UNIVERSIDAD HISPANOAMERICANA

ESCUELA DE INGENIERÍA INFORMÁTICA

TESIS PARA OPTAR EL GRADO DE LICENCIATURA EN INGENIERÍA INFORMÁTICA CON ÉNFASIS EN SISTEMAS DE INFORMACIÓN

PLAN DE CONTINUIDAD DEL NEGOCIO CON ÉNFASIS EN ÁREA TECNOLÓGICA PARA UNA INSTITUCIÓN EDUCATIVA, EL CENTRO DE ESTUDIOS Y CAPACITACIÓN COOPERATIVA, CENECOOP R.L.

Sustentante:
Fabián Alonso Soto Bogantes

Tutor:
Cynthia López Valerio

Noviembre, 2019

ÍNDICES

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

DECLARACIÓN JURADA

DECLARACIÓN JURADA

Yo Fabián Alonso Soto Bogantes, mayor de edad, portador de la cédula de identidad número 3-0482-0487 egresado de la carrera de Ingeniería Informática de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Ingeniería Informática con Énfasis en Sistemas de Información, juro solemnemente que mi trabajo de investigación titulado: Plan de Continuidad del Negocio con Énfasis en Área Tecnológica para una Institución Educativa, El Centro de Estudios y Capacitación Cooperativa, CENECOOP R.L, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los veintiocho días del mes de agosto del año dos mil veinte.

Fabián Alonso Soto Bogantes
Cédula: 3-0482-0487

CARTA DE APROBACIÓN DEL TUTOR, LECTOR Y DE LOS AUTORES PARA CONSULTA

CARTA DEL TUTOR

CARTA DEL TUTOR

San José, 27 de agosto de 2020

Sra. María Isabel Losilla Barrientos
Ingeniería Informática
Universidad Hispanoamericana

Estimado señor:

El estudiante Fabián Alonso Soto Bogantes, cédula de identidad número 3-0482-0487, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado: Plan de Continuidad del Negocio con Énfasis en Área Tecnológica para una Institución Educativa, El Centro de Estudios y Capacitación Cooperativa, CENECOOP R.L el cual ha elaborado para optar por el grado académico de Licenciatura en Ingeniería Informática con Énfasis en Sistemas de Información.
En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	10%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20%
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	30%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	20%
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	20%
	TOTAL		100%

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

CYNTHIA LOPEZ VALERIO (FIRMA)
Firmado digitalmente por CYNTHIA LOPEZ VALERIO (FIRMA)
Fecha: 2020.08.27 08:41:42 -06'00'

Ing. Cynthia López Valerio; Msc
Cédula identidad 1-0970-0997
Carné Colegio Profesional 1445

CARTA DEL LECTOR

CARTA DE LECTOR

San José,

Universidad Hispanoamericana
Sede Llorente
Carrera de Informatica

Estimado señor

El estudiante Fabián Alonso Soto Bogantes, cédula de identidad **3-0482-0487**, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado " Plan De Continuidad Del Negocio Con Énfasis En Área Tecnológica Para Una Institución Educativa, El Centro De Estudios Y Capacitación Cooperativa, Cenecoop R.L.", el cual ha elaborado para obtener su grado de Licenciatura En Ingeniería Informática Con Énfasis En Sistemas De Información.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. He verificado que se han hecho las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.
Atte.

Randall Vargas V
Firma
Randall Vargas Villalobos
Cédula: 1-1140-0113

CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 07 de octubre de 2020

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Fabián Alonso Soto Bogantes con número de identificación 3-0482-0487 autor (a) del trabajo de graduación titulado Plan de Continuidad del Negocio con Énfasis en Área Tecnológica para una Institución Educativa, El Centro de Estudios y Capacitación Cooperativa, CENECOOP R.L presentado y aprobado en el año 2020 como requisito para optar por el título de Licenciatura en Ingeniería Informática con énfasis en Sistemas de Información; SI autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

Cédula: 3-0482-0487

_____
Firma y Documento de Identidad

XX

ANEXO 1 (Versión en línea dentro del Repositorio)
LICENCIA Y AUTORIZACIÓN DE LOS AUTORES PARA PUBLICAR Y PERMITIR LA CONSULTA Y USO

Parte 1. Términos de la licencia general para publicación de obras en el repositorio institucional

Como titular del derecho de autor, confiero al Centro de Información Tecnológico (CENIT) una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, el autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito.

b) Autoriza al Centro de Información Tecnológico (CENIT) a publicar la obra en digital, los usuarios puedan consultar el contenido de su Trabajo Final de Graduación en la página Web de la Biblioteca Digital de la Universidad Hispanoamericana

c) Los autores aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) Los autores manifiestan que se trata de una obra original sobre la que tienen los derechos que autorizan y que son ellos quienes asumen total responsabilidad por el contenido de su obra ante el Centro de Información Tecnológico (CENIT) y ante terceros. En todo caso el Centro de Información Tecnológico (CENIT) se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

e) Autorizo al Centro de Información Tecnológica (CENIT) para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

f) Acepto que el Centro de Información Tecnológico (CENIT) pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

g) Autorizo que la obra sea puesta a disposición de la comunidad universitaria en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en las “Condiciones de uso de estricto cumplimiento” de los recursos publicados en Repositorio Institucional.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DEL CENTRO DE INFORMACIÓN TECNOLÓGICO (CENIT), EL AUTOR GARANTIZA QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.

DEDICATORIA

DEDICATORIA

A Dios porque siempre guía mis pasos, pensamientos y por las bendiciones que me ha dado, una de esas es mi familia quien siempre ha estado presente en cada momento de mi vida.

Dedico mi tesis a mis padres y hermana, quienes me motivaron para que concluya este trabajo pendiente y culminar exitosamente uno de los objetivos más importantes de mi vida profesional y personal, por ser el pilar más importante de mi existencia y demostrarme siempre su cariño y apoyo incondicional pese a las diferencias de opiniones.

AGRADECIMIENTO

AGRADECIMIENTO

Agradezco primeramente a Dios y a la Virgen por permitirme llegar hasta donde he llegado, porque hiciste realidad mi sueño anhelado y me dio la fortaleza durante toda esta etapa de mi vida.

Le agradezco profundamente a la Universidad Hispanoamericana, por darme la oportunidad de estudiar y ser el profesional que soy gracias a la calidad de sus docentes, además un especial reconocimiento a la tutora Cynthia López Valerio por su aporte en conocimientos y correcciones. Por último y no menos importante a todas aquellas personas que contribuyeron con el desarrollo de la investigación de una u otra manera.

ABREVIATURAS

ABREVIATURAS

BCI = Business Continuity Institute.

BCM = Business Continuity Management.

BCP = Business Continuity Plan.

BIA = Business Impact Analysis.

CAR = Capability Assessment for Readiness.

CGR = Contraloría General de la República.

COBIT = Control Objetives for Information Systems.

DRII = Disaster Recovery Institute Internacional.

DRP = Disaster Recovery Planning.

FEMA = Federal Emergency Management Agency.

FODA = Fortalezas, Oportunidades, Debilidades, Amenazas.

GPG = Good Practice Guidelines.

ICE = Instituto Costarricense de Electricidad.

IEC = InterExchange Carrier.

IGI = Índice de Gestión Institucional.

INTECO = Instituto de Normas Técnicas de Costa Rica.

ISACA = Information Systems Audit and Control Association.

ISO = International Organization for Standardization.

ISP = Internet Service Provider.

IyD = Investigación y Desarrollo.

MTD = Maximum Tolerable Downtime.

MTPOD = Maximum Tolerable Period Of Down time.

NFPA = National Fire Protection Association.

NTE = Normas Tecnológicas de Edificación.

PESTEL = Político, Económico, Sociocultural, Tecnológico, Económico, Legal.

PHVA = Plan, Do, Check, Act.

RPO = Recovery Point Objective.

RTO = Recovery Time Objective.

SGCI = Information Security Management System

SGCN = Business Continuity Management System.

S.O = Sistema Operativo.

SQL = Structured Query Language.

TI = Tecnología de la Información.

UPS = Uninterruptible Power Supply.

VPN = Virtual Private Network.

XSS = Cross Site Scripting.

RESUMEN

RESUMEN

El Centro de Estudios y Capacitación Cooperativa R.L (CENECOOP R.L.) es una empresa que se fundó en 1982, dedicada plenamente al cooperativismo, lo cual busca una solución de capacitación a todas los empleados de cooperativas de Costa Rica, actualmente la institución cuenta con cinco asociadas a lo largo del territorio nacional, estás empresas relacionadas son: Hotel del Sur, Formadores de Empresarios y Líderes de la Economía Social La Catalina R.L, Grupo Empresarial Cooperativo de Servicios Educativos R.L, Universidad Fundepos Alma Mater, Campamento Oikoumene y Hotel Palmar Sur.

El presente proyecto tiene como objetivo principal proponer un plan de continuidad del negocio para el departamento de Tecnología de la Información (TI) en CENECOOP R.L, con la finalidad de dotar a la empresa una herramienta que al ser implementada pueda atacar directamente a los incidentes que se presente de forma inesperada y pongan en riesgo la continuidad del negocio.

Para evaluar el contexto actual se realiza un diagnóstico de la situación actual en general para toda la organización y para el departamento de TI, así como el levantamiento de información, infraestructura técnica y aplicaciones, se aplican estándares internacionales que proporcionan ventajas no solo a la empresa sino también a los empleados y clientes.

Posteriormente se analizan todos los riesgos con diferentes herramientas de medición y se concluye que todos son considerados como críticos para poder mantener la continuidad, además que los servicios del departamento de TI son los que más impactan directamente a demás áreas de la empresa según las entrevistas realizadas a las jefaturas de la empresa.

Se plantea una propuesta de continuidad del negocio, donde se pueda aplicar como un modelo a seguir; dicha propuesta señala y definen los respectivos pasos a seguir para que la cooperativa tenga las bases necesarias para responder ante una determinada amenaza; se crean plantillas para los mantenimientos que en este tipo de plan es trascendental este tema, permitiendo así minimizar el impacto generado para cada uno de los riesgos.

CAPÍTULO I
PROBLEMA DEL PROYECTO

1.1 Antecedentes y justificación del proyecto

1.2 Marco de referencia empresarial y contextual

En las últimas décadas, con la globalización económica en marcha, el desarrollo de las nuevas tecnologías de la información y los retos de eficiencia empresarial, que se plantean a consecuencia de estos procesos, el CENECOOP R.L., ha venido adecuando sus planes de estudio para facilitar a los productores y productoras actuales, así como a las nuevas generaciones de cooperativistas, una amplia capacitación en el campo de la tecnología, así como en la administración y gestión de negocios.

El Centro de Estudios y Capacitación Cooperativa, CENECOOP R.L, nace en 1982, como un organismo auxiliar cooperativo sin fines de lucro, dedicado y comprometido con la educación, capacitación y actualización del movimiento cooperativo nacional, con el propósito de fortalecer su capacidad competitiva, en consonancia con los principios y valores cooperativos.

En el estatuto integral de 1988 destacan, entre sus objetivos: la educación del campo cooperativo y la capacitación de sus dirigentes, funcionarios y asociados; la realización de estudios e investigaciones sobre diferentes aspectos de la educación, formación y capacitación cooperativa; la gestión de políticas y la consecución de recursos, así como la vinculación con entidades y organismos representativos y sistemas afines al ideario cooperativo a nivel nacional e internacional.

1.2.1 Misión de la empresa

Educar y capacitar para el desarrollo del recurso humano de las empresas cooperativas, con el propósito de fortalecer su capacidad competitiva, en concordancia con los principios y valores cooperativos.

1.2.2 Visión de la empresa

Ser una institución cooperativa en la educación, capacitación, investigación, divulgación del modelo cooperativo y transferencia tecnológica del Movimiento Cooperativo Nacional, con amplia participación de la base cooperativa, comprometida con la calidad en el servicio y la mejora continua en las técnicas de capacitación.

1.2.3 **Valores**

- ✓ Innovación.
- ✓ Calidad.
- ✓ Mejora continua.
- ✓ Aprendizaje.
- ✓ Equidad.
- ✓ Transparencia.

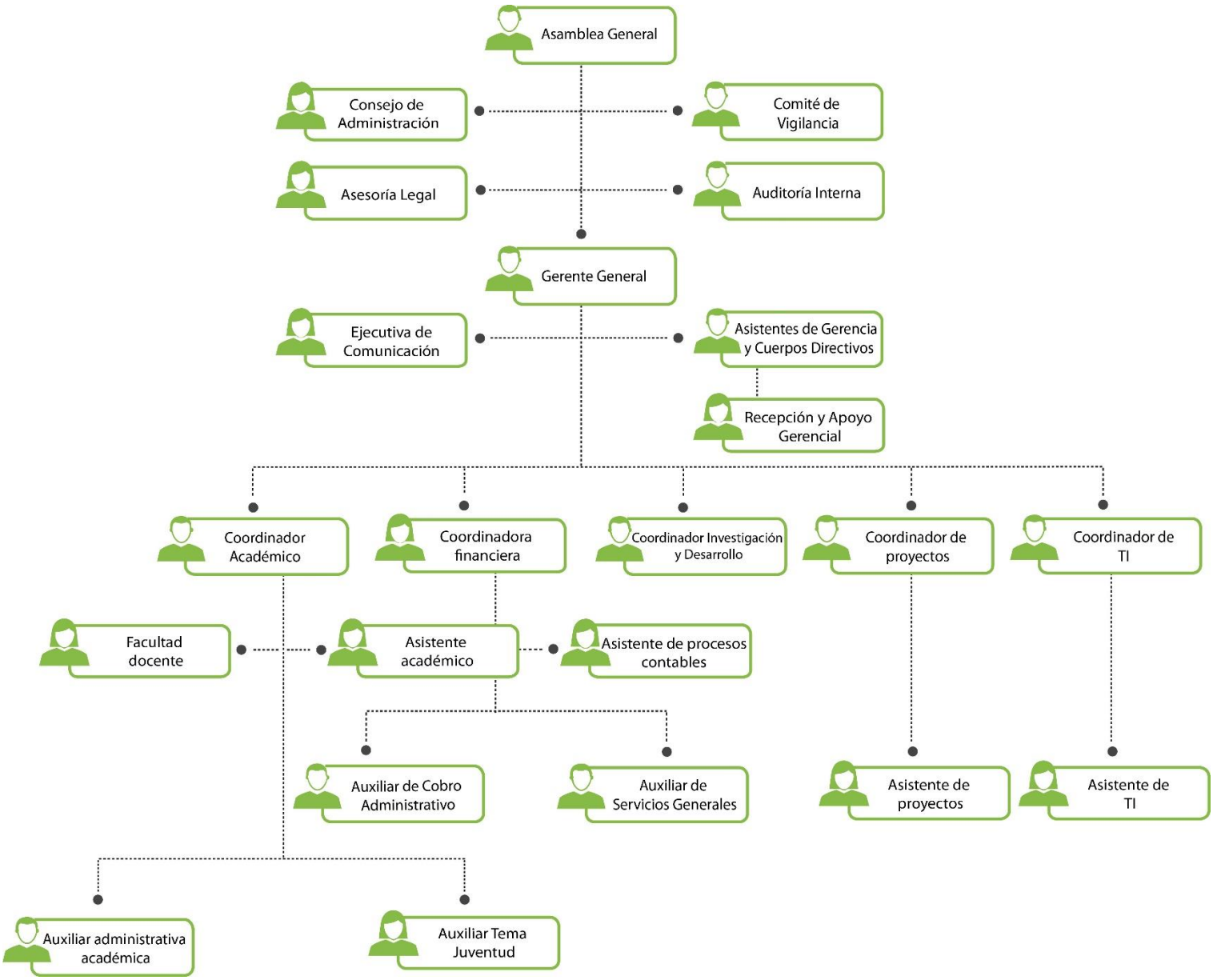
1.2.4 **Estructura organizacional**

El organigrama cuenta con tres divisiones claras, Cuerpos Directivos, Gerencia y Áreas. La alta dirección se compone por una Asamblea General, que es la máxima autoridad, seguidamente del Consejo de Administración, que se encarga de tomar las decisiones de la organización en compañía del Comité de Vigilancia, organismo a cargo de dar sugerencias, posteriormente por la Auditoría Interna como una dependencia del Consejo de Administración y la Asesoría Legal.

La Gerencia General se compone de dos áreas de soporte; Asistente de Gerencia y Ejecutiva de Comunicaciones y Relaciones Públicas, de la mano con áreas funcionales como Coordinación Académica, Coordinación Administrativa Financiera, Coordinador de Investigación y Desarrollo, Coordinador de Gestión de Desarrollo Humano, Coordinador de TI y Coordinación de Proyectos, seguido de áreas operativas.

La estructura organizacional de CENECOOP R.L. se encuentra claramente identificada y se detalla en la figura 1.

Figura 1 – Organigrama CENECOOP R.L.



Fuente: Salazar, A. (2019). Organigrama de CENECOOP R.L. Recuperado de: **https://www.cene.coop/organigrama/**

1.3 Justificación del proyecto

Hoy en día las compañías se enfrentan a varios retos tecnológicos que deben afrontar para poder permanecer en el mercado, la continuidad del negocio es uno de ellos, mantenerse operando a pesar de las eventualidades que puedan presentarse es de gran importancia para seguir compitiendo en el mercado. Además, por su parte, los estudiantes en la actualidad se vuelven más exigentes con los servicios educativos recibidos, aumentando la presión de las instituciones formativas del sector privado en Costa Rica, al ser las responsables de una función tan importante como es la formación académica. Actualmente son muchas las empresas que fracasan o incluso desaparecen por la falta de procesos, mecanismos o técnicas que disminuyan los riesgos a los que se exponen y de esta manera garanticen una alta disponibilidad en las operaciones (servicios) del negocio. Un análisis realizado por Gamer (Roberta Witty, Donna Scott, 2001), en el estudio Disaster Recovery Plans and Systems are Essential, aseguran que dos de cada cinco empresas que han experimentado un desastre quedan fuera del negocio en los siguientes cinco años, situación que podría perjudicar considerablemente el proceso operativo y productivo de CENECOOP R.L.

En esta categoría se encuentra actualmente CENECOOP R.L. entidad que está creciendo constantemente, atrayendo a gran cantidad de clientes importantes que requieren de sus servicios en un 100%. Un ejemplo de ello; es que en la actualidad la empresa cuenta con una plataforma e-learning que necesita estar las 24 horas del día y los 365 días del año en funcionamiento constante, además de todo el equipo que se encuentra en aulas y laboratorios, empleados que obligan a que sus equipos estén conectados para la formación educativa a diferentes cooperativas, de lo contrario significaría una pérdida de clientes importante, obligando que la compañía no puede seguir sin los mecanismos necesarios para hacer frente a una eventual amenaza que ponga en riesgo la continuidad del negocio.

Cabe destacar que la utilización de las Normas Internacionales genera un desempeño trascendental a la investigación, una de ellas es la denominada ISO 22301:2012, que establece cómo identificar las amenazas potenciales de una organización y los impactos en las operaciones del negocio, a fin de contar con capacidad de respuesta para salvaguardar sus intereses. Además, explica las fases del Plan de Continuidad del Negocio (BCP) como: descripción del negocio y análisis de riesgos, estrategias o mitigación del riesgo, desarrollo de implantación del plan y mantenimiento del plan (ISO, 2012).

Otra aplicación realmente importante en este mismo ámbito, es el marco de trabajo para el gobierno de TI, desarrollado por la Information Systems Audit and Control Association (ISACA), denominado COBIT 5, que tiene por objeto organizar y optimizar los estándares internacionales relacionados con la tecnología de la información en las organizaciones, presentando un conjunto de prácticas enfocadas al control, con base en criterios de calidad, confianza y seguridad. COBIT 5 se fundamenta en cinco principios notables: satisfacer las necesidades de las partes interesadas, cubrir la empresa de extremo a extremo, aplicar un marco de referencia único integrado, hacer posible un enfoque global y separar el gobierno de la gestión (ISACA, 2012).

Asimismo, la guía elaborada por el Business Continuity Institute (BCI), denominada Good Practice Guidelines (GPG), que en español se traduce como: buenas prácticas para la continuidad del negocio, explica el cómo y el porqué de los principios de la disciplina de continuidad del negocio, incluyendo la terminología de la norma ISO 22301, para asegurar los más altos estándares en su ejecución. Está integrada por seis secciones: el ciclo de vida de la gestión de continuidad del negocio (BCM) y programa de administración, entendimiento de la organización, determinando la estrategia de continuidad del negocio, desarrollo e implementación de responsabilidades, probar, dar mantenimiento y revisión del programa de continuidad del negocio y desarrollando una cultura de secuencia en la organización (BCI, 2013).

En nuestro país la Contraloría General de la República (CGR) es el ente que regula y exige que las diferentes entidades, cuenten con algún tipo de sistema tecnológico seguro, garantizando así la continuidad del servicio en sus operaciones; y es que según el Índice de Gestión Institucional (IGI) de la CGR la Cooperativa en el año 2018 no presentó ningún porcentaje en temas tecnológicos, es por esta razón que se desea dar una reestructuración en ese ámbito, satisfacer la necesidad de seguridad y continuidad frente a riesgos técnicos, mediante la recopilación de las mejores prácticas o referentes para la confección de un Plan de Continuidad del Negocio (BCP), que permita generar una propuesta para la empresa en el sector educativo de Costa Rica.

De manera que, la presente investigación plantea una propuesta de BCP para una institución educativa del sector privado de Costa Rica, que permita una recuperación ágil y ordenada frente a cualquier incidente e interrupción que amenace su normal funcionamiento; garantizando así la calidad del servicio y rentabilidad de la empresa. Es por este motivo que se plantea un plan de

continuidad del negocio, el cual pueda ser implementado logrando obtener algún tipo de mecanismo de defensa que pueda poner en riesgo la operación de CENECOOP R.L.

1.4 Definición del proyecto

1.4.1 Problemática

Las oficinas del Centro de Estudios y Capacitación Cooperativa, al estar ubicadas en San Pedro de Montes de Oca, presenta amenazas en su geografía, por ser un punto de constantes inundaciones y otros altercados, provocando un aumento en el índice de riesgo local, por lo que es necesario elaborar un plan de continuidad del negocio para proseguir con las actividades de la organización, así, se logrará minimizar el impacto que pueda generar interrupciones imprevistas en las funciones cotidianas que puedan perjudicar el servicio brindado.

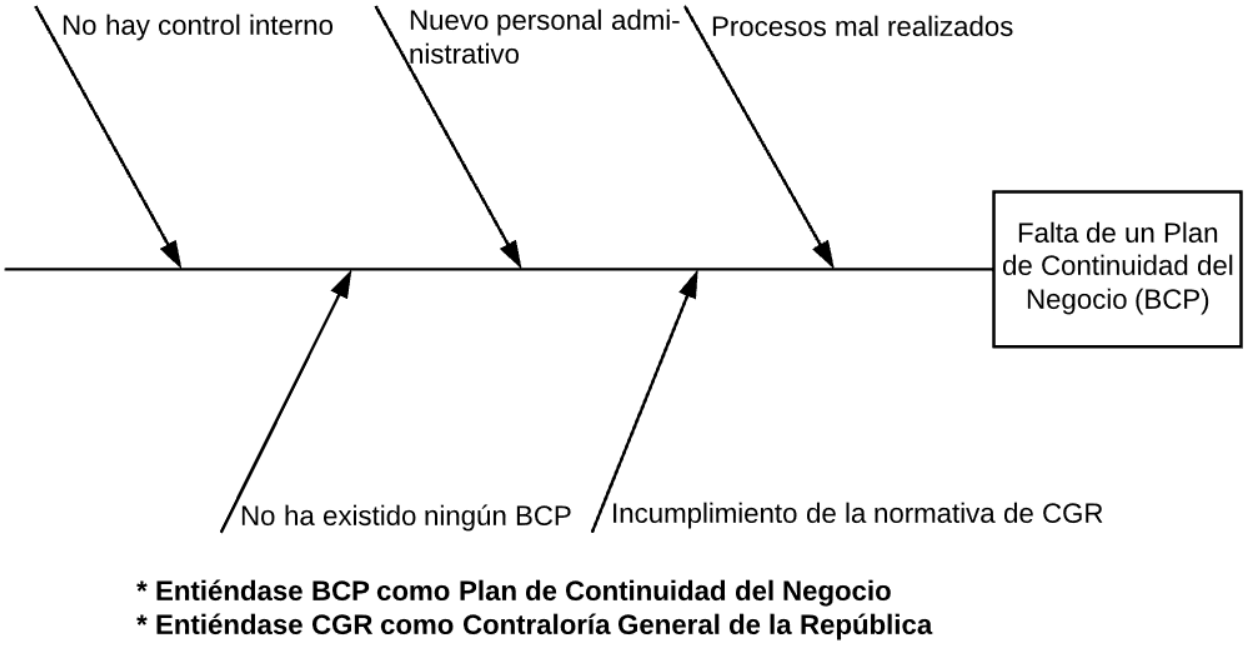
De esta manera, se logrará mantener una imagen sólida que pueda hacer frente a catástrofes y contar con una recuperación eficaz para satisfacer las necesidades de los clientes.

