuestra tabla de niveles, obtenemos que el modelo consta de **Excelente confiabilidad**, con un valor de **0.93**.

Tercero, **Coefficiente de Concordancia W de Kendall**; según Escobar – Cuervo[22], este coeficiente es usado para descubrir el grado de asociación entre un grupo de rangos. Teniendo como hipótesis H0 en el caso de no tener coincidencia de rangos y H1 en caso de tener una coincidencia relevante.

En la siguiente grafica visualizamos los resultados obtenidos, de acuerdo software estadístico informático SPSS:

N	3
W de Kendall ^a	.333
Chi-cuadrado	3.000
gl	3
Sig. asin.	.392

a. Coeficiente de concordancia de Kendall

Figura 7: Resultado de W Kendall

Finalmente, y posterior a la evaluación concluimos que el modelo propuesto tiene un nivel aceptable demostrando la concordancia con relación a las respuestas de los 3 expertos.