Las funciones que brinda el CENECOOP R.L., se han vuelto necesarias para los clientes que desean mantener una excelente operatividad en los servicios, no obstante, la entidad ha presentado bajas en su cartelera de clientes, ya que en el año 2019 tuvo una disminución de 12.000 personas en capacitación virtual, lo que equivale a un 55% de los clientes; en comparación a lo registrado en el 2018.

Es importante recalcar que la pérdida e insatisfacción de clientes debilitan enormemente las operaciones del CENECOOP R.L., dado que si los clientes continúan eligiendo a la competencia en temas educativos, las operaciones se verán afectadas poniendo en riesgo la continuidad del negocio.

1.4.2 Diagrama causa – efecto

Figura 2 – Diagrama causa - efecto



Fuente: elaboración propia.

1.5 Problema general

¿Cómo diseñar un Plan de Continuidad del Negocio (BCP) para el área de Tecnología de Información (TI) en el Centro de Estudios y Capacitación Cooperativa (CENECOOP R.L.) basado tanto en un análisis de riesgos como desastres y aplicando las normas técnicas para la Gestión y estándares internacionales para el plan de contingencia de TI?

1.6 Problemas específicos

1. ¿Cómo realizar un diagnóstico de la situación actual (prevención de desastres y análisis de riesgos) referente al Plan de Continuidad del Negocio (BCP)?
2. ¿Cuáles son las mejores prácticas para gestionar el Plan de Continuidad del Negocio a través de normativas internacionales relacionadas en este ámbito?
3. ¿Cómo desarrollar un plan de acción con las normativas técnicas que más se ajusten para implementar el BCP en el CENECOOP R.L.?

1.7 Objetivos

1.7.1 Objetivo general

- ✓ Desarrollar un plan de continuidad del negocio para el Centro de Estudios y Capacitación Cooperativa CENECOOP R.L, que tiene como finalidad la protección y seguridad de los activos de la empresa; como el recurso humano y la permanencia de sus clientes potenciales a través de procedimientos fundamentales: ISO 22301:2012, Norma NFPA 1600, COBIT 5 y Good Practice Guidelines (GPG).

1.7.2 Objetivos específicos

1. Analizar la situación actual, vulnerabilidades, período de recuperación y tiempo máximo de interrupción, presentes en la situación actual de la empresa CENECOOP R.L. en materia del plan de continuidad del negocio, mediante los análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas); PESTEL (Político, Económico, Socio-cultural, Tecnológico, Ecológico y Legal) y matrices para la determinación de los riesgos.
2. Definir los servicios críticos del Centro de Estudios que no pueden ser interrumpidos para mantener la continuidad del negocio con la aplicación de la ISO 22301:2012 (Norma Internacional para la Gestión de la Continuidad de Negocio) y Good Practice Guidelines (GPG) apartado de la norma ISO.
3. Desarrollar la propuesta del plan de continuidad del negocio, con las mejores prácticas para adaptarlos a la compañía CENECOOP R.L con la implementación de la norma NFPA 1600 y COBIT 5.

1.8 Alcance y limitaciones

1.8.1 Alcance del proyecto

a) Entregar un diagnóstico de la situación actual del departamento de informática de CENECOP R.L., a través de análisis FODA, PESTEL y entrevistas con las jefaturas de las áreas de informática e investigación y desarrollo; que permitan identificar claramente las necesidades de mejoras al diseñar el plan de continuidad del negocio.

b) Identificar las amenazas, prevención de desastres y análisis de riesgos más críticos del Centro de Estudios que impidan la operación y continuidad de la empresa mediante: la

norma ISO 22301:2012, matrices de riesgos definido en la Norma Australiana, matriz de riesgos para proyectos, matriz comparativa y semáforo de riesgos.

c) Formular un plan de continuidad del negocio adaptado para la institución educativa CENECOOP R.L., recopilando las mejores prácticas que vayan de la mano con el COBIT 5 y la Norma NFPA 1600.

1.8.2 Limitaciones del proyecto

Las presentes limitaciones restringirán la investigación:

i. **Falta de instrumentos disponibles:** en CENECOOP R.L. no se cuenta con ningún tipo de inventario actualizado del equipo físico ni su equipo virtual (servidores en la nube, licenciamiento y software).
ii. **Información confidencial:** tras utilizar información organizacional la empresa revisará previamente el proyecto final y podría limitar la publicación de información que considere pueda atentar con su integridad o permanencia en el mercado.
iii. **Cambios en Asamblea General:** el plan de continuidad del negocio se desarrollará con la información que el Centro de Estudios proporcione al momento de iniciar el proyecto, considerando que puede haber cambios tanto en el Consejo de Administración como en el Comité de Vigilancia.

Observaciones adicionales

Se trabajará en el proyecto con el apoyo de dos personas del Centro de Estudios y Capacitación Cooperativa, el coordinador de Tecnologías de Información y el coordinador de Investigación y Desarrollo.

CAPITULO II
MARCO TEÓRICO

2.1 **Definición de plan**

Se entenderá el concepto de plan como un conjunto de pasos a realizar para lograr alcanzar un objetivo. Cuando se realiza un plan deben definirse los alcances, se deben establecer las metas y el tiempo de la ejecución. (Rodríguez, 2005).

2.2 **Plan de continuidad**

Un plan de continuidad es donde la organización puede obtener los pasos por seguir la interrupción de sus labores.

Un plan de continuidad, también conocido por sus siglas en inglés (BCP = Business Continuity Plan) es un conjunto de procedimientos alternativos a la forma tradicional de operar de la empresa o institución y constituye una herramienta que ayuda a que los procesos considerados como críticos para la organización continúen funcionando en una situación de desastre, aún cuando este sea incontrolable en el entorno. (Juárez, 2011).

La continuidad de los servicios en el área de tecnología de información es fundamental para prevenir la interrupción de los procesos claves en las organizaciones. IT Governance Institute (2007) afirma: "Asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI" (p. 113), lo cual respalda que la implementación de un plan de continuidad mitiga los riesgos y, a su vez, disminuye las pérdidas. Para desarrollar e implementar un plan de continuidad de negocios, es necesario investigar conceptos y teorías que respalden los procesos que se ejecutan. En los marcos de trabajo y la norma ISO 22301, se puede adquirir conocimiento vital para efectuar los procesos requeridos y estos son las guías por seguir para asegurar que se realiza conforme lo indican los estándares y las mejores prácticas.

2.3 **Marco de trabajo**

El marco de trabajo en COBIT 5 es una herramienta que se encarga de orientar y aclarar la situación de la empresa. "Un marco de control para el gobierno TI define las razones de por qué se necesita el Gobierno de TI, los interesados y qué se necesita cumplir en el gobierno de TI" (IT Governance Institute, 2007).

Con la ayuda del marco de trabajo, se puede visualizar de forma transparente la situación de la organización en cuanto a riesgos y esto permite distinguir las áreas vulnerables en las que se deben aplicar mejoras en el departamento de tecnología de información del Centro de Estudios y

Capacitación Cooperativa, además se debe conocer la teoría del porqué se debe efectuar un plan de continuidad en las organizaciones basándose en un marco de trabajo.

Cada vez más, los altos mandos de la organización se están dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa y no es más considerado como el activo más importante de la empresa. La dirección espera un alto entendimiento de la manera en que la tecnología de información (TI) es operada y de la posibilidad que sea aprovechada con éxito para tener una ventaja competitiva (IT Governance Institute, 2007).

2.4 **Definición de COBIT**

Cobit es un marco de trabajo que guía a la organización a alinear los objetivos de la empresa con el área de tecnología de información, es desarrollado por la Information Systems and Control Association (ISACA), tiene por objeto organizar y optimizar los estándares internacionales relacionados con la tecnología de la información en las organizaciones. Presenta un conjunto de prácticas enfocadas al control, con base en criterios de calidad, confianza y seguridad. COBIT 5 se fundamenta en cinco principios (ISACA, 2012):

- ✓ Satisfacer las necesidades de las partes interesadas.
- ✓ Cubrir la empresa de extremo a extremo.
- ✓ Aplicar un marco de referencia único integrado.
- ✓ Hacer posible un enfoque holístico.
- ✓ Separar el gobierno de la gestión.

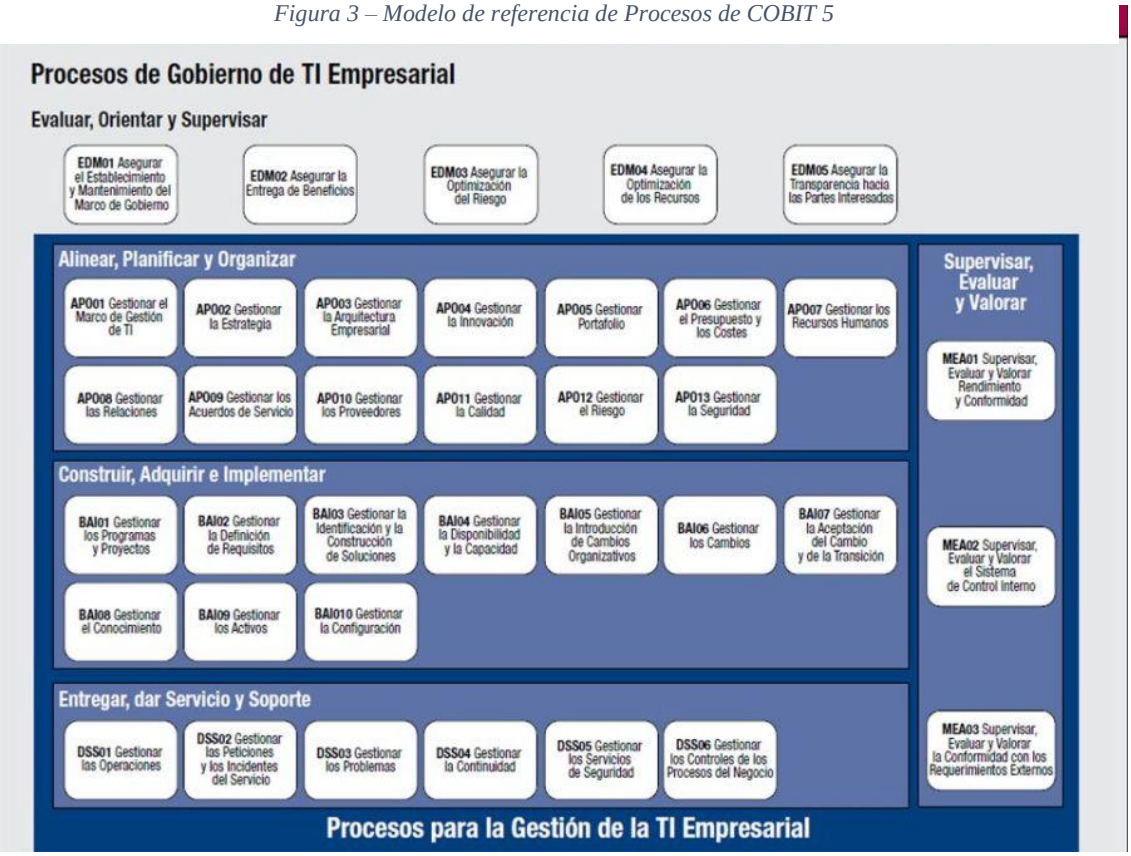
2.4.1 **Modelo de referencia de procesos de COBIT 5**

Los procesos habilitadores complementan el marco COBIT 5 y contienen una guía de referencia detallada sobre los procesos que están definidos en el modelo de referencia de procesos de COBIT 5.

El modelo de referencia de procesos de COBIT 5 subdivide las actividades prácticas de la organización relacionadas con la TI en dos áreas principales: el área de gobierno y la administración, siendo esta última dividida en dominios de procesos. Para COBIT 5, el dominio de Gobierno se asocia con cinco procesos enfocados hacia las prácticas de Evaluar, Dirigir y

Monitorear; por su parte los dominios de la Administración contemplan planificación, construcción, operación y monitoreo. A continuación, se presenta de manera gráfica.

Figura 3 – Modelo de referencia de Procesos de COBIT 5



Fuente: COBIT 5. (2012). Procesos de Gobierno de TI Empresarial. Recuperado de: **http://repositorio.puce.edu.ec/bitstream/handle/22000/6078/T-PUCE-6320.pdf?sequence=1**

A continuación, se hace una valoración de aquellos aspectos involucrados en cada una de las prácticas planteadas por DSS04:

- DSS04.01: definir la política y alcance de continuidad del negocio alineada con los objetivos de negocio y de las partes interesadas, identificando los procesos y actividades críticas, así como los roles y responsabilidades para definir y acordar la política de continuidad y su alcance. Identificar procesos esenciales de soporte al negocio y servicios TI relacionados. (Palacios, 2016).

- DSS04.02: evaluar las opciones de gestión de la continuidad del negocio y escoger una estrategia de la continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción. Identificar escenarios potenciales probables que puedan estimular eventos que puedan causar incidentes disruptivos importantes y que permitan realizar un análisis de impacto y efecto en el negocio. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad del negocio e identificar medidas que puedan reducir la probabilidad y el impacto. (Palacios, 2016)

- DSS04.03: desarrollar un plan de continuidad del negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas. Desarrollar y mantener planes de continuidad del negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de procesos, definiendo las acciones y comunicaciones de respuesta a incidentes que deben ser realizas. Definir las condiciones y procedimientos de recuperación. (Palacios, 2016)

- DSS04.04: probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera. Definir los objetivos para ejercitar y probar los sistemas del plan y acordar ejercicios que sean razonables con las partes interesadas. (Palacios, 2016)

- DSS04.05: realizar una revisión, por la dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo con el proceso de control de cambios para asegurar que el plan de continuidad se tenga actualizado y refleje

continuamente los requerimientos actuales del negocio. Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales, recomendando y comunicando los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades. (Palacios, 2016)

- DSS04.06: proporcionar a todas las partes implicadas, internas y externas de sesiones formativas regulares que contemplen los procedimientos, sus roles y responsabilidades en caso de disrupción. Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continua la planificación de la continuidad, el análisis de impacto, las evaluaciones de riesgos, la comunicación con los medios y la respuesta a incidentes. Supervisar habilidades y competencias. (Palacios, 2016)

- DSS04.07: mantener la disponibilidad de la información crítica del negocio. Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo con una planificación definida, considerando: frecuencia, modo de copias de seguridad automatizadas en línea, tipos de datos, creación de registros, datos de cálculos críticos de usuario final, localización física y lógica de las fuentes de los datos, seguridad y derechos de acceso, cifrado. Considerar la accesibilidad requerida a las copias de seguridad. (Palacios, 2016)

- DSS04.08: evaluar la adecuación del plan de continuidad del negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios ante una disrupción. Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, incidentes, infraestructura técnica y estructuras organizativas y relaciones. Identificar debilidades u omisiones en el plan, sus capacidades y haber recomendaciones para la mejora. (Palacios, 2016)

2.5 Seguridad de la información

La norma ISO 27001 define la seguridad de la información como, preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad.

2.5.1 Pilares de seguridad de la información

Para llegar a alcanzar los objetivos descritos por la seguridad de la información, dentro del proceso de gestión de la seguridad informática es necesario contemplar una serie de servicios o funciones que se enumeran más adelante.

2.5.1.1 Confidencialidad

Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático sólo podrá ser leído por su legítimo destinario, es decir si dicho mensaje cae en manos de terceras personas, éstas no podrán acceder al contenido del mensaje original. Por lo tanto, este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de backup y/o de los datos transmitidos a través de redes de comunicaciones. (Gómez, 2014)

2.5.1.2 Integridad

La función de integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática. De este modo, es posible detectar si se ha añadido o eliminado algún dato en un mensaje o fichero almacenado, procesado o transmitido por un sistema o red informática. (Gómez, 2014)

2.5.1.3 Disponibilidad

La disponibilidad del sistema informático también es una cuestión de especial importancia para garantiza el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar permanentemente a disposición de los usuarios que deseen acceder a sus servicios.

Dentro de la disponibilidad también debemos considerar la recuperación del sistema frente a posibles incidentes de seguridad, así como frente a desastres naturales o intencionados (incendios, inundaciones, sabotajes).

Se debe tener en cuenta que de nada sirven los demás servicios de seguridad si el sistema informático no se encuentra disponible para que pueda ser utilizado por sus legítimos usuarios y propietarios. (Gómez, 2014)

2.5.2 **Controles de seguridad de la información**

Los controles de seguridad son los mecanismos que se utilizan para controlar los accesos y privilegios que posee una organización, ya sea, un sistema o activo que se desee resguardar es responsabilidad del defensor velar por la seguridad de este, con la implementación y aplicación de controles tanto lógicos como físicos requeridos para la disponibilidad, confidencialidad e integridad del mismo.

2.5.2.1 **ISO 27002**

Es el nuevo nombre de la anterior norma ISO/IEC 17799:2005, aprobada en julio de 2007, se trata de una guía de buenas prácticas que describe 39 objetivos de control y 133 controles recomendables en cuanto a seguridad de la información, se agrupan en 11 dominios. La norma ISO/IEC 20771 contiene un anexo que resume todos los controles de la ISO/IEC 27002. (Gómez, 2014)

En España fue publicada por AENOR como la UNE-ISO/IEC 27002:2009 el 09 de diciembre de 2009. Los 11 dominios previstos en está norma para agrupar los controles de seguridad son los siguientes: (Gómez, 2014)

- Análisis de riesgos.
- Política de seguridad.
- Organización de seguridad (tanto interna como de terceras partes).
- Gestión de activos.
- Seguridad de los Recursos Humanos.
- Seguridad física.
- Gestión de comunicaciones y de operaciones de explotación.

- Desarrollo y mantenimiento de sistemas.
- Control de accesos.
- Gestión de incidentes.
- Plan de continuidad del negocio.
- Conformidad legal.

2.5.2.2 Controles de seguridad físicos

Los controles físicos es una medida de seguridad en una determinada estructura organizacional usada para prevenir o detener el acceso no autorizado a la información confidencial de la empresa que salvaguarda los activos tangibles de la empresa. Contemplan aquellos elementos relacionados con el entorno, algunos ejemplos de este control son: la autenticidad por parte de los empleados de la compañía en las puertas de entrada al edificio, cámaras de videovigilancia, alarmas en accesos restringidos, guardias de seguridad revisando personal sospechoso.

2.5.2.3 Controles de seguridad lógicos

Los controles lógicos son las medidas electrónicas para prevenir el ingreso de personas no autorizadas a sistemas empresariales, requieren que los usuarios realicen una identificación y posteriormente la autorización, estos controles están muy relacionados con el cifrado de datos y telecomunicaciones. Se intenta el uso correcto de software, sistemas operativos, acceso a sistemas organizacionales privilegiada a diferentes tipos de roles de usuario.

2.6 Sistema de gestión de seguridad de la información (SGSI)

Se define el Sistema de Gestión de la Seguridad de la Información (SGSI), según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Lo que permitirá conocer mejor la organización, funcionamiento y qué se podría hacer para que la situación mejore.

La norma específica que, como cualquier otro sistema de gestión, el SGSI incluye tanto la organización como las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Es decir, tanto la documentación de soporte como las

tareas que se realizan. Los sistemas de gestión que definen las normas ISO siempre están documentados, ya que, por un lado, es la mejor manera de formalizar normas e instrucciones y, por otro, son más fáciles de transmitir y comunicar, cosa que no sucedería si se confía en un traspaso de información verbal informal. (UNE-EN ISO 27001:2005, 2017)

2.6.1 **Sistema de gestión de continuidad del negocio (SGCN)**

La continuidad del negocio puede definirse como una estrategia y táctica de una organización para recuperar, restaurar sus funciones, planificar y responder ante incidentes o desastres que puedan afectar la disponibilidad, con el fin de darle continuidad a un nivel aceptable a los servicios.

El sistema de gestión de continuidad del negocio (SGCN), consiste en tener una preparación proactiva de recuperación desde los planes de contingencias, como de los servicios críticos de la organización, mediante el desarrollo de mecanismos de análisis y procesos claves para la restauración rápida con el fin de minimizar los impactos y mitigar los riesgos.

Según la norma ISO 22301 define el sistema de gestión de continuidad de negocio como parte del sistema general de gestión que establece, implementa, opera, monitorea, revisa, mantiene y mejora la continuidad de negocio. (Instituto de Normalización y Certificación, 2012)

2.6.2 **ISO 22301:2012**

La norma ISO 22301:2012 es en sí la primera norma de tipo internacional creada como sistema de gestión de la continuidad del negocio. Su creación se fundamenta en la necesidad de minimizar el riesgo de interrupciones en las empresas. Entre sus especificaciones se presentan los requisitos necesarios que permiten a las organizaciones responder y recuperarse lo más pronto posible de las interrupciones en el momento que sucedan. Para ello se especifica en los siguientes procesos: establecer, planificar, modelar, implantar, revisar, monitorear, mantener y mejorar el sistema de gestión. Estos requisitos pueden ser aplicados a todas las empresas, sin importar la naturaleza o tamaño de esta, puesto que la aplicación de estos depende de la complejidad de la empresa y el ambiente operativo en que se desarrolla. (ISO, 2012)

La norma internacional para la gestión de la continuidad del negocio, denominada ISO 22301:2012, establece cómo identificar las amenazas potenciales de una organización y los

impactos en las operaciones de negocio a fin de contar con capacidad de respuesta para salvaguardar sus intereses; además, explica las fases del BCP de la siguiente manera. (ISO, 2012)

- Descripción del negocio y análisis de riesgos.
- Estrategias o mitigación del riesgo.
- Desarrollo de implantación del plan.
- Mantenimiento del plan.

2.6.3 Good Practice Guidelines (GPG)

La guía elaborada por el Business Continuity Institute (BCI), denominada Good Practice Guidelines (GPG), que en español se traduce en: buenas prácticas para la continuidad del negocio, explica el cómo y el porqué de los principios de la disciplina de continuidad del negocio, incluyendo la terminología de la norma ISO 22301 para asegurar los más altos estándares en su ejecución. (BCI, 2013)

El sistema de Good Practice Guidelines contiene el ciclo de vida de la gestión de continuidad del negocio (BCM) y además cuenta con una detallada descripción de las seis prácticas profesionales, que son utilizadas por los especialistas de Business Continuity. (Saéz, 2015)

- Política de BCM y programa de administración.
- Entendimiento de la organización.
- Determinando la estrategia de continuidad del negocio.
- Desarrollo e implementación de responsabilidades.
- Probar, dar mantenimiento y revisión del programa de continuidad del negocio.
- Desarrollar una cultura de continuidad del negocio en la organización.

2.6.4 Objetivo del SGCN

Permite la planificación, administración, seguimiento, control y mejoramiento permanente de la estrategia de continuidad del negocio de la compañía para garantizar la continuidad del negocio.

2.7 Ciclo PHVA (Planear – Hacer – Verificar – Actual)

Deming en su obra lo define al ciclo PHVA como una herramienta de simple aplicación y que cuando se utiliza adecuadamente, puede ayudar mucho en la ejecución de actividades más organizadas y eficaces. El ciclo Deming está constituida básicamente por cuatro actividades:

planificar, realizar, comprobar, actúa, que forma un ciclo que se repite en forma continua. (Cuatrecasas, 2010)

El ciclo Deming es un procedimiento destinado al mejoramiento de los problemas analíticos o de oportunidades. Este ciclo busca inicialmente, reconocer las oportunidades, posteriormente probar la teoría planteada y observar los resultados y finalmente actuar en la oportunidad. (Scherkenbach, 1998, p.31)

El ciclo de Deming se desarrolla a través de cuatro etapas planificar, hacer, verificar y actuar, tomando medidas preventivas para que la mejora no sea reversible, o reestructurando el plan debido a que los resultados no fueron satisfactorios, con lo que se vuelve a iniciar el ciclo. (Cuatrecasas, 2010, p. 66)

El ciclo PHVA se puede resumir de la siguiente forma:

- Planificar: se establecen los objetivos, procesos, procedimientos de continuidad del negocio para así dar alcance a los resultados obtenidos, dando conformidad a los requisitos establecidos por la alta dirección y las políticas de la organización.
- Hacer: se implementa y se ejecuta los procesos y procedimientos de continuidad de negocio para lograr los objetivos.
- Verificar: se realiza un seguimiento a procesos, conforme a lo establecido en la primera fase del ciclo, de esta forma se reportan los resultados alcanzados, se efectúan hallazgos que permiten tomar acciones de mejoramiento.
- Actuar: se realizan acciones para promover la mejorar de los procesos, implementando acciones correctivas y se vuelve a iniciar el ciclo con un nuevo plan de mejora.

2.8 **Riesgos**

El riesgo no es más que la suma de las amenazas y vulnerabilidades encontradas o analizadas al sistema de información de una compañía o entidad. (Cuichán, 2014)

$$Amenaza + Vulnerabilidad = Riesgo$$

2.8.1 **Gestión de riesgos**

En términos generales la gestión del riesgo se refiere a los principios y metodología para la gestión eficaz del riesgo, mientras que gestionar el riesgo se refiere a la aplicación de estos principios y metodología a riesgos particulares.

La administración del riesgo comprende el conjunto de elementos de control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que pueden afectar de manera positiva o negativa el logro de sus objetivos institucionales. La administración del riesgo contribuye a que la entidad consolide su sistema de control interno y a que se genere una cultura de autocontrol y autoevaluación al interior de esta. (Universidad Nacional de Colom, 2013)

El principal objetivo de la gestión de riesgos es darle valor a todas las actividades más indispensables de la empresa, generando un futuro del lado positivo y negativo de todos aquellos factores potenciales que afectan directamente a CENECOOP R.L, aumenta el éxito y disminuye el fracaso como la incertidumbre en los objetivos generales de la organización, la gestión de riesgo debe ser todo un extenso proceso continuo y de desarrollo constante para lograr los objetivos estratégicos propuestos por el Centro de Estudios y Capacitación Cooperativa y de esta manera minimizar el impacto en las metas pasadas, presentes y más que todo futuras en la empresa. (Casares, 2013)

2.8.2 **Identificación de amenazas**

Se considera una amenaza a cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización. Se pueden establecer la siguiente clasificación a las amenazas a la seguridad; amenazas naturales, amenazas de agentes externos y amenazas de agentes internos. (Gómez, 2014)

De acuerdo con el estudio de los procesos empresariales y tomando en cuenta los recursos de TI utilizados, existen amenazas en el orden técnico, humano, naturales, estructurales y organizacionales los cuales se encuentran detallados en la siguiente tabla.

Tabla 1 – Identificación de amenazas

Origen de amenaza	Amenaza	Consecuencia
Técnicas	Mal funcionamiento de equipos.	Atasco en la operación.
	Software sin licencias.	Software malicioso.
	Fallas de las aplicaciones.	Pérdida de información.
	Falla de servicios contratados (ISP).	Fallos en los sistemas.
Humanas	Hacking.	Atentado a la confidencialidad de la información.
	Divulgación de información confidencial.	Estafas.
	Terrorismo.	Daño potencial a equipos informáticos.
	Negligencia en el manejo de activos de TI.	Libre acceso a la información.
Naturales	Terremotos.	Daño potencial a equipos tecnológicos.
	Tormentas eléctricas.	Fallos en las conexiones eléctricas.
	Inundaciones.	Daño potencial a equipos tecnológicos.
Estructurales	Incendios.	Daño potencial a equipos tecnológicos.
	Mal estado de instalaciones.	Daño potencial a equipos tecnológicos.
	Fallas eléctricas.	Atasco en la operación de la empresa.
Organizacionales	Flujo de personal.	Ventaja competitiva.
	Falta de políticas.	Libre acceso a la información.

	Falta de gestión de seguridad.	Filtro de información confidencial.

Fuente: elaboración propia.

2.8.3 **Identificación de vulnerabilidades**

Una vulnerabilidad es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización.

Las vulnerabilidades se corresponden con fallos en los sistemas físicos y/o lógicos, aunque también pueden tener su origen en los defectos de ubicación, instalación, configuración y mantenimiento de los equipos.

Pueden estar ligadas a aspectos organizativos (procedimientos mal definidos o sin actualizar, ausencia de políticas de seguridad), al factor humano (falta de formación y/o de sensibilización del personal con acceso a los recursos del sistema), a os propios equipos, a los programas y herramientas lógicas del sistema, a los locales y las condiciones ambientales del sistema (deficientes medidas de seguridad físicas, escasa protección contra incendios, mala ubicación de los locales con recursos críticos para el sistema). Se suele emplear una escala cuantitativa o cualitativa para definir el nivel de vulnerabilidad de un determinado equipo o recurso: Baja, Media y Alta. (Gómez, 2014)

Una vez identificadas las amenazas para poder determinar las vulnerabilidades se ha realizado un análisis detallado de los impactos en cada una de dichas amenazas y sus consecuencias en caso de que lleguen a ocurrir. En la tabla 2 se detalla una lista de vulnerabilidades relacionadas con las amenazas identificadas en el punto anterior.

Tabla 2 – Identificación de vulnerabilidades

Amenazas	Vulnerabilidades
Mal funcionamiento de los equipos.	Falta de mantenimiento preventivo a los equipos.
Software sin licencias.	Software altamente distribuido.
Fallas de las aplicaciones.	Configuraciones mal realizadas.
Falla de los servicios contratados (ISP).	Conexiones de red pública sin protección.

Hacking.	Infraestructura de red insegura.
Divulgación de información confidencial.	No existen acuerdos de confidencialidad.
Terrorismo.	Falta de personal de seguridad para resguardar la organización.
Negligencia en el manejo de activos de TI.	Uso indebido de los recursos tecnológicos.
Terremotos.	Estructuras en mal estado.
Tormentas eléctricas.	Falta de control en las UPS.
Inundaciones.	Falta de control de calidad en las instalaciones.
Incendios.	No se realiza una revisión en los extintores de la organización.
Mal estado de instalaciones.	No se realiza un control de las instalaciones.
Fallas eléctricas.	Falta de mantenimiento en planta de energía de respaldo.
Flujo de personal.	Procedimientos inadecuados de contratación.
Falla de políticas.	Falta de auditorías para controlar los procesos de TI.
Falta de gestión de seguridad informática.	Ausencia de personal de seguridad informática.

Fuente: elaboración propia.

2.8.4 **Identificación de riesgos**

La identificación de riesgos es un proceso sistemático que consiste en identificar las amenazas sobre estos activos y su probabilidad de ocurrencia, vulnerabilidades asociadas a cada activo y el impacto que las citadas amenazas pueden provocar sobre la disponibilidad de los mismo. Existen varias metodologías de identificación de riesgos, de igual manera soluciones de software que permiten automatizar dicho proceso, sin embargo, todas se basan en el siguiente esquema de funcionamiento:

- Identificar activos.
- Identificar y evaluar las amenazas.
- Identificar y valorar las vulnerabilidades.

Calcular el riesgo como la probabilidad de que se produzca un impacto determinado en la organización. Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (contratando un servicio o un seguro de cobertura), o en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario. (Bautista, 2014)

La identificación de riesgos es altamente peligrosa en el ámbito financiero (sin dejar de lado otros ámbitos) pero es que en este influye sobre cualquier otro y es que la pérdida de activos, capital, costes legales, llegando a uno de los activos más importante por cualquier empresa los clientes. La interrupción del negocio puede ser uno de los ataques más pasivos, pero a su vez más peligrosos en impactar una organización, que puede llegar a ser tan caótico como el cierre de sucursales, despido de personal e incluso quebrar cualquier entidad. (Balmaceda, 2019)

Existen una serie de pautas importantes que ayudan a la cuantificación de cualquier riesgo que son:

1. Conocer los proveedores del segundo y tercer nivel, es decir, aquellas empresas que proporcionan bienes, servicios o ingredientes que se requieren directamente con los servicios de la organización.
2. Identificar los activos no físicos críticos que generan un valor agregado a los ingresos en la empresa, incluyendo las tecnologías con un plan estratégico en tecnologías de información.
3. Conocer las áreas de mejora en cada uno de los departamentos de la organización.

2.8.4.1 **Escalas de medición del riesgo**

Los resultados obtenidos del análisis de riesgos serán evaluados en base a la norma NTE ISO/IEC 27005 [9].

Tabla 3 – Matriz escala de Probabilidad x Impacto

Matriz PxI			**Escala de probabilidad**				
			Muy improbable	Improbable	Posible	Probable	Muy probable
			1	2	3	4	5
Im	Bajo	1	1 x 1	2 x 1	3 x 1	4 x 1	5 x 1

	Medio	2	1 x 2	2 x 2	3 x 2	4 x 2	5 x 2
	Alto	3	1 x 3	2 x 3	3 x 3	4 x 3	5 x 3

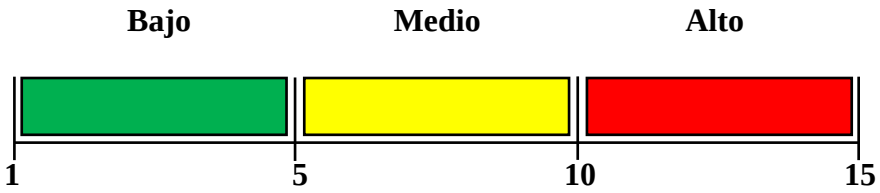
Fuente: elaborado por NTE ISO/IEC 27005.

2.8.4.2 **Categoría del riesgo**

Se plantean tres categorías del riesgo:

- Bajo: 1 – 5
- Medio: 6 – 10
- Alto: 11 – 15

Figura 4 – Categorías del riesgo



Fuente: elaboración propia. Todos los derechos reservados de NTE ISO/IEC 27005.

2.9 **Norma NFPA 1600**

Es la norma más antigua, creada en 1995 por el Comité de Gestión de Desastres, referente a la BCM por sus siglas inglés (Business Continuity Management) y estableció por primera vez criterios comunes para el gerenciamiento, manejo de desastres y emergencias para los programas de continuidad del negocio; desde su creación ha sido la base de la implementación del concepto que está detrás del BCM independientemente del tipo (pública o privada) y ubicación geográfica de la empresa. (Posada & Otero, 2013)

Proporciona una base estandarizada para la planificación y gestión de programas de continuidad de negocio en caso de desastres o emergencia en los sectores público y privado. En la edición del 2007, se expande un framework conceptual para la gestión de desastres o emergencias y programas de continuidad de negocio. Además, esta edición identifica la prevención como un aspecto del programa como adicional a los cuatro ya establecidos (mitigación, preparación, respuesta y

recuperación), haciendo que esta norma esté alineada con disciplinas relacionadas a la gestión de riesgos, seguridad y prevención de pérdidas. (National Fire Protection Association, 2007)

La valoración de riesgos debe clasificar los peligros por su frecuencia relativa y su severidad, teniendo en cuenta que podrían existir varias posibles combinaciones de frecuencia y severidad. La entidad debe intentar mitigar, prepararse, planificar y recuperarse de algunos peligros que podrían impactar significativamente a las personas, la propiedad, las operaciones, el entorno o la entidad en sí misma. (NFPA 1600, 2007)

Con el paso del tiempo, la norma ha sido objeto de varias actualizaciones que brevemente se resumen a continuación:

En la edición del 2000 el comité incorporo el "Enfoque Total del Programa" para manejo de desastres/emergencias y continuidad de negocio que provee una base estandarizada para la planeación y los programas en el sector público y privado, mediante elementos, técnicas y procesos comunes e incluyo material anexo referente a programas de BCM.

En la edición del 2004, básicamente se dio una actualización del formato de acuerdo con el manual de estilo del comité de documentos técnicos de NFPA y se actualizo la terminología. Adicionalmente se creó un puente entre FEMA CAR, NFPA 1600 y BCI &DRII.

La edición del 2007 incorpora algunos cambios a la edición del 2004, expandiendo el marco conceptual para manejo de desastres/emergencias y BCM, esta edición identifica la prevención como un aspecto diferenciador del programa, esta es quizás una de las adiciones más relevantes en el proceso evolutivo de la norma.

Finalmente, en la edición del 2010, la norma experimenta una reorganización y expansión que básicamente busca enfatizar el papel del liderazgo y el compromiso, sin embargo, el cambio más notable respecto a la edición del 2007 fue la reorganización del capítulo 5 en cuatro capítulos que siguen la metodología ciclo mejoramiento continuo PHVA (Planear, Hacer, Verificar y Actuar). Otros cambios que se incorporaron fueron una sección de asistencia y soporte al empleado, la ampliación de pruebas y ejercicios en el capítulo 7 y la incorporación de acciones correctivas y evaluaciones en el capítulo 8.

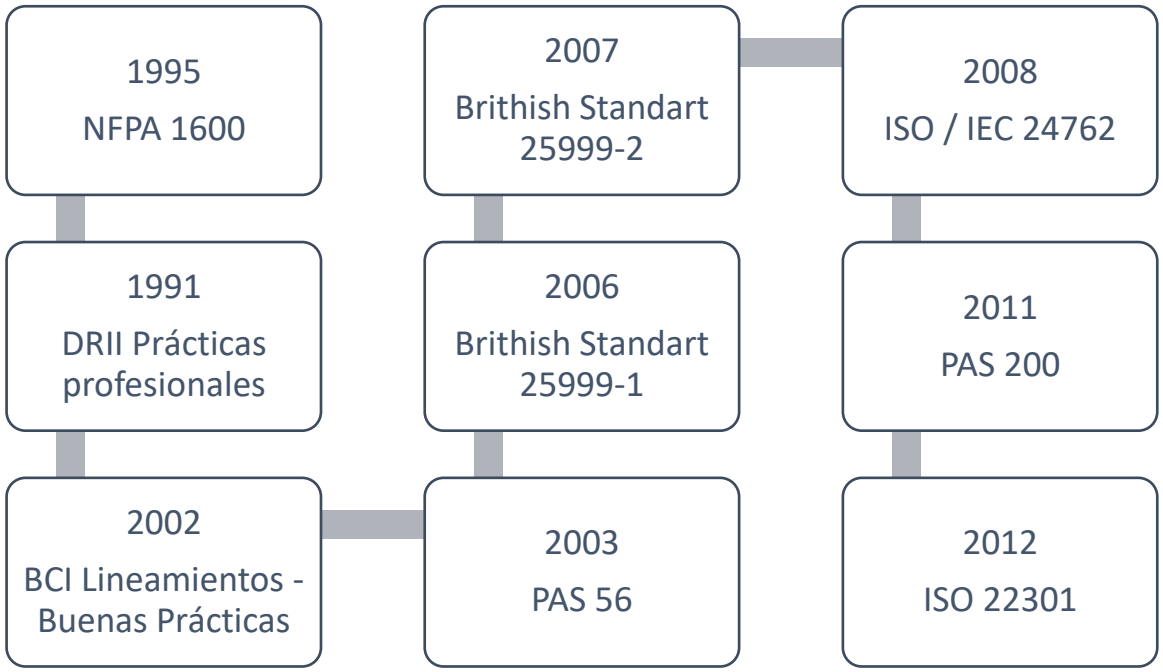
Algunos de los riesgos que la norma considera evaluar son:

- Riesgos naturales como geológicos, meteorológicos y biológicos.
- Eventos causados por humanos intencionales o accidentales.
- Eventos causados tecnológicamente accidentales o intencionales.

Esta norma introduce el concepto de análisis de impacto al negocio, BIA por sus siglas en inglés (Business Impact Analisys) que es básicamente un análisis de nivel gerencial que identifica el impacto de la perdida de recursos de la empresa. (Posada & Otero, 2013)

En la siguiente figura se ilustra la evolución de los estándares iniciando en 1995 con la norma NFPA 1600 pionera en la definición de conceptos de evaluación de riesgos que pueden comprometer la continuidad de negocio, hasta llegar a la norma ISO 22301:2012 que reemplaza a los estándares previos existentes y hace una coalición con las normas ampliamente aplicadas en las empresas como lo son: ISO 9001, ISO 14001, ISO 18001.

Figura 5 – Evolución de los estándares relacionados con BCP



Fuente: elaboración propia. Todos los derechos reservados de Organización Internacional de Estandarización.

2.10 **Recuperación de desastres**

El DRP (Disaster Recovery Planning, por sus siglas en inglés) según Bautista (2014) lo define como: “El proceso de evaluación de los riesgos que enfrenta una organización, para luego desarrollar, documentar, implementar, probar y mantener procedimientos que ayudan a la organización a retornar rápidamente a las operaciones normales y reducir al mínimo las pérdidas después de un desastre. Un DRP está enfocado a los sistemas de información, diseñado para restablecer la operación de los servicios informáticos críticos específicos (hardware y software), con instalaciones, infraestructura y procedimientos alternos, en caso de una emergencia; el responsable del DRP es el departamento de TI de la organización”.

Es por ello que el DRP debería estar alineado con la estrategia de la organización; la criticidad de los diferentes sistemas de información depende de la naturaleza del negocio, así como también, del valor que cada aplicación aporta a la empresa.

Debido a que cada organización tiene su identidad, cultura, clima organizacional, relaciones con sus clientes, socios de negocios y el público en general. Estas relaciones deberían conducir a una organización en el emprendimiento de una iniciativa de planificación de recuperación de desastres. (Bautista, 2014)

El CENECOOP R.L en la actualidad no cuenta con ningún tipo de plan de recuperación de desastres (DRP) que considere los equipos y aplicativos que soportan los procesos críticos de la misma, el cuál sería utilizado para mantener la continuidad de las operaciones en caso de una eventual destrucción temporal o permanentes de las instalaciones o equipos.

La realización del BCP/DRP en la organización trae grandes ventajas como las que se nombran a continuación:

- Se puede administrar la continuidad del negocio.
- Resistencia del negocio ante interrupciones.
- Detectar los servicios más vulnerables y las posibles causas.
- Protege y asegura la imagen del Centro de Estudios y Capacitación Cooperativa.
- Genera oportunidades de mercado.
- Aumenta la disponibilidad del negocio en los servicios que se brindan. (Peralta & Bolivar, 2017)

2.11 **Análisis de impacto sobre el negocio (BIA)**

El análisis de impacto sobre el negocio (Business Impact Analysis o BIA por sus siglas en inglés), es otra de las herramientas empleadas para evaluar las consecuencias que podría sufrir una organización producto de alguna eventualidad o un desastre que tenga lugar en el entorno de esta. (Mendoza, 2014)

El BIA constituye un proceso más especializado que se basa específicamente en el "cómo" las organizaciones serían afectadas por las amenazas que atentan contra la seguridad de estas, atendiendo a la determinación, análisis y a la evaluación de los impactos económicos, probabilidad de ocurrencia y consecuencias que tendrían los riesgos sobre las operaciones y activos del negocio. (Mendoza, 2014)

Dentro del BIA según Mendoza existen varios conceptos importantes, como:

- ✓ Punto de recuperación objetivo (Recovery Point Objective – RPO): hace alusión a la antigüedad máxima de los datos para su restauración, es decir, la tolerancia que la empresa puede permitir para operar con datos de respaldo, por lo que el RPO estará en función de las actividades de una organización.

Tabla 4 – Estimación de RPO

Valor	Descripción
1	La actividad o el proceso requiere alta disponibilidad (100%).
2	La actividad o el proceso no puede estar interrumpida más de 4 horas.
3	La actividad o el proceso no puede estar interrumpida más de 8 horas.
4	La actividad o el proceso no puede estar interrumpida más de 24 horas.
5	Otros requisitos menos restrictivos que los indicados previamente.

Fuente: elaboración propia según estándares del Instituto Nacional de Ciberseguridad (2014).

- ✓ Tiempo de recuperación objetivo (Recovery Point Objective – RTO): es el período permitido para la recuperación de una función o recurso de negocio a un nivel aceptable luego de una interrupción o desastre.

Tabla 5 – Estimación de RTO

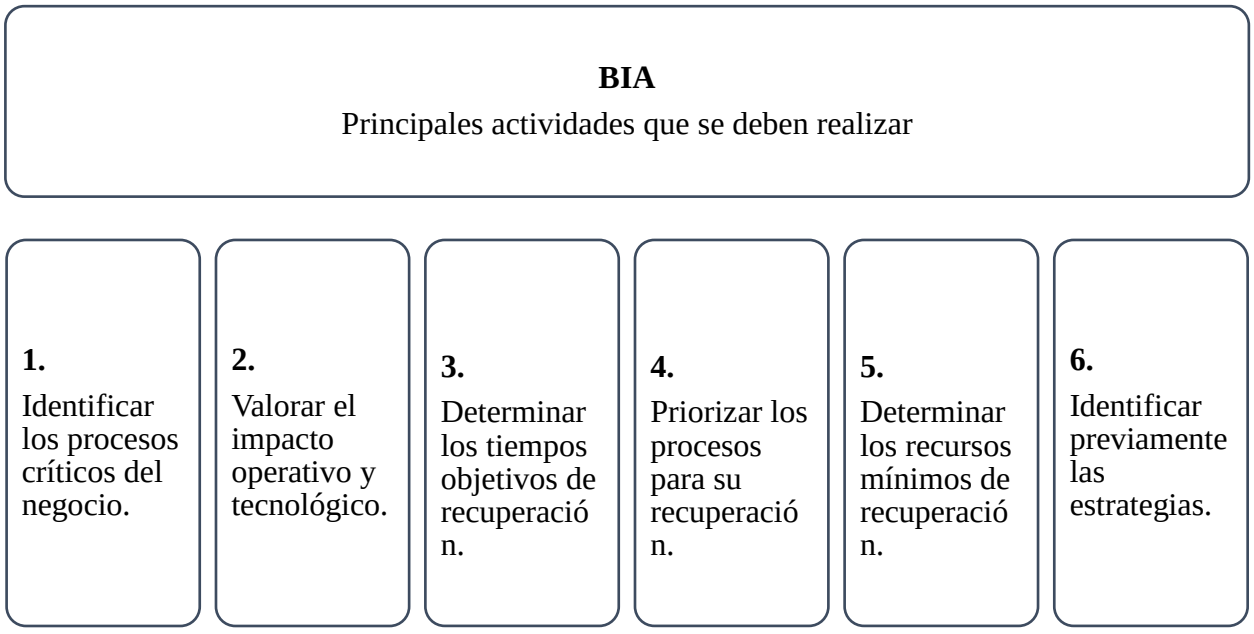
Valor	Descripción
1	La actividad o el proceso requiere alta disponibilidad (100%).
2	La actividad o el proceso no puede estar interrumpida más de 8 horas.
3	La actividad o el proceso no puede estar interrumpida más de 24 horas.
4	La actividad o el proceso no puede estar interrumpida más de 72 horas.
5	Otros requisitos menos restrictivos que los indicados previamente.

Fuente: elaboración propia según estándares del Instituto Nacional de Ciberseguridad (2014).

- ✓ Período máximo tolerable de tiempo de inactividad (Maximum Tolerable Period Of Down time – MTPOD): es el período máximo de no disponibilidad para las actividades, activos o procesos, antes de que la empresa deje de operar.

En la siguiente figura se describe cada una de las etapas o actividades que se implementan para realizar un análisis de impacto al negocio.

Figura 6 – Etapas del análisis de impacto al negocio



Fuente: elaboración propia.

2.12 **Comparación de estándares de continuidad del negocio**

En la siguiente tabla se muestra un punto de partida en el proceso de cada uno de los estándares, cualquier estándar de continuidad de negocio se puede usar en una organización.

Tabla 6 – Comparación de estándares de continuidad del negocio

Característica	ISO 22301	NFPA 1600	COBIT 5
Origen	Estándar Internacional de ISO.	Estándar local de EE.UU de la NFPA.	Origen británico por ISACA.
Creado el	2012	1995	1996
Costo	Costosa	Si costo	Costosa
Objetivo	Mantener la continuidad de las actividades de una organización, proteger sus intereses defendiendo los intereses de sus empleados y partes interesadas	Evaluar los programas actuales de gestión de desastres y gestión de emergencias y de continuidad de actividades.	Alcanzar los objetivos estratégicos y obtener los beneficios de negocio a través del uso efectivo e innovador de las TI.
Mejora en	Planificación de recursos para garantizar la continuidad.	Evaluación de riesgos mucho más precisos.	Mapeo de procesos de TI.
Responsabilidad	Jefatura de tecnología, partes interesadas.	Jefatura de tecnología, partes interesadas.	Jefatura de tecnología, partes interesadas.
¿Quiénes lo evalúan?	Empresa consultora de TI.	La misma organización.	Empresa consultora de TI.
Certificable	Sí	No	No
Integrable	Sí	Sí	Sí
Estructura	10 dominios.	10 dominios.	34 procesos de TI agrupados en 4 dominios.
Actualización constante	Sí	No (En 2012 se convierte a ISO 22301).	Sí

Tipo de organización	Muy flexible, todo tipo de organización.	Organizaciones medianas y grandes.	Muy flexible, todo tipo de organización.
Mejora continua	Capítulo 10.2	Capítulo 8	DS4.10
BIA	Capítulo 8.4.2	Capítulo 5.5	-
Identificación de recursos	Capítulo 7.1	Capítulo 6.1	DS4.3
Roles y responsabilidades	Capítulo 5.4	Capítulo 6.6	DS4.6
Testeo y pruebas	Capítulo 8.6.1	Capítulo 7	DS4.5
Seguimiento y evaluación	Capítulo 9.1	-	DS4.4
Auditoría interna	Capítulo 9.2	-	-
Acciones correctivas	Capítulo 10.1	-	DS4.7

Fuente: elaboración propia.

CAPÍTULO III
MARCO METODOLÓGICO

3.1 **Tipo de investigación**

En la presente tesis, se seleccionaron variables que posteriormente fueron analizadas por el investigador, esto hace hincapié que el estudio en su primera fase es descriptivo, Sampieri lo define como: “los estudios que buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis”. (2003) De esta forma todos los procesos críticos de la organización pudieron identificarse y analizarse gracias al estudio descriptivo y así llegar a dar soluciones concretas y efectivas para el problema planteado.

La investigación termina siendo del tipo aplicada, ya que se empleó el conocimiento obtenido en la investigación descriptiva con el fin de diseñar un modelo de continuidad del negocio para que sea aplicado por la empresa y así tener los mecanismos necesarios para afrontar las consecuencias en caso de que se materialice un desastre y se pueda dar la continuidad del negocio.

3.1.1 **Enfoque de la investigación**

El método mixto representa un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (metainferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (Hernández Sampieri y Mendoza, 2008).

El enfoque del proyecto es mixto, debido a que, en el transcurso de toda la investigación, resultan variables que se pueden cuantificar, sin embargo, otras no son posibles cuantificar, además la meta es la descripción del problema. Exponiendo cuantas cualidades presentan el problema de continuidad del negocio en la organización, se trata de acercar la realidad a través del contacto con la obligación de la entidad, partiendo de una metodología.

Este tipo de enfoque da una mayor solidez al método científico, asimismo de mayor posibilidad de éxito al presentar los resultados, permite una mejor exploración y utilización de los datos.

3.2 Fuentes y sujetos de información

3.2.1 Fuentes primarias

Se coordina con los encargados de los departamentos de Tecnologías de Información como de Investigación y Desarrollo de la organización para obtener información acerca de los procesos críticos del Centro de Estudios y Capacitación Cooperativa CENECOOP R.L.

De igual manera se adquirió información de la materia, perteneciente a proyectos de graduación anteriores realizados por estudiantes de universidades públicas y privadas.

Se consultó la norma ISO 22301: Societal security – Business continuity management systems y la guía de mejores prácticas COBIT 5 an Isaca Framework.

Se analizó la normativa NFPA 1600: Standard on disaster/emergency management and business continuity programs,

3.2.2 Fuentes secundarias

Se tomaron en cuenta las siguientes fuentes secundarias:

- Datos de los resultados del Índice de Gestión Institucional (IGI) de la Contraloría General de la República en el año 2018 en el área de tecnologías de información, que tiene como objetivo mantener la confiabilidad, disponibilidad e integridad de la información, así como facilitar el mejor aprovechamiento de los recursos informáticos y telecomunicaciones, que se encuentran a disposición del CENECOOP R.L, para alcanzar la misión institucional. (Ver apéndice 1.3)

3.2.3 Fuentes terciarias

Entre estas fuentes se toman en cuenta:

- National Business Continuity Management.
- Instituto Nacional de Tecnologías de la Comunicación.

3.2.4 **Sujetos de información**

Son todos aquellos medios de los cuales procede la información, que satisfacen las necesidades de conocimiento de una situación o problema presentado y, que posteriormente será utilizado para lograr los objetivos esperados. (Sampieri et al., 2003)

Las personas de contacto para la recolección de información son los expertos de las áreas de CENECOOP R.L, así como las diferentes herramientas para análisis de riesgos, estos sujetos de información colaboran directamente con la investigación, suministrando información o bien interactuando a ciencia cierta con el proyecto, estás personas son las que se detallan en la tabla 1.

Tabla 7 – Sujetos de información

Descripción general	**Puesto u Oficio**	**Experiencia**	**Relación con el tema**
Jefatura de TI	Ingeniero en Informática.	4 años como encargado del departamento.	Conoce los problemas de la organización, es el guía y aprueba el proyecto de graduación.
Técnico informático	Ingeniero en computación	3 años de experiencia.	Colabora enormemente con su conocimiento en el proyecto, experimenta problemas.
Jefatura de IyD	Ingeniero químico.	7 años como encargado del departamento.	Colabora con sus conocimientos en el proyecto, encargado de recolectar información, graficar y además ofrecer soluciones para resolver el problema.
Colaboradores de CENECOOP R.L.	Operadores de servicios.	En conjunto más de 20 años de experiencia.	Usuario que vive el día a día en la organización,

			utiliza cada uno de los servicios que se brindan.

Fuente: elaboración propia.

3.3 Técnicas y herramientas de recolección de datos

La recolección de datos consiste en recoger los datos pertinentes sobre los atributos, conceptos o variables de las unidades de análisis o casos (participantes, grupos, organizaciones, étcetera), implica elaborar un plan detallado de procedimientos que nos conduzcan a reunir con un propósito específico, este plan incluye:

a) ¿Cuáles son las fuentes de donde se obtendrán los datos? Es decir, los datos van a ser proporcionados por personas, se producirán de observaciones o se encuentran en documentos, archivos, bases de datos, etcétera.
b) ¿En dónde se localizan tales fuentes? Regularmente en la muestra seleccionada, pero es indispensable definir con precisión.
c) ¿A través de qué medio o método vamos a recolectar los datos? Esta fase implica elegir uno o varios medios y definir los procedimientos que utilizaremos en la recolección de los datos. El método o métodos deben ser confiables, válidos y objetivos.
d) Una vez recolectados, ¿de qué forma vamos a prepararlos para que puedan analizarse y respondamos al planteamiento del problema? (Sampieri et al., 2003)

Para la recolección de datos se necesita una gran diversidad de técnicas y herramientas que el investigador pueda utilizar para desarrollar de una mejor manera la solución a cada uno de los servicios críticos de la empresa, todos los instrumentos se aplican en un momento determinado de la investigación, con la finalidad de obtener la información en el instante preciso, las técnicas de recolección de datos usadas en este trabajo son:

- ✓ Entrevista.
- ✓ Encuesta.
- ✓ Observación.
- ✓ Documentos (normas y registros).
- ✓ Lluvia de ideas.

3.3.1 **Entrevista**

Para Sampieri, Fernández, & Baptista (2010), una entrevista es una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (entrevistado) u otras (entrevistados). Al hablar de entrevistados se refiere a una pareja o un grupo pequeño como una familia. Por su parte (Obando, 2012), hace hincapié en que la entrevista es un proceso de obtención de información oral que se da dentro de una situación cara a cara, en donde la información no solo se transmite en un solo sentido, sino que en ambos. Este tipo de enfoques se aplican directamente con la jefatura de TI y de los servicios críticos en la cooperativa (ver tabla 2 y tabla 3), con el fin de obtener información importante sobre el plan de continuidad del negocio en el Centro de Estudios y Capacitación Cooperativa, CENECOOP R.L, de esta forma se puede dimensionar el plan. (Ver apéndice 1.1)

Tabla 8 – Definición de cuestionario de entrevista a jefaturas de CENECOOP R.L.

Sección	Objetivo del cuestionario	Descripción
Pregunta 1	Conocer el tamaño que implica el plan de continuidad del negocio.	¿Cuántas sucursales tiene CENECOOP R.L.?
Pregunta 2	Identificar el conocimiento de empleados de los altos rangos en tema de BCP.	¿Considera que es el plan de continuidad del negocio para TI es la mejor opción para la productividad en caso de una interrupción en la organización?
Pregunta 3	Conocer la perspectiva que poseen los altos mandos del plan de continuidad del negocio.	¿Tiene la empresa (sucursales) un plan de continuidad del negocio?
Pregunta 4	Conocer todas las funciones realizadas por Centro de Estudios y así categorizar cada uno.	¿Qué tan probable un servicio falla a la semana en la empresa CENECOOP R.L.?

Pregunta 5	Conocer las referencias críticas donde pueden estar los problemas más críticos en los servicios de la empresa y adaptarlo al BCP.	¿Cuánto tiempo espera generalmente al momento de interrupción en algún servicio crítico de la organización?
Pregunta 6	Analizar como los empleados evalúan los servicios ofrecidos por la institución académica.	¿Marque con una "X" de acuerdo a la escala que se brinda más adelante la disponibilidad de los servicios del Centro de Estudios según considere? (siendo 1 la más baja y 10 la más alta)

Fuente: elaboración propia.

3.3.2 **Encuesta**

Se considera la primera instancia, como una técnica de recogida de datos a través de la interrogación de los sujetos cuya finalidad es la de obtener de manera sistemática medidas sobre los conceptos que se derivan de una problemática de investigación previamente construida. La recogida de los datos se realiza a través de un cuestionario, instrumento de recogida de los datos (de medición) y la forma protocolaria de realizar las preguntas que se administra a la población o una muestra extensa de ella mediante una entrevista donde es característico el anonimato del sujeto. (López & Fachelli, 2015)

Esta herramienta se aplica a todas las jefaturas de CENECOOP R.L. para medir la satisfacción que tiene con los servicios que actualmente se ofrecen, así como la página web. La encuesta es del tipo mixta, ya que es necesario ponderar satisfacciones. (Ver apéndice 1.1)

3.3.3 **Observación**

Este método de recolección de datos consiste en el registro sistemático, válido y confiable de comportamientos y situaciones observables, a través de un conjunto de categorías y subcategorías. En la investigación cualitativa necesitamos estar entrenados para observar y es diferente de

simplemente ver (lo cual hacemos cotidianamente). Es una cuestión de grado. Y la "observación investigativa" no se limita al sentido de la vista, implica todos los sentidos. (Sampieri et al., 2010)

Dicha técnica se emplea al visitar los departamentos y visualizar los diferentes servicios que se brindan en cada uno de ellos, también se observa el funcionamiento de los diferentes sistemas de software por los usuarios finales de la compañía.

3.3.4 **Documentos y registros**

Es una fuente muy valiosa de datos cualitativos, se incluyen: documentos, materiales, artefactos diversos, ayudan a entender el fenómeno central de estudio prácticamente la mayoría de las personas, grupos, organizaciones, comunidades y sociedades los producen y narran, o delinean sus historias y estatus actuales. Le sirven al investigador para conocer los antecedentes de un ambiente, así como las vivencias o situaciones que se producen en él y su funcionamiento cotidiano y anormal. (Sampieri et al., 2010)

Está técnica consiste en revisar el Índice de Gestión Institucional (IGI) de la Contraloría General de la República de la Cooperativa de los años anteriores, además las evaluaciones realizadas por las jefaturas de periodos anteriores para verificar el grado de satisfacción por parte de los usuarios con los sistemas y/o servicios del Centro de Estudios que involucran directamente el departamento de TI, es importante analizar estos datos y sacar conclusiones al respecto.

3.3.5 **Lluvia de ideas**

De las diversas reuniones y encuestas que se obtienen con las jefaturas de TI como de Investigación y Desarrollo, se realiza una lluvia de ideas para seleccionar las preguntas más determinantes (servicios críticos) y las tentativas solvencias a dichos problemas, esta técnica permite representar de una mejor forma las preguntas planteadas.

3.4 Variable

Tabla 9 – Variables

Objetivo específico	Variable	Definición conceptual	Indicador	Medida	Tipo de variable	Instrumento
Analizar la situación actual, vulnerabilidades, período de recuperación y tiempo máximo de interrupción presentes en la situación actual de la empresa CENECOOP R.L. en materia del plan de continuidad del negocio mediante los análisis FODA;	Situación actual de la empresa en materia del plan de continuidad del negocio. Vulnerabilidades, tiempo de recuperación, tiempo de interrupción, FODA, PESTEL y matrices para la determinación de riesgos.	Contexto actual en el cual se encuentra CENECOOP R.L en cuanto al desarrollo de un BCP.	Procedimientos existentes en la empresa en materia del plan de continuidad del negocio.	Listado de procedimientos establecidos en la empresa.	Cualitativa.	Encuesta.
			Cantidad de actividades y/o procesos implementados en los departamentos de la organización referentes al BCP.	Existen – Sí - o - No.	Cuantitativa.	Encuesta a los encargados de las áreas de la empresa (ver apéndice 1.2).

PESTEL y matrices para la determinación de los riesgos.			Cantidad de riesgos representantes en los procesos críticos de la organización aplicando alguna herramienta para la gestión.	Identificaciones obtenidas por matrices de riesgos.	Cuantitativa.	Matriz comparativa, matriz de riesgos para proyectos y semáforo de riesgos. Matriz de riesgos definido en la Norma Australiana.
Definir los servicios críticos del Centro de Estudios que no pueden ser interrumpidos para mantener la continuidad del negocio con la aplicación de la ISO 22301:2012 (Norma Internacional para la	Servicios críticos de la empresa que no pueden ser interrumpidos para mantener la continuidad del negocio. ISO 22301:2012, Good Practice Guidelines.	Aquellos procesos y funciones de la empresa que deben ser restaurados en caso de ser interrumpidos con el propósito de garantizar el	Criterios de importancia que impactan los procesos y puestos de la organización.	Se enumeran servicios críticos según resultados.	Cualitativa	Entrevistas con las jefaturas de cada área de la empresa. Y resultados obtenidos en el último Índice de Gestión Institucional de la CGR.

Gestión de la Continuidad de Negocio) y Good Practice Guidelines (GPG) apartado de la norma ISO.		flujo normal de la empresa.	Porcentaje de ingresos y pérdidas de acuerdo con servicios brindados en la actualidad.	Total de ingresos - Gastos = Utilidad o pérdida de CENECOOP R.L.	Cuantitativa	Análisis de información (estados financieros auditados en último año).
			Tiempos necesarios para reiniciar los sistemas críticos en la cooperativa.	(De 10 a 30 min, de 31 a 59 min, de 1 a 3 h, y más de 3 h.).	Cuantitativa.	Encuesta (ver apéndice 1.1).
Desarrollar la propuesta del plan de continuidad del negocio con las mejores prácticas para adaptarlos a la compañía	Plan de continuidad del negocio para la empresa. Aplicación de norma NFPA 1600 y COBIT 5.	Propuesta donde se especifican los aspectos básicos para la implementación de un plan de	Cantidad de requisitos aplicables en CENECOOP R.L.	Valoración de riesgos.	Cualitativa	Norma NFPA 1600.

CENECOOP R.L con la implementación de la norma NFPA 1600 y COBIT 5.		continuidad del negocio.	Cantidad de requisitos aplicables a la empresa según normativa.	Lista de estrategias definidas.	Cuantitativa.	Requerimientos según INTE/ISO 22301:2012. Análisis de información.
			Porcentaje de cobertura de los riesgos altos presentes en la organización.	Creación de plan para prevención y recuperación de riesgos.	Cuantitativa.	Guía práctica para PYMES: cómo implementar un BCP de INTECO y Deloitte, análisis de información.

Fuente: elaboración propia.

3.5 **Diseño de la investigación**

Una vez que se ha definido el tipo de estudio a realizar y establecido las hipótesis de investigación o los lineamientos para la investigación, el investigador debe concebir la manera práctica y concreta de responder a las preguntas de investigación. Esto implica seleccionar o desarrollar un diseño de investigación y aplicarlo al contexto particular de su estudio. El diseño señala al investigador lo que debe hacer para alcanzar sus objetivos de estudio, contestar las interrogantes que se ha planteado y analizar la certeza de las hipótesis formuladas en un contexto en particular. (Sampieri et al., 2010)

En esta sección del documento se muestra el proceso que conlleva el trabajo de investigación, a continuación, se detallan las etapas y fases del proyecto, indicando las técnicas y herramientas empleadas por etapa, además de los resultados esperados.

Etapa 1 Investigación – Identificación de las actividades que deben ser realizadas de forma previa. Elaboración de la política de continuidad del negocio que determine los objetivos y el alcance. Planificar el proyecto, programar y desarrollar el plan de trabajo el cual debe satisfacer los objetivos planteados en la política.

- Técnica 1 – Entrevista: se emplea está técnica para conocer como está actualmente los servicios brindados por CENECOOP R.L, tanto los servicios que se dan en sitio como virtuales.
- Técnica 2 – Encuesta: la idea principal de aplicar una encuesta a las jefaturas del Centro de Estudios es conseguir antecedentes del conocimiento que poseen en temas relacionados al plan de continuidad de negocio y cuál es la satisfacción del usuario final.
- Técnica 3 – Observación: está técnica se aplica con el objetivo de obtener datos de los servicios en general que da la institución, así como la manipulación que los empleados realizan en ellos.

Etapa 2 Análisis de riesgos – Identificar los servicios claves de la empresa y los riesgos a los que están expuestos. Examinar los servicios críticos de la empresa estimar el impacto u las consecuencias de los posibles fallos en esos servicios, reconocer y valorar los riesgos que puedan interrumpir la continuidad del negocio.

- ❖ Técnica 4 – Documentos y registros: se corroboran documentos y registros existentes para obtener información del software empleado.

Etapa 3 Medidas preventivas – Se implementan medidas de seguridad preventivas y proactivas para evitar o gestionar los incidentes graves. La empresa debe identificar y aplicar controles o medidas de seguridad que:

- Reducir la probabilidad de que las actividades críticas sufran interrupciones.
- Disminuir el tiempo de una eventual interrupción.
- Limitar el impacto que una paralización de las actividades críticas pueda provocar en la organización.
- Incrementar la fortaleza del negocio mediante la eliminación de puntos de fallo únicos.

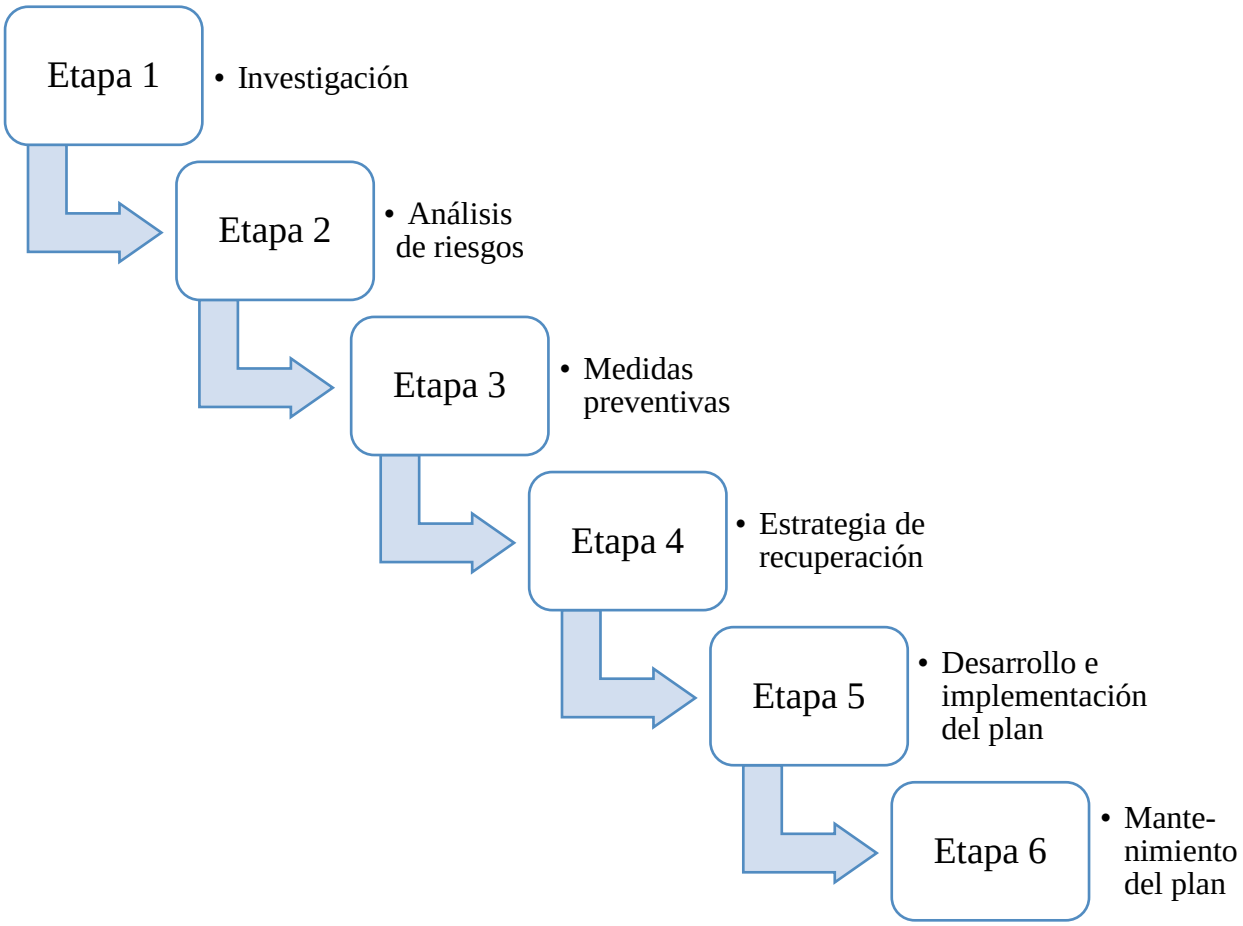
- ❖ Técnica 5 – Lluvia de ideas: es aplicada con el fin de obtener diferentes soluciones a las reuniones provenientes de las jefaturas respectivas, además para sintetizar de una mejor manera las opiniones expuestas.

Etapa 4 Estrategia de recuperación – La idea principal es establecer objetivos y prioridades de recuperación en función de los riesgos que impactan en las operaciones del negocio. La organización debe tener en cuenta los posibles daños potenciales a la hora de revisar y seleccionar las diferentes soluciones o alternativas de recuperación de sus actividades prioritarias.

Etapa 5 Desarrollo e implementación del plan – En esta etapa se dan todos los procedimientos a seguir para la recuperación de la de las operaciones críticas después de producirse un desastre. Se deben definir los equipos necesarios para la activación y ejecución del plan de continuidad de negocio. Se desarrollan los procedimientos de alerta y actuación, se dispone de los medios y recursos necesarios para ejecutar el BCP.

Etapa 6 Mantenimiento del plan – En dicha etapa se entrega el producto final a la empresa, el plan de continuidad del negocio como tal, los resultados obtenidos son expuestos al coordinador de TI de CENECOOP R.L, es importante aclarar que el mantenimiento una vez que sea terminado es tan vital como mismísimo plan de contingencia.

Figura 7 – Flujo de las etapas del proyecto



Fuente: elaboración propia.

3.6 **Matriz de coherencia**

En la siguiente tabla se puede visualizar la relación entre los objetivos, los entregables, instrumentos y los temas del marco teórico con el fin de ordenar y entender de mejor forma el proceso metodológico de esta investigación.

Tabla 10 – Relación matriz de coherencia

Objetivo	Entregable	Fase	Técnicas	Temas
Analizar la situación actual, vulnerabilidades, período de recuperación y tiempo máximo de interrupción presentes en la situación actual de la empresa CENECOOP R.L. en materia del plan de continuidad del negocio mediante los análisis FODA; PESTEL y matrices para la determinación de los riesgos.	Análisis de vulnerabilidades y riesgos más críticos de la organización. Prevención de desastres.	Investigación. Análisis de riesgos.	Encuesta (lluvia de ideas). Documentos y registros.	• Plan de continuidad. • Marco de trabajo. • Ciclo PHVA. • Riesgos. • Gestión de riesgos. • Identificación de riesgos. • Identificación de amenazas. • Identificación de vulnerabilidades.
Definir los servicios críticos del Centro de Estudios que no pueden ser interrumpidos para mantener la continuidad	Definir alcance, políticas, requisitos, estrategias de mitigación.	Análisis de riesgos. Medidas preventivas.	Entrevista.	• Seguridad de la información. • Pilares de seguridad de la información. • Confidencialidad. • Integridad.

del negocio con la aplicación de la ISO 22301:2012 (Norma Internacional para la Gestión de la Continuidad de Negocio) y Good Practice Guidelines (GPG) apartado de la norma ISO.	Definir procedimientos, análisis de impacto, informe de incidencias.			• Disponibilidad. • Controles de seguridad de la información. • ISO 27002. • Controles de seguridad físicos. • Controles de seguridad lógicos. • Sistema de gestión de seguridad de la información. • Sistema de gestión de continuidad del negocio. • ISO 22301. • Good Practice Guidelines. • Objetivo del SGCN. • Amenazas naturales. • Amenazas de agentes externos. • Amenazas de agentes internos.
Desarrollar la propuesta del plan de continuidad del negocio con las mejores prácticas para	Desarrollo del plan de continuidad del negocio.	Estrategias de recuperación.	Observación. Documentos y registros.	• COBIT 5. • Modelo de referencia de procesos de COBIT 5.

adaptarlos a la compañía CENECOOP R.L con la implementación de la norma NFPA 1600 y COBIT 5.	Revisión del plan con coordinadores encargados. Propuesta de mejora utilizando las pautas de buenas prácticas. Presentación de informe y propuesta del plan de continuidad del negocio.	Desarrollo e implementación del plan. Mantenimiento del plan.		• Norma NFPA 1600. • Recuperación de desastres. • Análisis de impacto sobre el negocio (BIA).

Fuente: elaboración propia.

La tabla anterior entrelaza todo el marco teórico con los objetivos del proyecto de esta forma solventa la necesidad del plan de continuidad del negocio.

CAPITULO IV
DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

4.1 Situación actual

El presente capítulo tiene como finalidad identificar claramente el proceso de diagnóstico de la cooperativa y determinar el ámbito en que se desarrolla. Además, se analiza el diagnostico que actualmente presenta el CENECOOP R.L, en términos de la infraestructura de TI.

La labor de un diagnóstico se define como: “un estudio previo a toda planificación o proyecto y que consiste en la recopilación de información, su ordenamiento, su interpretación y la obtención de conclusiones e hipótesis. Consiste en analizar un sistema y comprender su funcionamiento, de tal manera de poder proponer cambios en el mismo y cuyos resultados sean previsibles.” (Rodríguez, 2007)

De acuerdo con lo anterior y enmarcando la situación en el CENECOOP R.L., se reconoce que mediante el diagnóstico aplicado se permitirá brindar a la organización una proximidad, a la realidad que existe en la institución, todo esto con el objetivo de identificar los mecanismos que requieren mayor atención a fin de garantizar satisfactoriamente su debida gestión y funcionamiento. Los elementos que incluyen este diagnóstico son:

- Administrativo: es un estudio sistemático en TI, que tiene como propósito conocer la organización administrativa de las jefaturas de acuerdo con entrevistas y el funcionamiento del área objeto de estudio con la finalidad de detectar las causas y efectos de los problemas administrativos de la cooperativa. Las etapas que dividen al diagnóstico administrativo del proyecto son: políticas internas de seguridad, documentos existentes, e intranet interna.
- Técnico: es la revisión de infraestructura física y lógica a nivel de TI en CENECOOP R.L., se detalla en el inventario físico los equipos por área (computadoras e impresoras), servidores y dispositivos de red. En el inventario lógico se abarcan tres importantes datos como lo son: seguridad informática, servidores en la nube, enlace de internet y sistemas operativos.
- Percepción: en este tipo de diagnóstico se analizan los resultados de las herramientas de aplicación (entrevistas y encuestas), se deben de plasmar los resultados obtenidos a partir de la respuesta de los empleados o personas que estuvieron relacionadas con dichas aplicaciones. Las entrevistas se realizaron a las diez jefaturas de la cooperativa, se detallan las cuatro preguntas más sobresalientes. Para la sección de la encuesta se

utilizó la herramienta de Microsoft llamada Forms, donde se le envío un enlace a los 27 empleados de la compañía para que completaran la encuesta, todo el análisis se muestra en dicha sección.

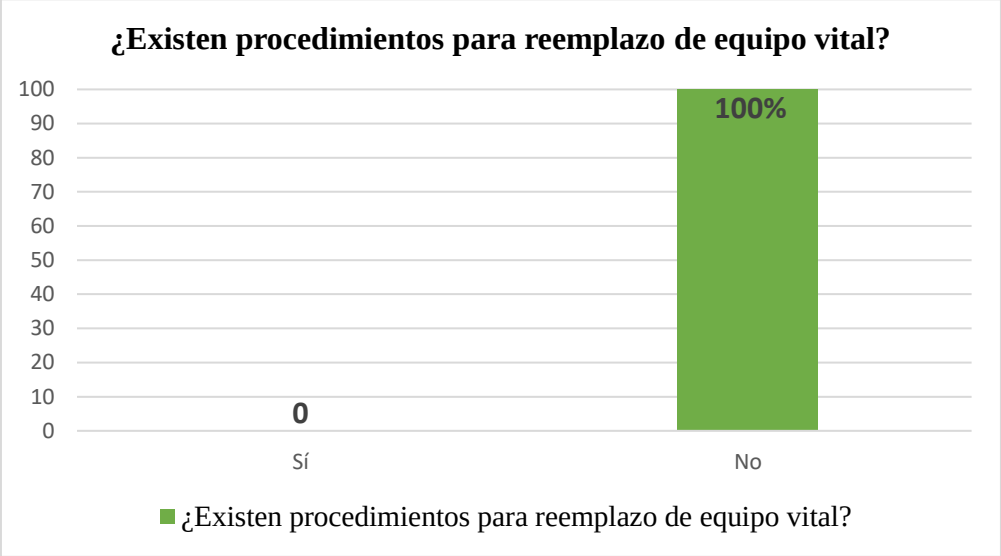
- Conclusiones: se obtienen las brechas finales del diagnóstico donde se ve el impacto negativo que genera el no tener un plan de continuidad de negocio, se revelan los problemas potenciales de la organización en el departamento de TI y de esta manera se determina como las distintas conclusiones implican en como se debe constituir para fundamentar el proyecto.

4.2 Diagnóstico administrativo

Se consulta a las jefaturas sobre el conocimiento en materia del plan de continuidad del negocio, aplicando entrevistas en sitio a un total de cuatro personas, que son las jefaturas más importantes del Centro de Estudios y Capacitación Cooperativa CENECOOP R.L, se obtiene que la probabilidad de que las jefaturas conozcan lo que es un plan de continuidad del negocio es de un 25%, donde solamente la jefatura de Tecnologías de Información tenía conocimiento acerca del tema.

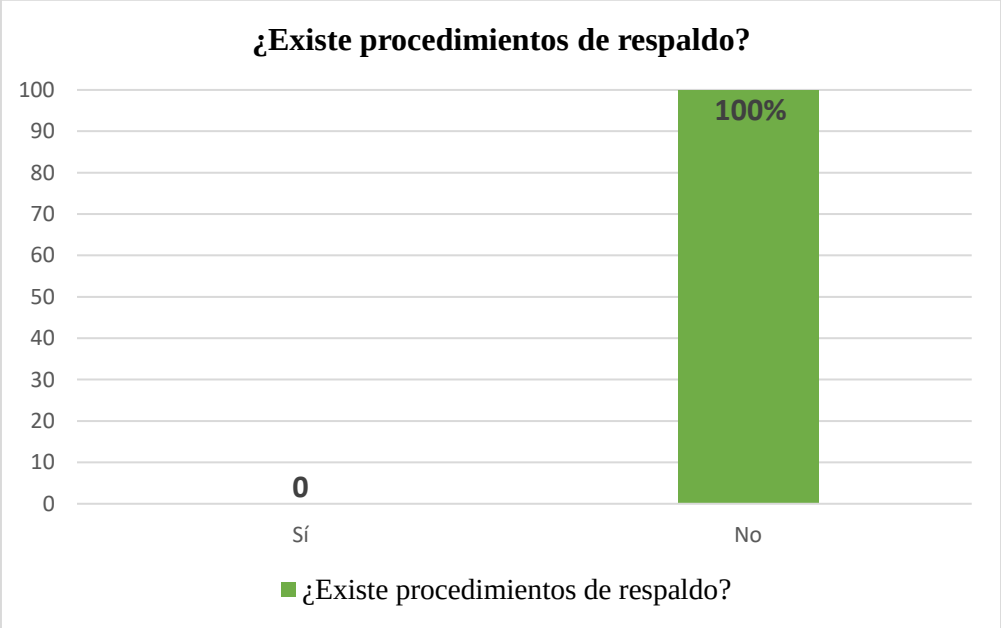
Existencia de procedimientos: como se observa en los siguientes gráficos indican que el 100% del personal de la empresa manifiesta que actualmente no se cuentan con procedimientos establecidos que indiquen la existencia de un plan de continuidad del negocio implementado por CENECOOP, ni procedimientos que indiquen como proceder en caso de que alguno de los procedimientos de trabajo actuales falle y signifiquen un verdadero riesgo de continuidad en operaciones para el Centro de Estudios.

Gráfico 1 – Existen procedimientos de reemplazo en CENECOOP R.L.



Fuente: elaboración propia.

Gráfico 2 – Existen procedimientos de respaldo en CENECOOP R.L.



Fuente: elaboración propia.

4.2.1 **Políticas internas de seguridad**

Recientemente la cooperativa ha realizado un manual de políticas de TI, debido a las constantes fallas que se dan en sus sistemas, el mismo se realizó en enero del 2020 por la auditoría interna en conjunto con la jefatura de TI y lleva de nombre "MANUAL DE POLITICAS DE TECNOLOGIAS DE INFORMACION ENERO 2020" donde se detallan todas las políticas que deben aplicarse en la organización, además se indica que cómo parte de las funciones del departamento de TI se actualice formalmente mínimo una vez cada dos años y cada modificación que se haga en las políticas debe ser autorizada por la auditoría interna e informada al Consejo de Administración del CENECOOP R.L.

4.2.2 **Documentos existentes**

Figura 8 – Pantallazo del documento de políticas internas de TI

LISTADO DE POLÍTICAS

En la siguiente tabla se detallan las políticas definidas y aprobadas, el número de página donde se puede ubicar dentro de este manual y la referencia al objetivo de control de las Normas Técnicas para la Gestión y El Control de las Tecnologías de Información (NTCGR).

NOMBRE DE POLÍTICA	No. PÁGINA	REFERENCIA NTCGR
PO-TI-001 – Uso de Recursos Tecnológicos		1.4 Gestión de la Seguridad de la Información
PO-TI-002 – Clasificación de la Información		1.4 Gestión de la Seguridad de la Información
PO-TI-003– Administración de Cuentas de Usuario y Contraseñas		1.4 Gestión de la Seguridad de la Información
PO-TI-004 – Uso de Correo Electrónico		1.4 Gestión de la Seguridad de la Información
PO-TI-005 – Uso del Internet		1.4 Gestión de la Seguridad de la Información
PO-TI-006 – Concienciación y Capacitación		1.4 Gestión de la Seguridad de la Información
PO-TI-007 – Seguridad Física y Ambiental		1.4 Gestión de la Seguridad de la Información
PO-TI-008 – Administración de Amenazas y Vulnerabilidades		1.4 Gestión de la Seguridad de la Información
PO-TI-009 – Manipulación y Destrucción de Datos		1.4 Gestión de la Seguridad de la Información
PO-TI-010 – Privacidad y Protección de la Información		1.4 Gestión de la Seguridad de la Información

Fuente: Mata, R. (2020). MANUAL DE POLITICAS DE TECNOLOGIAS DE INFORMACION ABRIL 2020. Recuperado de: **http://intranet.cene.coop/index.php/acceso**

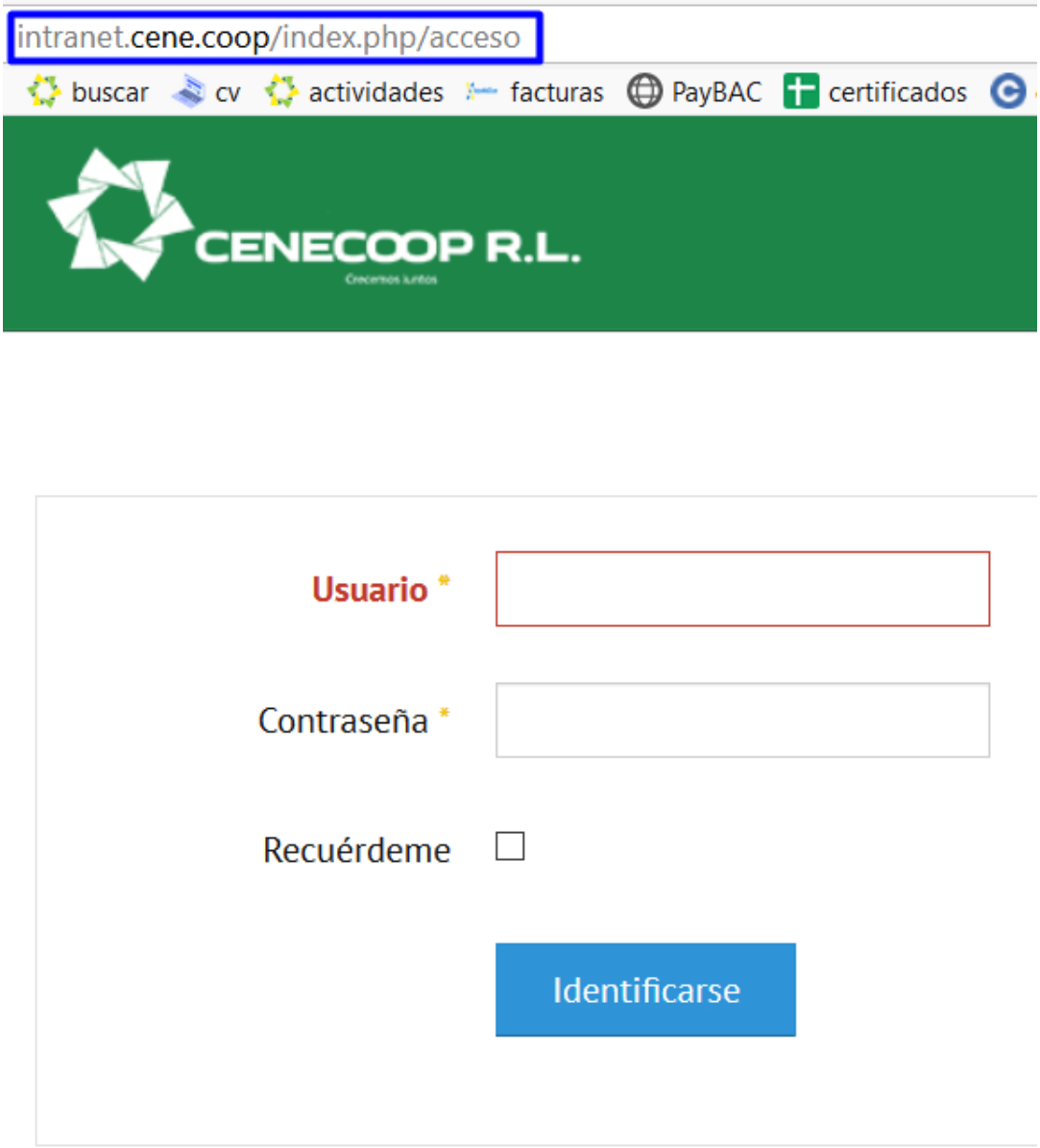
En la figura anterior se evidencia el documento para el departamento de Tecnología de la Información, es el auditor quién crea y pública dichas políticas en abril del presente año (2020) sin embargo en el archivo no se expresa en lo absoluto sobre la continuidad del negocio, no obstante, se solicita al coordinador de TI la necesidad del BCP y exigen que antes de diciembre de 2020, debe existir al menos una propuesta para la implementación del plan de continuidad del negocio.

4.2.3 **Intranet interna**

El Centro de Estudios y Capacitación Cooperativa utiliza una intranet donde todos los colaboradores de la cooperativa pueden comunicarse entre sí, una intranet es un sitio web interno generalmente restringido por IP, el objetivo principal es que la información que se almacena reside como objetivo asistir a los trabajadores en la generación de valor en la organización.

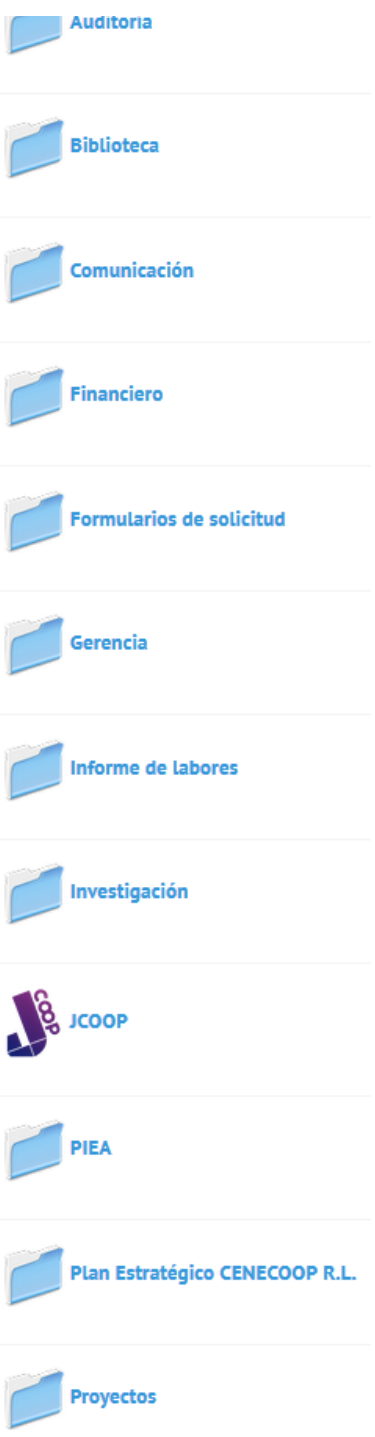
En CENECOOP R.L, la intranet se lo toman con la seriedad del caso, ya que poseen documentos realmente valiosos, todos los archivos se encuentran ordenados por carpetas y divididos por cada uno de los departamentos. Los documentos más sensibles no poseen ningún tipo de contraseña por lo que cualquier colaborador puede visualizarlo. A continuación, se detallan pantallazos.

Figura 9 – Captura del inicio de sesión a intranet de CENECOOP R.L



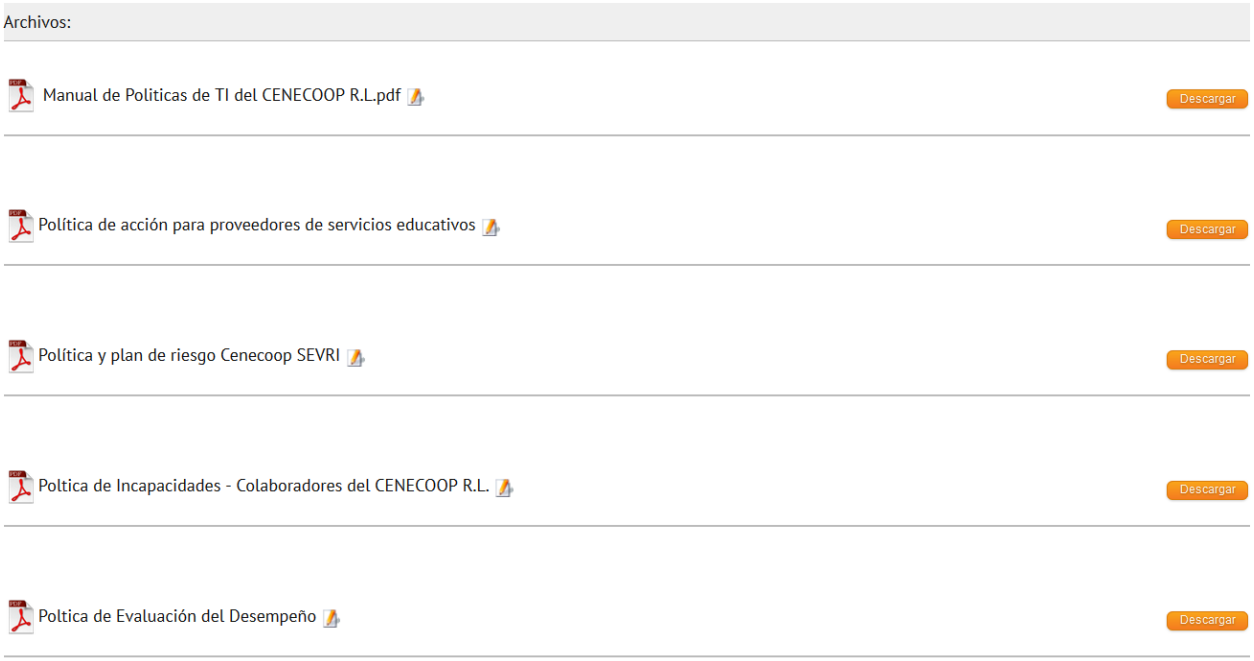
Fuente: Salazar, A. (2018). Intranet interna de CENECOOP R.L. Recuperado de: **http://intranet.cene.coop/index.php/acceso**

Figura 10 – Captura de carpetas en intranet de CENECOOP R.L



Fuente: Salazar, A. (2018). Documentos en intranet interna de CENECOOP R.L. Recuperado de: **http://intranet.cene.coop/index.php/cenecoop/documentos**

Figura 11 – Captura de visualización de documentos en intranet de CENECOOP R.L



Fuente: Salazar, A. (2018). Intranet interna de CENECOOP R.L. Recuperado de: **http://intranet.cene.coop/index.php/cenecoop/documentos/category/77-auditoria-interna**

Como se logra visualizar en las imágenes anteriores los documentos por más delicados que parezca no cuentan con algún tipo de cifrado en ellos, las únicas políticas de seguridad que se encuentran en ella es el manual de políticas internas de TI, en la intranet no hay modelos operativos, procedimientos ni mucho menos reglamentos internos.

4.3 Diagnóstico técnico

El departamento de TI de CENECOOP R.L, es un área clave ya que, tiene sus responsabilidades que básicamente se enfocan en cuatro campos que son: infraestructura, aplicativos, operaciones y servicio a los clientes internos como externos tales como: soporte a los empleados, servicios de red, mantenimiento preventivo y soporte a clientes de plataforma educativa.

4.3.1 Dispositivos físicos TI

La organización cuenta con una infraestructura de TI no tan robusta como debería tenerla, conformada por una red de fibra óptica de 85 megabytes, a la que se conectan 50 usuarios (todos locales). El hecho de analizar todos los componentes de hardware es importante para brindar una panorámica de la situación que se vive en la actualidad. Se analizarán los componentes de la

infraestructura física del Centro de Estudios y Capacitación Cooperativa R.L, dividiendo dicho análisis en servidores, computadoras, impresoras y teléfonos IP; se eligieron estos elementos porque son los que predominan en la empresa, además es más sencillo subdividir la categoría en estos elementos.

Cada tabla mostrará el estado del equipo, además de su capacidad de almacenamiento, procesamiento y demás especificaciones. El estado de los equipos se ha dividido en tres grandes categorías para poder clasificarlos y evaluarlos, a continuación, se adjunta la tabla de valoración:

Tabla 11 – Clasificación de los equipos de CENECOOP R.L.

Estado	Descripción
Malo	El funcionamiento de los equipos no es el indicado, sufren problemas de almacenamiento, capacidad de procesamiento, además se incluyen los equipos obsoletos por antigüedad y que presentan fallas constantes.
Normal	El funcionamiento es normal, pero se recomienda hacerles un mantenimiento preventivo y correctivo en ciertos momentos.
Bueno	Los equipos están aptos para su uso y reúnen las condiciones necesarias para funcionamiento adecuado.

Fuente: elaboración propia.

4.3.1.1 **Servidores**

Tabla 12 – Inventario de servidores de CENECOOP R.L.

Nombre	Núcleos	Procesador	RAM	Disco Duro	Sistema operativo	Tipo	Estado
VPS-SISMA	12	Intel® Xeon® CPU E52680 @ 2.40GHz	25.4 GB	1 TB	Windows Server 2012 R2	Virtual	Bueno
s10XX.sureserver.com	4	Intel® Xeon® Quad-Core 1.60GHz	8 GB	200 GB	Red Hat Linux	Virtual	Bueno

s10XX.sureserver.com	10	Intel® Xeon® @ 2.40GHz	32 GB	1 TB	Red Hat Linux	Virtual	Bueno
CENECOOP	8	Intel® Xeon® Quad-Core 1.60GHz	8 GB	512 GB	Windows Server 2012	Físico	Bueno

Fuente: elaboración propia con datos proporcionados por Alonso Salazar, Coordinador de TI de CENECOOP R.L.

La arquitectura de los servidores es de x86, actualmente posee 4 servidores (3 virtuales y 1 físico) que soportan diferentes aplicativos y procesos de la organización. Sin embargo, ninguno de ellos cuenta con ningún tipo de redundancia. Se realiza un respaldo de base de datos como de datos en los servidores virtuales, excepto en el físico, en ese no se realiza ningún tipo de procedimiento de backup ni mantenimiento.

4.3.1.2 **Computadoras**

Tabla 13 – Inventario de computadoras de CENECOOP R.L.

Departamento	**Tipo**	**Marca**	**Procesador**	**RAM**	**Disco duro**	**Sistema operativo**	**Estado**
Gerencia	Portátil	Dell	Intel i7	16 GB	1 TB	Windows 10	Bueno
	Portátil	HP	Intel i5	4 GB	512 GB	Windows 10	Bueno
	Portátil	Lenovo	Intel i5	8 GB	1 TB	Windows 10	Bueno
	Portátil	Lenovo	Intel i5	8 GB	1 TB	Windows 10	Bueno
Académico	Portátil	Lenovo	Intel i5	8 GB	1 TB	Windows 10	Bueno
	Escritorio	HP	Intel Core 2	2 GB	250 GB	Windows 7	Malo
	Escritorio	HP	Intel Core 2	2 GB	250 GB	Windows 7	Malo
Financiero	Escritorio	Dell	Intel i7	8 GB	1 TB	Windows 10	Bueno
	Escritorio	Dell	Intel i7	8 GB	1 TB	Windows 10	Bueno

	Escritorio	HP	Intel Core 2	2 GB	250 GB	Windows 7	Malo
Auditoría	Portátil	Lenovo	Intel i5	8 GB	1 TB	Windows 10	Bueno
Comunicación	Portátil	Lenovo	Intel i5	8 GB	1 TB	Windows 10	Bueno
IyD	Portátil	Mac	Intel i7	8 GB	1 TB	macOS Catalina	Bueno
TI	Escritorio	Dell	Intel i7	8 GB	1 TB	Windows 10	Bueno
	Portátil	Dell	Intel i5	8 GB	512 GB	Windows 10	Bueno
	Portátil	Dell	Intel i5	8 GB	512 GB	Windows 10	Bueno
	Portátil	Mac	Intel i7	8 GB	1 TB	macOS Catalina	Bueno
Proyectos	Portátil	Mac	Intel i7	8 GB	1 TB	macOS Catalina	Bueno
	Portátil	Dell	Intel i5	8 GB	512 GB	Windows 10	Bueno
	Portátil	Lenovo	Intel i5	8 GB	1 TB	Windows 10	Bueno
Juventud	Portátil	Surface	Intel i5	4 GB	256 GB	Windows 10	Bueno
	Portátil	Lenovo	Intel i5	8 GB	1 TB	Windows 10	Bueno
Asesoría legal	Escritorio	HP	Intel i3	4 GB	250 GB	Windows 7	Normal
	Portátil	Mac	Intel i7	8 GB	1 TB	macOS Catalina	Bueno

Fuente: elaboración propia con datos proporcionados por Alonso Salazar, Coordinador de TI de Cenecoop R.L.

Con la información recopilada, se resume que algunas computadoras como por ejemplo la de Asesoría Legal, dos de Académico y una de Financiero se encuentran obsoletas y con capacidades de almacenamiento y procesamiento limitadas, además es urgente realizar un mantenimiento preventivo y correctivo para minimizar los problemas que tienen actualmente como la falta de espacio en el disco duro, exceso de polvo en su interior, falta de memoria RAM. En cuanto al resto de computadoras se determina que su estado actual es normal, pero siempre es recomendable el mantenimiento preventivo y correctivo, ya que, ayuda a prolongar la vida útil del equipo.

4.3.1.3 **Impresoras**

Tabla 14 – Inventario de impresoras de CENECOOP R.L.

Cantidad	Marca	Modelo	Tipo	Estado
1	HP	400 MFP	Laser multifuncional	Normal
1	HP	Pro-8100	Multifuncional	Normal
2	HP	2050	Multifuncional	Normal
1	Epson	LX-350	Multifuncional	Normal
3	Epson	L805	Multifuncional	Bueno
1	Epson	L-380	Multifuncional	Bueno
1	Canon	--	Multifuncional	Malo

Fuente: elaboración propia con datos proporcionados por Alonso Salazar, Coordinador de TI de Cenecoop R.L.

Con respecto al cuadro anterior, se puede entender que, exceptuando la Canon, las demás impresoras se encuentran en condiciones adecuadas, las impresoras que lo permite están compartidas por direccionamiento IP. Más adelante en las brechas del diagnóstico, se indica de la posibilidad de alquiler de las impresoras, esto debido al alto gasto de consumibles y mantenimiento que podrían ahorrar al tratar con este método.

4.3.1.4 **Conexión a internet**

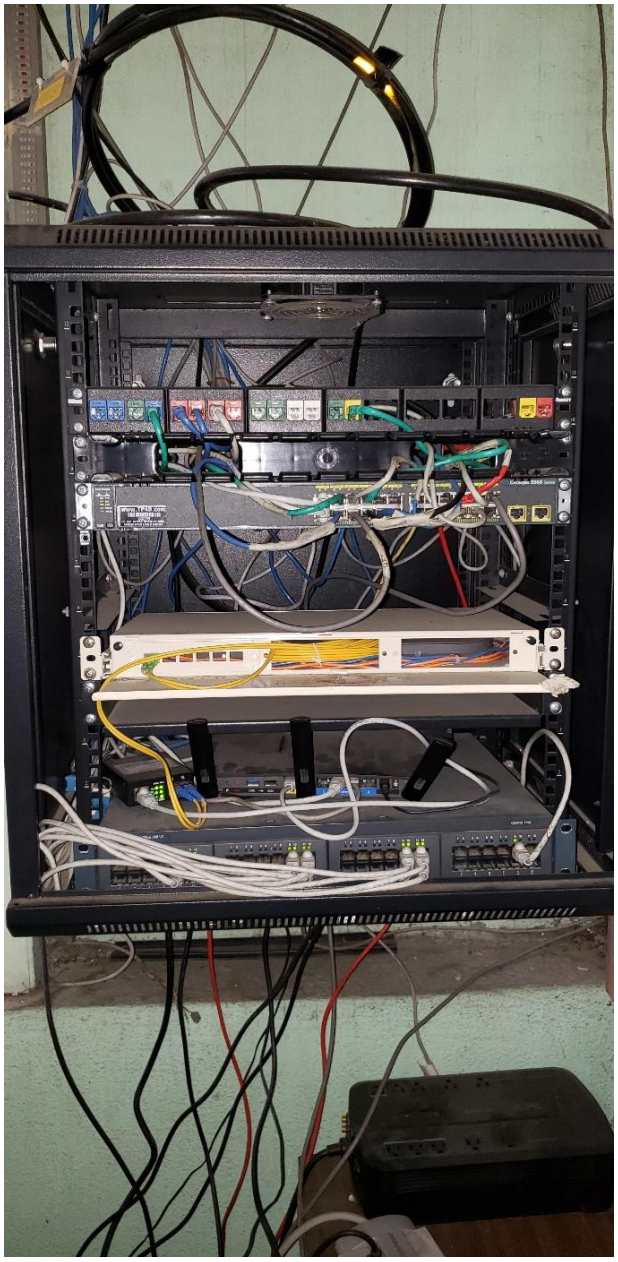
Tabla 15 – Conexión a internet de CENECOOP R.L.

Tipo de enlace	Velocidad	Proveedor	Estado
Fibra óptica	85 MB	ICE	Bueno

Fuente: elaboración propia con datos proporcionados por Alonso Salazar, Coordinador de TI de Cenecoop R.L.

El enlace de 85 MB es bueno, pero la queja de los empleados es constante, ya que la conexión a internet falla constantemente, afectando la labor de las personas. En la revisión que se realiza a toda la instalación de red, se logra visualizar que la mayoría de los departamentos tienen todos los puertos de red malos, por lo que adaptan un repetidor y conectan todas las máquinas directamente a él, tal y como se muestra en la siguiente figura.

Figura 12 − Rack principal de telecomunicaciones de CENECOOP R.L

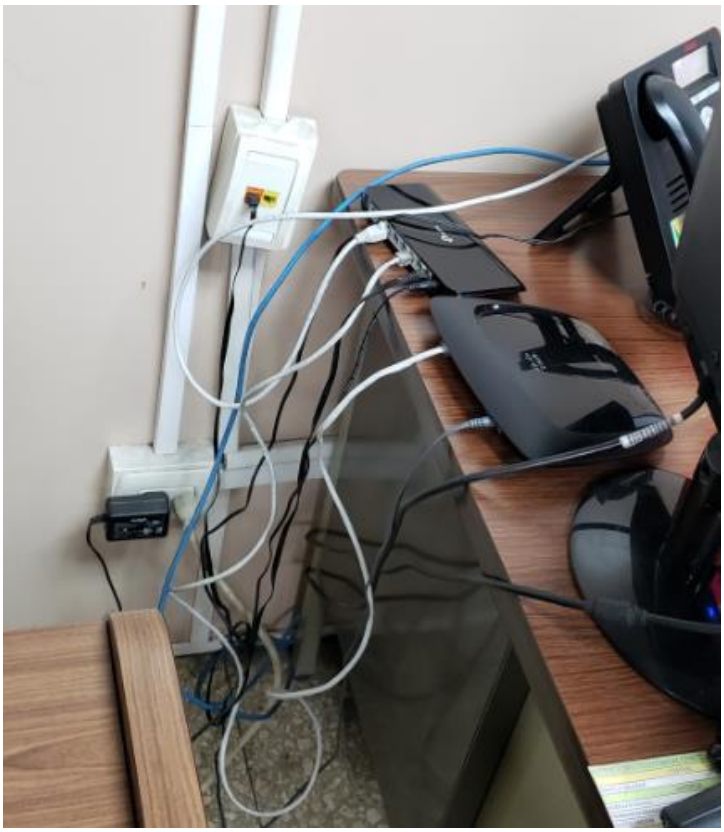


Fuente: Salazar, A. (2020). Cuarto de telecomunicaciones de CENECOOP R.L.

Se puede observar el desorden de cables, además de diferentes tipos de color sin ningún tipo de etiquetado, además el mantenimiento es mínimo en la imagen se puede visualizar mucho polvo en la superficie de los equipos, además todos los artefactos están conectados a una sola regleta y la misma no cuenta con UPS, por lo que al haber un corte de corriente los equipos se apagan de inmediato.

En el reconocimiento que se realiza en las instalaciones de la cooperativa, se logra visualizar que en casi todos los departamentos tienen los puertos de red malos, por lo que instalan repetidores y conectan los cables UTP directamente a él, tal como se muestra en la siguiente figura.

Figura 13 – Repetidor en departamento académico de CENECOOP R.L



Fuente: Salazar, A. (2020). Departamento académico en CENECOOP R.L.

En la figura anterior se muestra la falta de mantenimiento preventivo como correctivo que presentan los equipos de red en el Centro de Estudios y Capacitación Cooperativa R.L y es que según el coordinador de informática y asistente Mauriel Cabalceta Calderón en las entrevistas aseguran que en la cooperativa no tienen fechas definidas para hacer mantenimientos, sino que cada vez que falle algún equipo de red o alguna computadora de los colaboradores, se realiza la corrección inmediatamente; es frecuente que a los equipos pierdan el acceso a internet, ya que las configuraciones están obsoletas, las VPN actualmente están desconfiguradas y aún no se han reconectado.

Figura 14 – Equipos en departamento contable de CENECOOP R.L

.

Fuente: Salazar, A. (2020). Departamento financiero en CENECOOP R.L.

La mala instalación de los equipos en los puestos de trabajo es evidente, los cables están expuestos, enredados, no hay aseo por parte de los colaboradores tanto del área financiera como informática según la imagen anterior, además todo está conectado a una sola regleta, en la entrevista con Alonso Salazar Céspedes (coordinador de TI) le consulté acerca del escaso mantenimiento que se observa en cada departamento y él me comentó que el tiempo que cuenta para realizar estas funciones es mínimo, al mismo tiempo indicó que al delegar estas órdenes a los otros colaboradores expresan que actualmente se encuentran en otras funciones importantes por lo que están sobrecargados de trabajo, los empleados se molestan y el mantenimiento queda sin reparación hasta que ocurre la falla inminente en los equipos.

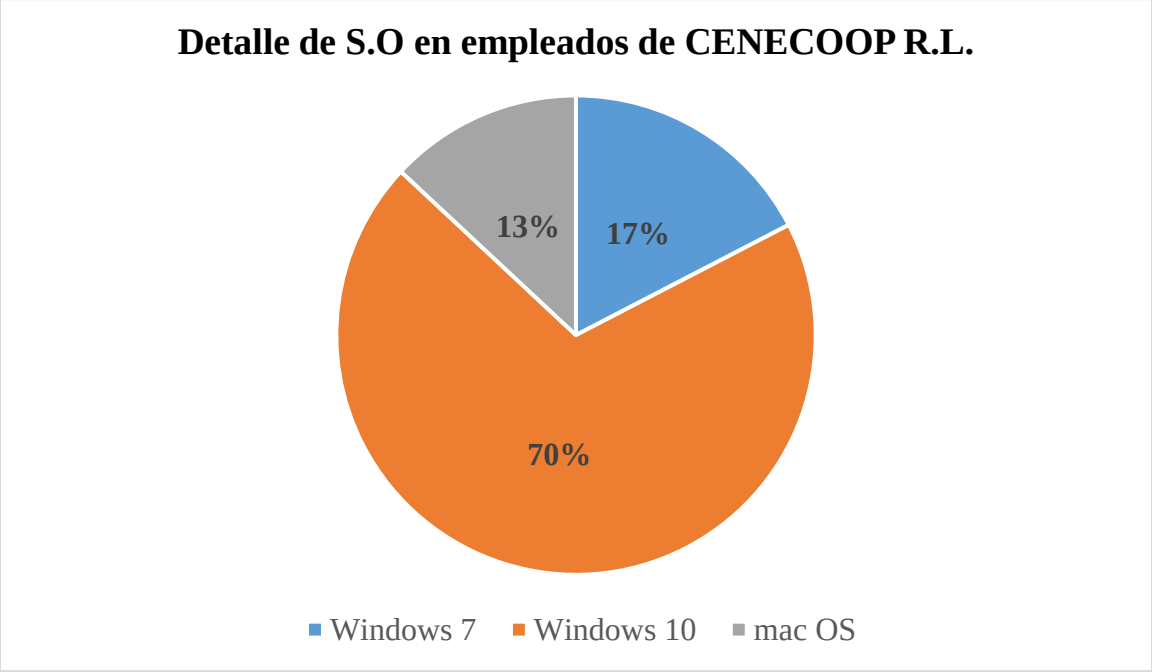
4.3.2 **Dispositivos lógicos TI**

En el diagnóstico lógico efectuado en el departamento de Tecnología de Información de la empresa CENECOOP R.L, se detecta los siguiente:

4.3.2.1 **Sistemas operativos de las computadoras**

La mayoría de los equipos poseen el sistema operativo Windows 10, pero también algunos equipos cuentan con Windows 7 y por último se cuenta con tres computadoras MacBook Pro, que utiliza macOS Catalina.

Gráfico 3 – Sistemas operativos de las computadoras de CENECOOP R.L



Fuente: elaboración propia.

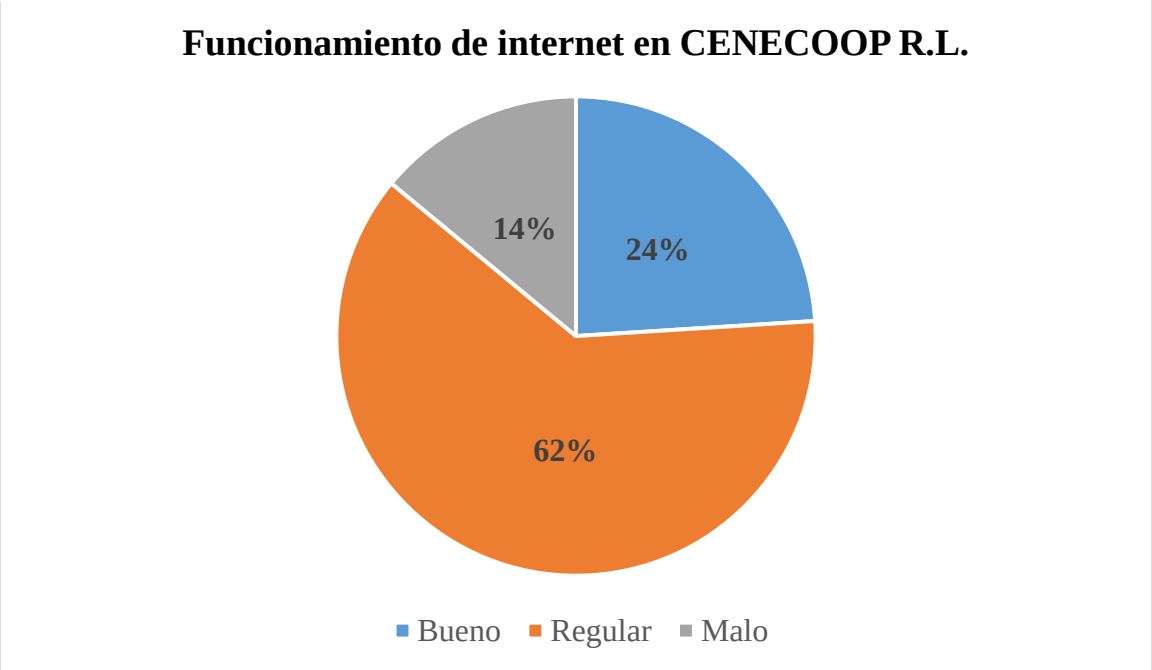
La idea de mostrar la gráfica es ver la dependencia que se tiene en CENECOOP R.L, con las empresas de software licenciado, porque en la cooperativa no utilizan ningún tipo de software libre.

Con respecto a los paquetes de ofimática utilizados, todos los equipos tienen versiones distintas de Microsoft Office, que van desde la 2010, hasta Office 365 y está situación debe ser regulada más estrictamente, ya que, en algunos casos las computadoras pasan tiempo sin activarle la clave de productos.

4.3.2.2 **Conexión a internet**

El enlace de fibra óptica de 85 MB funciona a la perfección, sin embargo, según mencionan los empleados que laboran dentro de la cooperativa, el internet es inconsistente, fallando la mayoría de los días por motivos como: la desconexión o interrupción del fluido eléctrico.

Gráfico 4 – Funcionamiento del internet de CENECOOP R.L



Fuente: elaboración propia.

Con el estudio del gráfico anterior podemos determinar la opinión de los funcionarios, ya que la mayoría indica que el internet es regular y no responde a las expectativas de los empleados, la queja más notaria es que se cae la conexión y dura unos minutos en volver a reestablecerse.

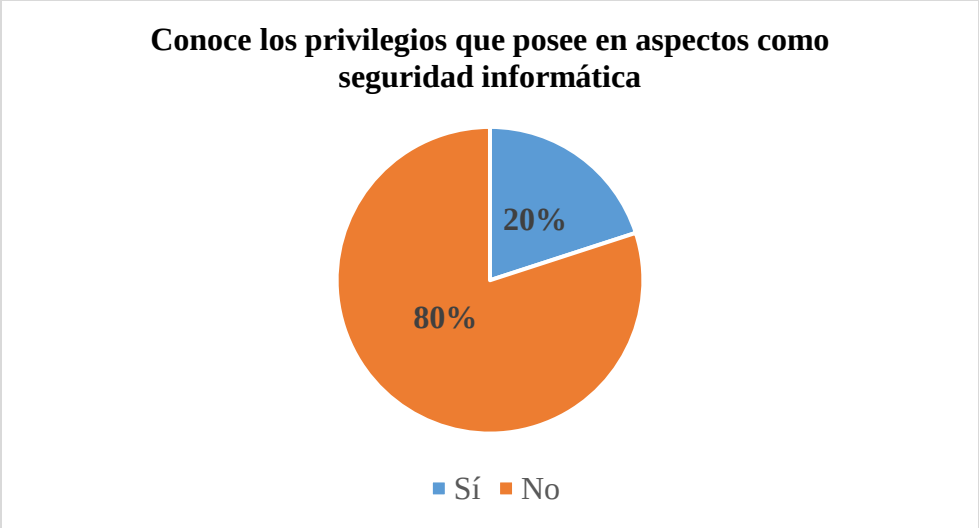
Se debe ir pensando en vías redundantes que se pueden prever para el futuro, ya que sí el enlace de fibra óptica actual falla la cooperativa no puede seguir laborando. Se le hizo la consulta al encargado de TI, Alonso Salazar y expresó lo siguiente: “Compañero sinceramente cuando yo llegué a CENECOP en el año 2014, la red ya estaba hecha, sin embargo, eso es una telaraña por que el enlace principal va a un switch del departamento académico para iniciar ahí la distribución a los demás departamentos y no tengo idea porqué, desde entonces no se le ha dado mantenimiento a la red y eso sigue igual”.

4.3.2.3 **Seguridad informática**

En el Centro de Estudios y Capacitación Cooperativa R.L, laboran alrededor de 27 personas, de todas ellas la mayoría tienen funciones administrativas; cada departamento cuenta con su propio personal, su equipo de cómputo y sus herramientas para desarrollo de sus funciones.

Se realizó una consulta a los empleados sobre el conocimiento de los roles y limitaciones que tienen dentro de la red, en cuanto accesos a documentos, instalación de aplicaciones e incluso el uso de la red inalámbrica y es que la totalidad de los funcionarios no conocen sobre las medidas de seguridad con las que cuenta, tales como accesos, uso de equipo de cómputo.

Gráfico 5 – Privilegios en seguridad informática de CENECOOP R.L



Fuente: elaboración propia.

Además, en la identificación de funcionarios se identificó que la configuración en telecomunicaciones no tiene ningún tipo de configuración segura como VLAN por lo que la red sigue propensa a ataques cibernéticos y el acceso a documentos confiables que se manejan en la institución por el sistema web de la intranet interna se ve perjudicado ante una posible intrusión.

No se realizan ningún tipo de respaldo para las configuraciones base de switches, routers, firewall.

4.3.2.4 **Servidores**

Los servidores de aplicaciones no cuentan con redundancia, lo cual no garantiza la continuidad del negocio ante los clientes y los sistemas o aplicaciones que se encuentran instalados en ellos. Diariamente se realiza una copia de seguridad en cada una de las bases de datos y archivos que estás son guardadas en un sitio alterno de cada uno de los servidores, sin embargo, el mantenimiento que le dan a estos dispositivos es casi nula por diferentes motivos, el mayormente mencionado por la jefatura de TI es el poco tiempo y el recargo de tareas al departamento.

Todos los programas instalados en cada uno de los servidores cuentan con su respectiva licencia, no obstante, en estos equipos hay instalados aplicativos que no se utilizan por lo que esto puede ocasionar problemas de almacenamiento, memoria RAM e inclusive ataques cibernéticos, que, en este último aspecto, ya tuvieron un altercado en diciembre del año 2018, cuando el servidor Windows Server 2012 que tiene CENECOOP R.L en la nube fue hackeado y encriptada toda su información como también sus respectivas bases de datos SQL Server, ya que en el mismo no contaban con ningún tipo de software de defensa ante ataques de este tipo, desde entonces han tomado medidas no tan drásticas para combatir estas acometidas a los servidores virtuales donde está al momento han tenido éxito.

4.4 Diagnóstico de percepción

En el diagnóstico de percepción realizado en la cooperativa, efectuado por los resultados de las entrevistas y encuestas a los empleados de la organización, en este apartado se grafican los resultados realizadas por el investigador.

4.4.1 Entrevistas

La entrevista se aplica al coordinador de cada una de las áreas de la cooperativa asociado a los servicios que se desarrollan en cada una de ellas. La entrevista consta de 6 preguntas. A continuación, se exponen las 4 más relevantes para el diagnóstico de percepción:

1. ¿Considera que es el plan de continuidad del negocio para TI es la mejor opción para la productividad en caso de una interrupción en la organización?

Gráfico 6 – Importancia del Plan de Continuidad de Negocio para CENECOOP R.L

Fuente: elaboración propia.

De las 5 personas consultadas, en un 100% coinciden en que es necesaria la implementación de un plan de continuidad para mitigar riesgos y aumentar la productividad, así como mejorar el funcionamiento de la organización.

2. ¿Tiene la empresa (sucursales) un plan de continuidad del negocio?

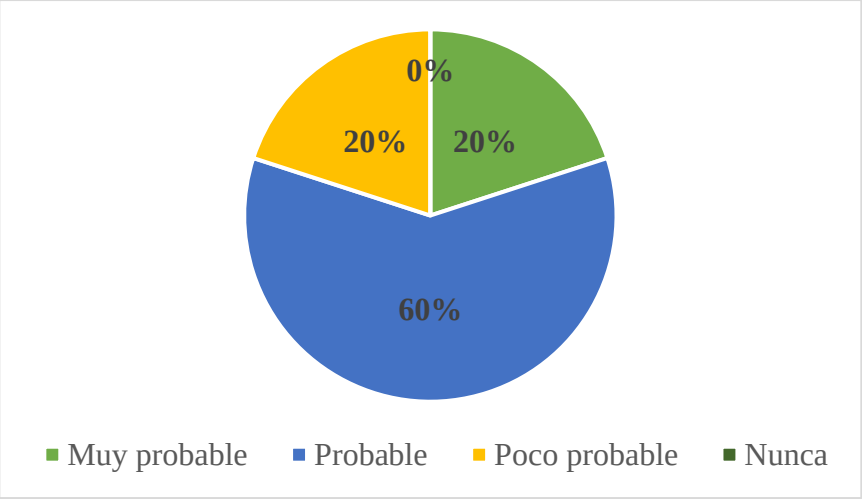
Gráfico 7 – Plan de Continuidad del Negocio en CENECOOP R.L.

Fuente: elaboración propia.

Todas las personas consultadas, el 100% indica que no existe un plan de continuidad de negocio en la cooperativa ni en las diferentes sucursales que tiene el Centro de Estudios y Capacitación Cooperativa R.L.

3. ¿Qué tan probable un servicio falla a la semana en la empresa CENECOOP R.L.?

Gráfico 8 – Fallas en los servicios de CENECOOP R.L.

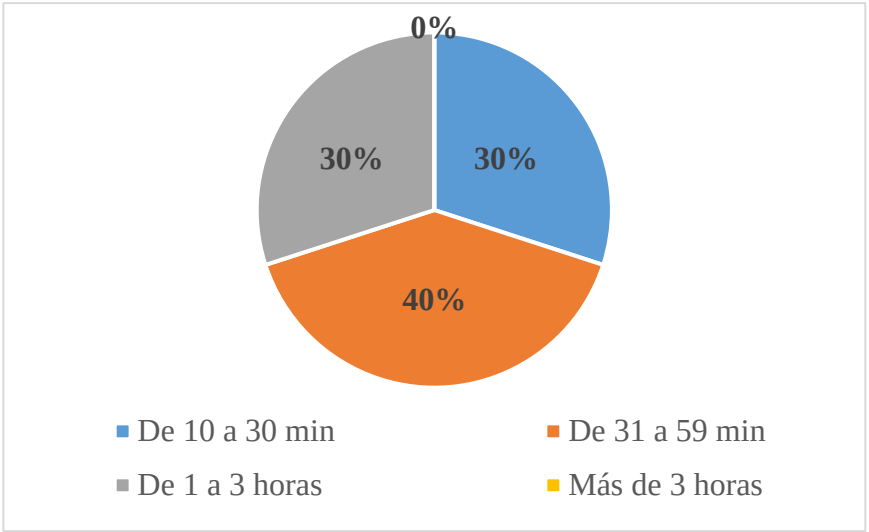


Fuente: elaboración propia.

Cuando se les consulta que tan frecuente un servicio falla en la empresa, 4 entrevistados contestan de manera afirmativa que es probable o muy probable que los servicios se vean interrumpidos semanalmente y 1 responde que es poco probable, esto muestra la importancia que puede llegar a tener un plan de continuidad en la cooperativa.

4. ¿Cuánto tiempo espera generalmente al momento de interrupción en algún servicio crítico de la organización?

Gráfico 9 – Tiempos en los servicios de CENECOOP R.L.



Fuente: elaboración propia.

Del 100% de las personas consultadas, el 80% señala que deben esperar de 10 a 30 minutos para que restablezcan el servicio en CENECOOP R.L y solo el 10% indica que espera de 31 a 59 minutos, además tres de los entrevistados denuncia que se produce un deterioro en la imagen de la organización. Nuevamente se ve evidenciado la insuficiencia que tiene la cooperativa en aspectos como la continuidad. En la sección 1.3 de los anexos se encuentran las respuestas de estas entrevistas.

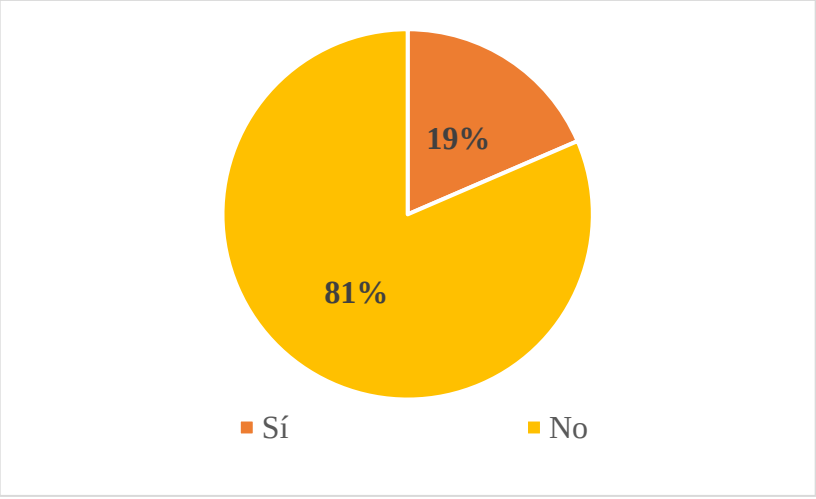
4.4.2 **Encuestas**

La encuesta se realizó vía web a todos los colaboradores de CENECOOP R.L, la empresa cuenta con un total de 27 empleados. Se grafican únicamente las preguntas más trascendentales relacionadas al plan de continuidad del negocio para CENECOOP R.L, todas las preguntas con sus respectivas respuestas se pueden visualizar desde el siguiente enlace: **clic aquí**.

Pregunta 1: "¿En su empresa o departamento hay implementado un plan de continuidad del negocio?". Los 27 encuestados de la cooperativa marcan que "No", lo cual demuestra la necesidad que tienen en temas de continuidad.

Pregunta 2: "¿Existen procedimientos o actividades de respaldo que realicen en caso de que sus procedimientos normales fallen, son procedimientos establecidos por la empresa?". El 81% de los colaboradores indican que no existe ningún tipo de procedimiento de respaldo ni mucho menos la empresa ha establecido políticas o protocolos a seguir, solo el 19% de ellos señala que existen procedimientos de respaldo.

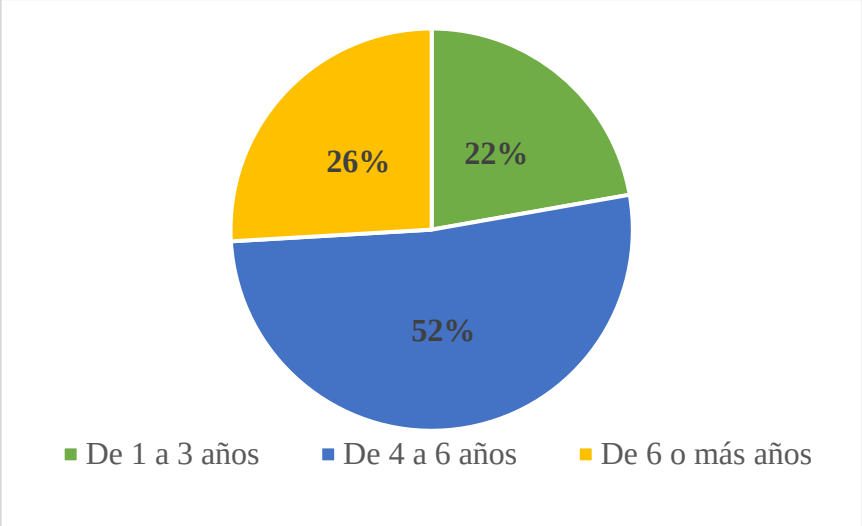
Gráfico 10 – Existencia de procedimientos de respaldo en CENECOOP R.L.



Fuente: elaboración propia.

Pregunta 3: “¿Hace cuántos años tiene su equipo de cómputo?”. En está pregunta se da una variedad de resultados, por tal motivo se grafica el resultado en la figura 8.

Gráfico 11 – Equipo físico de empleados en CENECOOP R.L.



Fuente: elaboración propia.

Pregunta 4: “¿Cuáles de sus funciones considera usted críticas, que en caso de no realizarse los demás procesos de la organización se pueden ver afectados, de ser este el caso que departamentos podrían ser afectados?”.

Se describen a continuación las respuestas más claras y concisas, sin embargo, es importante tomar en consideración que algunos empleados no estaban seguros acerca de cuáles eran sus funciones más críticas, por lo que se debe trabajar en identificar estos servicios en los funcionarios de la organización.

Los departamentos que se toman en cuenta para la siguiente pregunta son: informática (TI), proyectos, auditoría, académico, comunicación e imagen, gerencial, mercadeo, financiero e investigación y desarrollo (IyD).

Tabla 16 – Funciones críticas por departamento en CENECOOP R.L.

#	Persona	Información	Afecta a
1	anonymous	Analizar la información financiera, brindada por el departamento financiero.	Todos los departamentos.
2	anonymous	La digitalización de los documentos al sistema, por lo que si no se realiza las otras funciones se paralizarán.	Financiero, auditoría y gerencia.
3	anonymous	Confección de certificados.	Comunicación e imagen y académico.
4	anonymous	Actualización de información contable (sistemas), declaraciones de impuestos.	Todos los departamentos
5	anonymous	La relación con nuestros clientes. El servicio al cliente. La imagen de la empresa.	Comunicación e imagen, académico, proyectos y mercadeo.
6	anonymous	Control y seguimiento a proyectos en marcha.	TI, académico, IyD y proyectos.
7	anonymous	Dismunición de matrícula. No vender servicios.	Todos los departamentos.
8	anonymous	Elaborar y actualizar de documentos administrativos del CENECOOP R.L., para la diligencia de información, políticas y normas que contribuyen al respectivo funcionamiento de la entidad, en caso de no ser así, el departamento Gerencial podría presentar inconvenientes y limitaciones en la coordinación.	Todos los departamentos
9	anonymous	Convocatorias a actividades académicas.	Académico, comunicación e imagen.
10	anonymous	Diseño de procesos educativos.	Académico, proyectos, IyD y comunicación e imagen.
11	anonymous	Llevar un control del área virtual, por ejemplo, el no abrir cursos para el inicio de los períodos.	TI, mercadeo y financiero.

12	anonymous	Desarrollo y actualización de sistemas y plataformas educativas	Todos los departamentos.
13	anonymous	Diseño gráfico (artes, flyers) ediciones de vídeo e imagen.	TI, proyectos, académico, comunicación e imagen y mercadeo.

Fuente: elaboración propia, con base en los resultados obtenidos de la encuesta realizada a los colaboradores de CENECOOP R.L.

4.5 Brechas y recomendaciones del diagnóstico

Tabla 17 – Brechas del diagnóstico en CENECOOP R.L.

Análisis de la situación actual

#	Brecha	Estándares	Recomendación
1	No se cuenta con un proceso que le permita identificar si se encuentra en una situación de contingencia.	COBIT 5 DS4.1: desarrollar planes de continuidad de TI, diseñado para reducir el impacto de una interrupción.	1. Identificar la urgencia de la continuidad del negocio por parte del departamento tecnológico, comunicarlo a los altos mandos. 2. Convocar a reunión para que todos estén anuentes a colaborador en la implementación. 3. Desarrollar un plan de continuidad del negocio para la cooperativa.
2	No se tienen definidos los servicios críticos relacionados con la continuidad del negocio que se brinda en CENECOOP R.L.	ISO 22301 (Punto en ISO 8.2.1): identificar los procesos críticos de la organización, entradas, resultados, la relación con otros procesos de la organización.	1. Realizar primeramente un diagnóstico de la situación actual para determinar falencias en procesos y servicios de la organización. 2. Empezar un listado de los servicios de CENECOOP R.L en todos sus departamentos con el fin de identificar los servicios más críticos.

			3. Determinar posteriormente los servicios críticos del departamento tecnológico y analizar como disminuir el impacto que genere al activarse.
3	No se lleva un análisis de impacto ni riesgos según la continuidad del negocio.	ISO 22301 (Punto en ISO 8.2.2): se debe establecer, implementar y mantener un proceso formal y documentado para el análisis de impacto y valoración del riesgo.	1. Antes de llevar a cabo el análisis se debe estudiar la situación actual de la empresa, se abarcan todos los departamentos. 2. Se recomienda la realización del análisis de impacto, amenazas, vulnerabilidades y riesgos a través de matrices que determinan con mayor exactitud, ya que esto es la base fundamental de un BCP.
4	No se les imparte a los funcionarios capacitaciones con respecto a la continuidad.	COBIT 5 DS4.6: entrenamiento del BCP, asegurarse de que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.	1. Revisar el plan de continuidad, verificar como se puede mitigar esta brecha. 2. Comunicarle a coordinadora de recursos humanos de la importancia en este tema. 3. Capacitar a todos los colaboradores al finalizar la etapa de aplicación del plan, esto con el fin de que todos estén relacionados e identificados con la aplicación del plan de continuidad para un éxito garantizado. 4. Motivación para un eficaz manejo de la continuidad en la organización.
5	La cooperativa no cuenta con planta eléctrica, lo cual es un riesgo en los servicios críticos.	ISO 22301 (Punto en ISO 8.2.3): Se deben establecer necesidades de recursos, tales como: edificios,	1. Comunicar a los altos mandos de la cooperativa del problema inherente. 2. El departamento de TI debe buscar y cotizar cuál es la aplicación para eliminar esta amenaza.

		ambiente de trabajo, servicios asociados, sistemas de información, tecnología de comunicación y proveedores.	3. En caso de falla eléctrica está brecha genera un impacto negativo por el tipo de servicio que brinda la cooperativa. 4. Adquirida la plata o el nuevo servicio verificar el funcionamiento de esta.
6	No cuenta con dos proveedores de internet.		1. Comunicar a los altos mandos de la cooperativa del problema inherente. 2. El departamento de TI debe buscar y cotizar cuál es el mejor proveedor para duplicar el servicio actual de internet. 3. En caso de falla por parte del proveedor el segundo enlace de fibra óptica debe levantar inmediatamente para disminuir el impacto a CENECOOP R.L. 4. Realizar pruebas pertinentes del nuevo enlace de internet.
7	Los servidores no cuentan con software especializado para la detección de intrusos, se detecta que los servidores de aplicación no cuentan con redundancia.	COBIT 5 DS4.3: asegurarse de la compatibilidad de hardware y software para poder recuperar los datos. La jefatura de TI debe asegurar evaluaciones constantes para la protección y seguridad.	1. Comunicar al coordinador la importancia de la redundancia en los servidores, así como la urgencia de instalación de software para la detección de intrusos y proteger los activos más importantes de la empresa (información). 2. Cotización de software para servidores en la nube (Linux y Windows). 3. Instalación de software en los equipos correspondientes, es positivo que los servidores de aplicación tengan redundancia sin embargo no cuentan con el 100% de redundancia, por lo que se recomienda se aplique esta práctica en

			general a todos los servidores de la organización.
8	No se realiza un respaldo en las computadoras de los funcionarios de la cooperativa, por lo que la información puede perderse en caso de un daño en un equipo.	ISO 22301 (Punto en ISO 8.4.1): la cooperativa debe enfocarse en las siguientes actividades: distribución, acceso, recuperación, almacenamiento y conservación	1. Comunicarle a cada uno de los coordinadores de las diferentes áreas de la cooperativa de la necesidad y próxima aplicación de software para respaldos, porque el departamento de TI no realiza de forma recurrente. 2. Configurar el servidor físico para destino de respaldos, para aprovechar que el servidor se encuentra en la misma red y de fácil acceso. 3. Instalación de software en las computadoras de los colaboradores para que se realice de forma automática y de manera incremental (se suben los archivos actualizados o bien los documentos o archivos nuevos).
9	En materia de red tiene vulnerabilidades en aspectos como: cableado estructurado, configuraciones y estandarizado.	ISO 22301 (Punto en ISO 8.4.1): se debe evaluar el desempeño y su eficacia. Las evaluaciones deben llevarse a cabo a través de revisiones periódicas, pruebas y reportes después de incidentes.	1. Se deben realizar pruebas de penetración a la red interna y externa. 2. Revisar configuraciones de conmutadores y enrutadores de red, porque no se le da mantenimiento desde el año 2015 (según información descrita por Alonso Salazar, coordinador de TI). 3. Configurar firewall en toda la red de CENECOOP R.L para bloquear el acceso no autorizado ya que, actualmente no se ha configurado y es de vital importancia para evitar ataques informáticos.

10	Tomar en consideración la factibilidad de alquilar (leasing) de equipo de cómputo e impresoras.	Preserva la liquidez disponible, lo que permite hacer más con menos.	1. Comunicar a los altos mandos de la cooperativa del problema inherente. 2. El departamento de TI debe buscar y cotizar cuál es el mejor proveedor de alquiler de equipo. 3. Analizar la factibilidad de la compra vs alquiler de equipos. 4. Considerando que actualmente poseen 12 computadoras por este método en la empresa COCOCO (Grupo 3C) se puede consultar la adquisición de más equipo tecnológico lo cual es una necesidad obligatoria.

Fuente: elaboración propia.

CAPITULO V
PROPUESTA DE PROYECTO

5.1 Propuesta del proyecto

Se plantea una propuesta como una solución de desarrollo del plan de continuidad del negocio, donde se pueda aplicar un modelo a seguir, el presente capítulo se clasifica en tres divisiones que son: la situación actual, análisis de riesgos y el desarrollo de la propuesta.

La situación actual en la empresa lo que busca es examinar y comprender las circunstancias, tecnologías y procesos a groso modo de la institución educativa, esto permite estudiar y poder abordar las fases posteriores con garantías sobre una base sólida, en esta etapa se evidencia las falencias en cada uno de los sectores de la compañía.

En la segunda sección la propuesta enuncia los respectivos análisis a realizar como el de riesgo, impacto y probabilidad en la cooperativa, pero el estudio se centra finalmente en el departamento tecnológico. En función de los riesgos identificados se analiza el impacto que genera en el negocio cada uno de estos en CENECOOP R.L, para realizar una propuesta donde se logre disminuir la afectación a la continuidad o bien, como enfrentarlos eficientemente ante una eventual situación.

Los problemas dentro de la organización son muy frecuentes y ya generan una pérdida importante para la cooperativa causando una inestabilidad financiera, sin dejar de lado la calidad del servicio que se brinda para su cartera de clientes, es por lo que las relaciones con estos y proveedores potenciales no se encuentran en las mejores condiciones.

El apartado tres se desarrolla un plan de continuidad del negocio en la organización aplicando las mejores prácticas con base en la situación actual, riesgos, vulnerabilidad y amenazas que se demuestra en las dos primeras secciones, con esto se busca proponer y generar una mayor confianza en las soluciones integrales en la gestión de incidentes que puedan presentarse en la empresa que impidan el curso normal en las operaciones del negocio.

5.2 Situación actual de CENECOOP R.L.

5.2.1 Análisis PESTEL

El análisis PESTEL es una herramienta de gran utilidad para entender el crecimiento o la disminución de un mercado y en consecuencia la posición, potencial y dirección de un negocio en este caso cooperativa. Es una herramienta de medición. PESTEL está compuesto por las iniciales de los factores: Políticos, Económicos, Sociales, Tecnológicos, Ecológicos y Legales, que se utilizan para evaluar el mercado en el que se encuentra la empresa. (Chapman, s. f.)

Tabla 18 – Análisis PESTEL de CENECOOP R.L.

Aspecto	Características	*Impacto		
		A	M	B
Político	• Inestabilidad política en el país (riesgo país).	⊗		
	• Reformas a los estatutos que rigen a la cooperativa.	⊗		
	• Inestabilidad política en el constante cambio de asamblea y representantes de CENECOOP R.L.	⊗		
Económico	• Alta competencia en el mercado y en precios.	⊗		
	• Aumento de carga impositiva.		⊗	
	• Frecuentes cambios en aranceles e impuestos en Costa Rica.	⊗		
Social	• No cumplir con brindar beneficios sociales a los empleados.		⊗	
	• Demanda por estabilidad laboral.	⊗		
	• No satisfacer las necesidades y expectativas de los clientes en búsqueda de soluciones.	⊗		
Tecnológico	• Fallos en la red informática.	⊗		
	• Ataques externos a los sistemas informáticos de la institución.	⊗		
	• Constantes fallos en la energía eléctrica y equipos de comunicación.	⊗		
Ecológico	• Incendios	⊗		
	• Terremotos	⊗		
	• Erupciones volcánicas.	⊗		
Legal	• Enviar un diagnóstico erróneo a la auditoría.	⊗		
	• Extorsión.	⊗		
	• Limitación de instalación de infraestructura por parte del Centro de Estudios y Capacitación Cooperativa.			⊗

*El impacto se muestra en una escala: Alto (A), Medio (M) y Bajo (B).

Fuente: elaboración propia.

5.2.2 **Análisis FODA a CENECOOP R.L.**

Con el objetivo de identificar el estado de la situación actual de CENECOOP R.L. se procede a realizar un análisis FODA, con el análisis no solo se trata de identificar las fortalezas, debilidades, oportunidades y amenazas, sino cómo generar algún tipo de valor agregado para la organización.

El análisis FODA es una evaluación subjetiva de datos organizados en el mismo formato, que los coloca en un orden lógico que ayuda a comprender, presentar, discutir y tomar decisiones. Puede ser utilizado en cualquier tipo de toma de decisiones El análisis FODA evalúa la empresa o propuesta de negocio, los factores analizados son internos (fortalezas y debilidades) y externos (oportunidades y amenazas). (Chapman, s. f.)

El FODA se presenta como una matriz de cuatro secciones (pros y contras), una para cada uno de los elementos Fortalezas, Oportunidades, Debilidades y Amenazas. En la siguiente tabla (12) se muestra un análisis tanto interno como externo para proceder con la matriz FODA.

Tabla 19 – Análisis FODA de CENECOOP R.L.

<table>
<tr><th colspan="2">Análisis interno</th></tr>
<tr><td>Fortalezas</td><td rowspan="11">▪ Crear un buen ambiente laboral para mejorar el desempeño dentro de la empresa.
▪ Evaluar y mejorar los procesos de contratación de recursos humanos.
▪ Incentivar una cultura organizacional, con valores y compromisos.
▪ Definir claramente las funciones que se llevan día a día e implementar jornadas de capacitación.</td></tr>
<tr><td>1. Experiencia de 30 años en educación cooperativa.</td></tr>
<tr><td>2. Calidad en el servicio corporativo.</td></tr>
<tr><td>3. Creación de servicios innovadores y de alta calidad.</td></tr>
<tr><td>4. Especialistas en el campo de capacitación.</td></tr>
<tr><td>5. Contar con buen ambiente para trabajar.</td></tr>
<tr><td>Debilidades</td></tr>
<tr><td>1. Escasa capacitación para el personal.</td></tr>
<tr><td>2. Cuentas por cobrar altas.</td></tr>
<tr><td>3. Falta de interés del personal en participación de actividades dentro de la empresa.</td></tr>
<tr><td>4. Carencia de habilidades y capacidades clave.</td></tr>
<tr><th colspan="2">Análisis externo</th></tr>
<tr><td>Oportunidades</td><td></td></tr>
</table>

1. Los clientes tienen la necesidad de adquirir los servicios ofertados.	▪ Contar con una Plan Estratégico adecuado para el funcionamiento de la empresa. ▪ Mantener una constante renovación de imagen en el mercado. ▪ Tomar en cuenta la participación de los clientes externos para la continua mejora de los productos.
2. Servicios que generan un valor agregado diferente a la competencia.	
3. Mejora continua de la calidad de los servicios.	
4. Entrar a nuevos segmentos de mercado.	
Amenazas	
1. Entrada de nuevos competidores.	
2. Reformas en las normativas de entidades reguladoras.	
3. Constante entrada y salida de personal.	
4. Problemas internos en recursos humanos.	

Fuente: elaboración propia.

Tabla 20 – Interpretación análisis FODA de CENECOOP R.L.

	Fortalezas	**Debilidades**
FODA	▪ Experiencia de 30 años en educación cooperativa. ▪ Calidad en el servicio corporativo. ▪ Creación de servicios innovadores y de alta calidad. ▪ Especialistas en el campo de capacitación. ▪ Contar con buen ambiente para trabajar.	▪ Escasa capacitación para el personal. ▪ Cuentas por cobrar altas. ▪ Falta de interés del personal en participación de actividades dentro de la empresa. ▪ Carencia de habilidades y capacidades clave.

Oportunidades	▪ Los clientes tienen la necesidad de adquirir los servicios ofertados. ▪ Servicios que generan un valor agregado diferente a la competencia. ▪ Mejora continua de la calidad de los servicios. ▪ Entrar a nuevos segmentos de mercado.	**Estrategias (FO)** a) Incrementar la publicidad en diferentes medios de comunicación para atraer nuevos clientes. b) Ofrecer mejoras y nuevos servicios a clientes para ser siempre su primera opción.	**Estrategias (DO)** a) Crear un plan de capacitación continua para el personal. b) Consolidar un plan estratégico. c) Fortalecer los lazos de comunicación a deudores.
Amenazas	▪ Entrada de nuevos competidores. ▪ Reformas en las normativas de entidades reguladoras. ▪ Constante entrada y salida de personal. ▪ Problemas internos en recursos humanos.	**Estrategias (FA)** a) Aumentar la calidad en los servicios ofertados. b) Hacer un estudio y sectorización del mercado. c) Desarrollar actividades en conjunto para generar un ambiente laboral tranquilo.	**Estrategias (DA)** a) Crear políticas internas para las actividades dentro de la empresa. b) Consolidar una fuerte estructura organizacional una mejor gestión en la empresa.

Fuente: elaboración propia.

Una vez realizado el análisis, se debe tratar de explotar al máximo las oportunidades para generar estrategias de valor, de esta forma mantener a la organización como una empresa líder en el mercado de capacitación dentro de la línea de negocio. Además, se deben revisar las amenazas con el propósito de evitar todo tipo de acciones que perjudiquen directamente la organización, ya que estas podrían quebrar totalmente la empresa.

Es importante destacar que las debilidades mencionadas anteriormente se pueden convertir en fortalezas, con base a este análisis en la **tabla 13** se observa que de las diferentes estrategias se originan ventajas competitivas y preparar a la empresa contra amenazas tomando en cuenta los factores. La cooperativa presenta problemas que pueden ser muy graves, uno de los principales es la entrada de nuevos competidores. Otro de los problemas que pueden afectar a largo plazo es la constante entrada y salida del personal, debido a que no cuentan con el departamento de recursos humanos bien consolidado.

5.2.2.1 Situación actual del departamento de TI

La gerencia del Centro de Estudios y Capacitación Cooperativa es un área clave dentro de la cooperativa, ya que tiene responsabilidades que básicamente se enfocan en tres campos que son: aplicaciones, operaciones, infraestructura y servicio al cliente interno tales como soporte al usuario, servicios de red y mantenimiento preventivo y correctivo.

5.2.2.2 Análisis FODA de TI

Tabla 21 – Análisis FODA del departamento de TI

Análisis interno	
Fortalezas	▪ Dar a conocer a los empleados el funcionamiento de toda la empresa para que tengan el conocimiento de todos los procesos y se pueda realizar un mejor trabajo. ▪ Mantener la constante actualización de licencias de software, para lograr mantener la alta calidad en sus servicios.
1. Adaptación a nuevas tecnologías.	
2. Personal competitivo capaz de brindar rápidas soluciones.	
3. El ambiente laboral es bueno.	
Debilidades	
1. Falta de personal para todas las funciones del departamento.	
2. Los empleados del departamento de TI no tienen conocimiento completo de las actividades específicas del negocio.	
3. Falta de actualización de licenciamiento de software.	
Análisis externo	
Oportunidades	

1. Todos los sectores laborales se centran en el departamento de TI. 2. Los clientes internos como externos requieren los servicios del departamento de TI. **Amenazas** 1. Los cursos virtuales presentan materiales didácticos no gestionados por el departamento (tercerizado). 2. Falta de recursos para renovar la infraestructura tecnológica.	▪ Mejorar la calidad del servicio en todas las áreas de negocio. ▪ Tener un control total sobre las actividades que deben ser administradas por el departamento de TI. ▪ Llevar una correcta gestión en la contratación de proveedores para obtener un óptimo control en la calidad.

Fuente: elaboración propia.

Tabla 22 – Interpretación análisis FODA del departamento de TI

FODA	**Fortalezas**	**Debilidades**
	▪ Adaptación a nuevas tecnologías. ▪ Personal competitivo capaz de brindar rápidas soluciones. ▪ El ambiente laboral es bueno.	▪ Falta de personal para todas las funciones del departamento. ▪ Los empleados del departamento de TI no tienen conocimiento completo de las actividades específicas del negocio. ▪ Falta de actualización de licenciamiento de software.

Oportunidades	▪ Todos los sectores laborales se centran en el departamento de TI. ▪ Los clientes internos como externos requieren los servicios del departamento de TI.	**Estrategias (FO)** a) Hacer inversiones en la mejora de aplicaciones. b) Fortalecer el servicio de soporte.	**Estrategias (DO)** a) Planificar capacitaciones para el conocimiento del negocio. b) Planear la actualización de licenciamiento a los equipos que necesiten renovación.
Amenazas	▪ Los cursos virtuales presentan materiales didácticos no gestionados por el departamento (tercerizado). ▪ Falta de recursos para renovar la infraestructura tecnológica.	**Estrategias (FA)** a) Tener los servicios dentro del departamento TI para evitar contrataciones a terceros. b) Desarrollar un plan para la renovación de equipos físicos.	**Estrategias (DA)** a) Centralizar los procesos en el departamento de TI para gestionarlos de mejor manera. b) Realizar evaluaciones de desempeño para evaluar al personal.

Fuente: elaboración propia.

Con el análisis FODA realizado se puede obtener un diagnóstico de la situación del departamento de TI, esto permite tomar las mejores decisiones con base en los elementos descritos en la **tabla 15,** con el fin de mejorar las falencias del departamento y posicionarlo en lo más alto dentro de la empresa.

Adicionalmente se deben reducir las debilidades y proteger al departamento de las amenazas que actualmente afectan directamente en las operaciones, las estrategias no solamente fortalecen al departamento, sino también a la organización entera, ya que las funciones son enfocadas a dicho departamento. Se determina que el departamento de TI no juega un papel determinando al momento de la toma de decisiones tecnológicas, porque depende de la aprobación del departamento financiero para la adquisición de la infraestructura tecnológica de la empresa.

5.2.3 **Análisis CAME**

El análisis CAME, acrónimo de varias palabras que es este caso significan “corregir, afrontar, mantener y explotar” es una metodología que complementa el análisis FODA, que otorga pautas para actuar sobre aspectos identificados en los diagnósticos del FODA.

Una vez completado el análisis FODA, se analiza como corregir las debilidades, afrontar las amenazas, mantener las fortalezas y explotar las oportunidades que se derivan del FODA. A partir de esto se identifican las más importantes, según nuestro objetivo inicial como organización e investigación.

Tabla 23 – Análisis CAME para CENECOOP R.L.

Debilidades	→	**Corregir**
Escasa capacitación para el personal.		Detectar necesidades, establecer los objetivos y elaborar un programa a la medida para ejecutar y evaluar los resultados.
Cuentas por cobrar altas.		Penalizar a los clientes que no se paguen a tiempo u ofrecer descuentos a los clientes para reducir los plazos de pago.
Amenazas	→	**Afrontar**
Entradas de nuevos competidores.		Abarcar nuevos mercados aplicando un mejor servicio al cliente creando más canales de ventas. Identificar competidores.
Constante entrada y salida de personal.		Definir muy bien el perfil de cada puesto de trabajo, incentivar económicamente para retener el talento.
Fortalezas	→	**Mantener**
Experiencia de 30 años en educación cooperativa		Establecer nuevos mecanismos para alcanzar otro público meta y de esta manera expandirse a nivel nacional y porque no internacionalmente.

Especialistas en el campo de capacitación.	Constante innovación en los servicios y aplicación persistente de actualización y capacitación al personal del área.
Oportunidades →	**Explotar**
Entrar a nuevos sectores del mercado.	Identificar y evaluar el mercado al ingresar, diseñar una buena estrategia de marketing y posteriormente ofrecer los servicios.
Servicios que generan un valor agregado diferente a la competencia.	Agregar un valor extra más allá de los servicios brindados poniendo personalidad en marca y en caso de ser posible ayudar en alguna causa que tenga sentido con la cooperativa y servicios brindados.

Fuente: elaboración propia.

Tabla 24 – Análisis CAME del departamento de TI

Debilidades →	**Corregir**
Falta de personal para las funciones de TI.	Jefe de área de TI debe delegar funciones al personal o bien, contratación de personal capacitado.
Empleados no poseen conocimiento de actividades del negocio.	Es responsabilidad de los altos mandos una capacitación al departamento de TI, donde se expliquen las actividades de CENECOOP R.L.
Amenazas →	**Afrontar**
Falta de recursos para infraestructura tecnológica.	Es compromiso del jefe de TI la asignación adecuada de recursos para cumplir con los requisitos propuestos; se debe ver como una inversión y no como gasto.
Existen servicios críticos no gestionados directamente con el departamento de TI (tercerizado).	Capacitación de funciones al personal de TI y evitar la contratación de un tercero y me genera un mayor ingreso o bien, buscar otro proveedor con resultados más rápidos y eficientes.

Fortalezas	→	**Mantener**
Adaptación a nuevas tecnologías.		Seguir siendo flexible y originales ante los cambios del mercado, además es muy importante reconocer las nuevas tecnologías.
El ambiente laboral es bueno.		Fomentar la cooperación en lugar de la competencia entre el departamento, mantener un clima de respeto mutuo.
Oportunidades	→	**Explotar**
Todas las áreas se centran en el departamento de TI.		La capacitación es la estrategia más importante que permite potenciar el área de TI y por consecuente la influencia en la cooperativa.
Los clientes requieren los servicios de TI.		Se debe motivar, dirigir y coordinar las acciones del departamento de TI con el fin de ofrecer soluciones ágiles y oportunas a los clientes.

Fuente: elaboración propia.

5.2.3.1 **Interpretación análisis CAME**

Una vez realizado el análisis CAME, se deben tomar acciones con base en los resultados anteriores, a continuación, se definen las diferentes estrategias a seguir, cada una de ellas se complementa con dos herramientas del análisis FODA.

Estrategia de reorientación (D y O): transforma la situación aplicando cambios que eliminen nuestras debilidades y creen nuevas fortalezas. Predominan corregir debilidades y explotar oportunidades.

Estrategia de supervivencia (D y A): se busca eliminar los aspectos negativos que perjudican a la organización. Predominan a corregir debilidades y afrontar amenazas.

Estrategia ofensiva (F y O): busca perfeccionar la situación actual (ganar cuota de mercado). Predominan las acciones de explotar oportunidades y mantener fortalezas.

Estrategia defensiva (A y F): consiste en evitar que empeore nuestra situación actual (perder cuota de mercado). Predomina afrontar amenazas y mantener fortalezas.

Tabla 25 – Estrategias de interpretación análisis CAME

FODA – CAME Planificación estratégica		**Fortalezas (F)**	**Debilidades (D)**
		F1: Adaptación a nuevas tecnologías. **F2:** El ambiente laboral es bueno.	**D1:** Falta de personal para las funciones de TI. **D2:** Empleados no poseen conocimiento de actividades del negocio.
Oportunidades (O)	**O1:** Todas las áreas se centran en el departamento de TI. **O2:** Los clientes requieren los servicios de TI.	**Estrategia de ataque** **O1F1:** innovación constante y ofrecer a usuarios aplicación móvil que hasta el día de hoy no poseen, donde se puedan adquirir servicios como en la página web.	**Estrategia de reorientación** **O2D1:** establecer prioridades entre los empleados de TI, ver posibilidad de pasar tareas administrativas a empleados fuera del área para sacar enfocar atención a clientes.
Amenazas (A)	**A1:** Falta de recursos para infraestructura tecnológica. **A2:**Existen servicios críticos no gestionados directamente con el departamento de TI.	**Estrategia defensiva** **A2F1:** capacitar al personal para que adapte a tecnología brindada por proveedor para luego poder prescindir del contrato y quede centralizado en el departamento de TI.	**Estrategia de supervivencia** **A1:** ante esta amenaza quitar un mínimo presupuesto a demás áreas, para poder brindarlo a necesidades del departamento de TI y de esta manera cubrir sus necesidades.

Fuente: elaboración propia.

5.2.4 **Análisis de riesgos para la empresa CENECOOP R.L según ISO 27001**

El análisis de riesgo valora la posibilidad de que se produzca un daño que afecte a los activos de la empresa. En el contexto de un Plan de Continuidad de Negocio, el análisis de riesgos debe valorar los elementos que soportan a los procesos esenciales o críticos y los diversos riesgos que pueden afectar: intencionados, negligencias o eventos naturales. Con cada uno de los riesgos se

busca establecer la probabilidad de ocurrencia de este y sus consecuencias, este último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

En la siguiente tabla se muestra una comparación entre vulnerabilidades, amenazas y riesgos de seguridad más frecuentes según la norma ISO 27001 / 27002 que más adelante se comprueban mediante pruebas documentales.

Tabla 26 – Vulnerabilidad, amenazas y riesgos según ISO 27001 / 27002

ID	Vulnerabilidad	Amenazas	Riesgo potencial
		Hardware	
V1	Falta de equipos UPS's para contingencia.	Cortes de energía o sobrecarga en los equipos.	Pérdida de información, daños en los equipos, pérdida de tiempo en procesos repetidos.
		Software	
V2	Software no licenciado.	Virus informáticos, malware.	Mal funcionamiento de sistemas de CENECOOP R.L, destrucción de SO, destrucción de aplicativos.
V3	Software con problemas de seguridad en el desarrollo.	Ataques de inyección SQL, información inconsistente, errores de integridad de datos.	Perdida o modificación de información, robo de clave de usuario, bases de datos inseguras por permisos o privilegios.
V4	Actualización de S.O en los equipos.	Ataques exploit.	Intrusión no autorizada en los equipos de usuarios para modificación, borrado o robo de información.
		Seguridad física	
V5	No existe control de acceso físico a oficinas y equipos informático.	Manipulación de información sin control	Robo, destrucción, modificación o borrado de

		de acceso, desastres provocados.	información, destrucción o desarticulación física.
Seguridad lógica			
V6	Deficiente control de accesos a los sistemas.	Suplantación de identidad.	Robo de datos, alteración o destrucción de los mismos, suplantación de usuarios, robo de claves a usuarios.
Red de comunicaciones			
V7	Vulnerabilidad de navegadores utilizados.	Ataques XSS.	Alteración en el funcionamiento del código, programas y sitios web.
Personal			
V8	Falta de una política de seguridad clara.	Ataques no intencionados, phishing.	Borrado o eliminación de archivos, destrucción del S.O.

Fuente: elaboración propia.

Escala para cuantificar los activos informáticos:

Tabla 27 – Cuantificación de activos según ISO 27002

Nivel	**Valor**
Muy alto (MA)	Monto > $10.000.000
Alto (A)	$10.000.000 < Monto > $5.000.000
Medio (M)	$5.000.000 < Monto > $1.000.000
Muy bajo (MB)	$1.000.000 < Monto > $500.000

Fuente: elaboración propia.

Tabla 28 – Valoración de activos según ISO 27002

Daño	**Valor**
Daño catastrófico	10
Daño grave	7 – 9
Daño moderado	4 – 6

Daño leve	1 – 3
Daño irrelevante	0

Fuente: elaboración propia.

Tabla 29 – Criterios de evaluación de seguridad de la información

Dimensiones						
Tipo de activo	**Nombre de activo**	**Confidencialidad** Daño	**Integridad** Perjuicio	**Disponibilidad** Perjuicio	**Autenticidad** Perjuicio	**Trazabilidad** Daño
Activo de información	Datos de clientes y proveedores	(8)(A)	(8)(A)	(5)(B)	(7)(M)	--
Software o aplicación	Software sin licencia	--	--	(10)(MA)	--	--
Hardware	Servicio de internet	(9)(A)	(9)(A)	(7)(M)	(5)(B)	--
Instalación eléctrica	Cumplimiento de normas	--	(8)(A)	(8)(A)	--	--
Personal	Personal usuario sistemas	(9)(A)	(9)(A)	(9)(A)	(8)(A)	(8)(A)

Fuente: elaboración propia.

Una vez evaluados los criterios se procede a la valoración de riesgos en la escala de probabilidad e impacto según norma ISO 27002.

Tabla 30 – Esca de valoración de ocurrencia según ISO 27002

Frecuencia	**Ocurrencia**
Frecuencia muy alta (MA)	1 o más veces al día
Frecuencia alta (A)	1 vez a la semana
Frecuencia media (M)	1 vez cada mes
Frecuencia baja (B)	1 vez cada dos meses

Frecuencia muy baja (MB)	1 vez cada seis meses

Fuente: elaboración propia.

Tabla 31 – Valoración de impacto según ISO 27002

Escala	Valoración
Catastrófico	66% a 100%
Moderado	31% a 65%
Leve	0% a 30%

Fuente: elaboración propia.

Tabla 32 – Valoración de riesgos por probabilidad e impacto según ISO 27002

Riesgos / Valoración		Probabilidad					Impacto		
		MA	A	M	B	MB	L	M	C
Hardware (en porcentaje)									
V1	Falta de UPS		X						100
Software (en porcentaje)									
V2	Software no licenciado	X							100
V3	Sistemas sin restricciones		X					65	
V4	Falta de control de cambios		X					60	
Seguridad física (en porcentaje)									
V5	Poca restricción de acceso		X						70
V6	Poco control de acceso a oficina	X							100
Seguridad lógica (en porcentaje)									
V7	Deficiente control a usuarios		X					65	
Redes y comunicación (en porcentaje)									
V8	Vulnerabilidad en navegadores		X						70
Personal (en porcentaje)									
V9	Usuarios sin capacitación	X							70

V10	Personal sin experiencia			X			30		

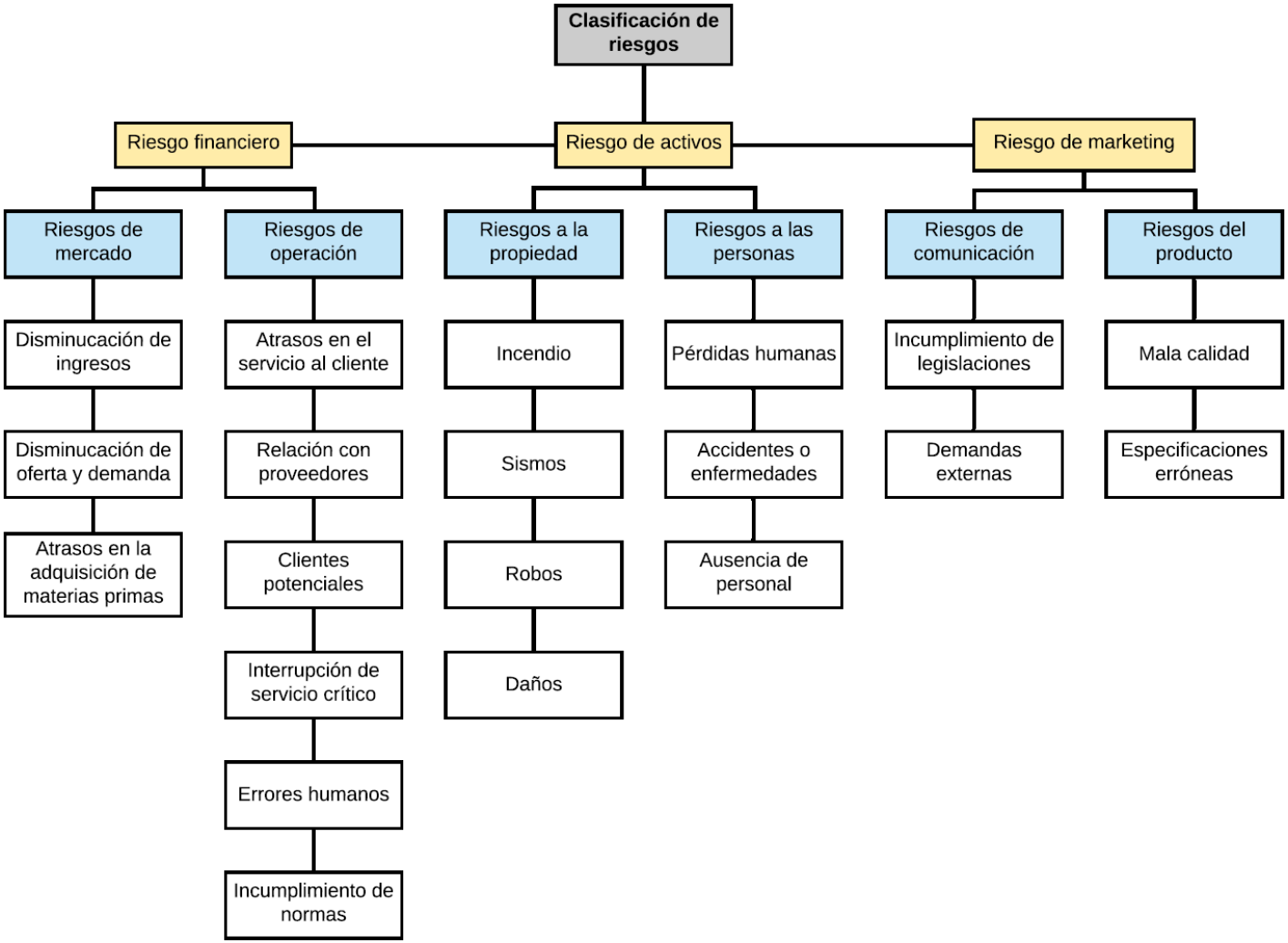
Fuente: elaboración propia.

Según los resultados obtenidos en la valoración se evidencia que los problemas de seguridad en CENECOOP R.L están relacionados principalmente con el desconocimiento o nula existencia de la aplicación de las normas de seguridad de la información y las limitaciones en la administración de seguridad informática, lo cuál compromete enormemente la imagen de la cooperativa. Las posibles causas son la mínima cultura en el tema de seguridad de la información, no hay responsables de la seguridad en el Centro de Estudios, falta de cumplimiento de las políticas y procedimientos internos de seguridad dentro de la organización, en general la competencia limitada del personal para proteger los activos informáticos frente a las amenazas y riesgos de la actualidad.

A continuación, se describen los pasos a realizar para la identificación general y el análisis de riesgos para la cooperativa.

1. Se toma la clasificación de los riesgos presentes en la empresa.

Figura 15 – Clasificación general de riesgos a CENECOOP R.L.



Fuente: elaboración propia.

2. Con la clasificación de riesgos, se procede a determinar para cada uno de ellos todas las fuentes posibles que pueden generar el riesgo indicado además las áreas de impacto que tendrían si se llegaran a materializar los riesgos. Tanto las fuentes como las áreas de impacto fueron definidos mediante las entrevistas realizadas a las jefaturas, en la tabla 16 se muestran los resultados.

Tabla 33 – Descripción de los riesgos, fuentes y áreas de impacto

				Áreas de impacto		
Riesgo	Fuentes de riesgo	Ingresos	Costos	Aplicaciones	Personal	Equipos
Disminución de ingresos	No facturación	X		X	X	
	No venta de servicios	X			X	
	No renovación de contratos	X				
	Disminución de leyes a cooperativa (INFOCOOP)	X				
Disminución de oferta y demanda	Mala imagen	X	X	X	X	X
	Situación económica del país	X				X
Atrasos en adquisición de materia prima	Problemas con el software		X	X	X	
	Atrasos contables para compras		X	X	X	
Atrasos en el servicio al cliente	Mala atención a estudiantes			X	X	X
	Tiempo de respuesta extensa	X		X	X	
Relación con proveedores	Pérdida de proveedor importante	X			X	
	Cierre de servicios por parte de proveedores	X				
Pérdida de clientes potenciales	El servicio no opera como lo esperaban					X
	Falta de soluciones a necesidades		X			
	Falta de mantenimiento		X	X	X	

Interrupción de servicio crítico	Error humano crítico		X		X	
Errores humanos	Falta de capacitación al personal		X		X	
	Mala configuración de equipos		X	X	X	
Incumplimiento de normas			X		X	
Incendios	Cableado eléctrico		X			
Sismos	Región sísmica		X			
Robos	Personal mal intencionado		X		X	
Daños al equipo	Mala manipulación				X	X
Pérdidas humanas	Accidentes fatales de trabajo		X		X	
	Enfermedades terminales		X			
	Pandemias		X			
Accidentes laborales y enfermedades	No seguimiento de procedimientos de seguridad		X		X	
Ausencia de personal	Incapacidades		X		X	
	Situaciones personales de colaboradores		X		X	
Incumplimiento de legislaciones			X			
Demandas externas		X	X			
Mala calidad			X			X
Especificaciones erróneas	Error humano en solicitudes de activos		X		X	X

Fuente: elaboración propia.

Al ser una empresa comercial sus riesgos más trascendentales son aquellos orientados a la venta y servicio al cliente, proveedores, sistema financiero y capital humano.

3. Una vez que se establecen los riesgos y las fuentes generadoras de éstos se procede a realizar el análisis de los riesgos, tomando en cuenta el impacto que la materialización

de éstos tendría en la empresa y la probabilidad de que se lleven a cabo, para ello se utilizan las matrices que se presentan en la tabla 16 y las cuales fueron realizadas tomando las condiciones actuales de la empresa.

Tabla 34 – Matriz de impacto y probabilidad

Impacto – Descripción detallada por variable				
Nivel	Descriptor	Disminución ingresos	Incremento costos	Disminución equipos
1	Insignificante	Menor o igual a 5%	Menor o igual a 5%	Menor o igual a 2%
2	Menor	De 6% a 11%	De 6% a 10%	De 3 a 9
3	Moderado	De 12% a 18%	De 11% a 15%	De 10 a 15
4	Mayor	De 19% a 25%	De 16% a 20%	De 16 a 19
5	Catastrófico	Mayor a 25%	Mayor a 20%	Mayor a 20

Fuente: elaboración propia.

Las medidas utilizadas deberían reflejar las necesidades y naturaleza de la organización y actividad bajo estudio.

Disminución: mayor al 25% indica a la disminución de ₡3.000.000 al mes.

Incremento de costo: mayor al 20% indica el aumento de hasta ₡5.000.000.

Tabla 35 – Medidas cualitativas de probabilidad

Probabilidad – Medidas cualitativas de probabilidad		
Nivel	Descriptor	Tiempo recurrencia
A	Casi certeza	Ha sucedido más de una vez al año en CENECOOP R.L.
B	Probable	Ha sucedido al menos una vez en CENECOOP R.L.
C	Posible	Ha sucedido más de una vez en un año.
D	Improbable	Se ha escuchado hablar de eventos similares dentro de la empresa.
E	Raro	Nunca se ha escuchado hablar de evento similares en la empresa.

Fuente: elaboración propia.

4. Para la determinación del nivel de riesgo se utiliza la matriz que se muestra en la tabla 17.

Tabla 36 – Matriz de consecuencias de riesgos cualitativo – Nivel de riesgo

Consecuencias					
Probabilidad	Insignificante 1	Menores 2	Moderado 3	Mayores 4	Catastrófico 5
A	H	H	E	E	E
B	M	H	H	E	E
C	L	M	H	E	E
D	L	L	M	H	E
E	L	L	L	H	H

Fuente: Estándar Australiano.

5. Con las matrices mostradas en la figura 12 y tabla 16 se realiza el análisis de riesgos obteniendo así cuáles de ellos la empresa deberá de dar prioridad para atacar y cuáles de ellos se podrán aceptar. Para ellos se tomará en cuenta los riesgos definidos como H y E que representan el mayor riesgo para la continuidad del negocio de la empresa CENECOOP R.L. En la siguiente tabla (19) se muestra la evaluación inicial de los riesgos de la cooperativa.

Tabla 37 – Matriz de análisis de riesgos cualitativo – Nivel de riesgo

Riesgo	**Fuentes de riesgo**	**Impacto**	**Probabilidad**	**Resultado**
Disminución de ingresos	No facturación	Menor	Improbable	L
	No venta de servicios	Catastrófico	Casi certeza	E
	No renovación de contratos	Catastrófico	Posible	E
	Disminución de leyes a cooperativa (INFOCOOP)	Catastrófico	Posible	E
Disminución de oferta y demanda	Mala imagen	Moderado	Raro	M
	Situación económica del país	Catastrófico	Posible	E
	Problemas con el software	Catastrófico	Casi certeza	E

Atrasos en adquisición de materia prima	Atrasos contables para compras	Catastrófico	Posible	E
Atrasos en el servicio al cliente	Mala atención a estudiantes	Menor	Casi certeza	H
	Tiempo de respuesta extensa	Menor	Casi certeza	H
Relación con proveedores	Pérdida de proveedor importante	Catastrófico	Casi certeza	E
	Cierre de servicios por parte de proveedores	Moderado	Raro	M
Pérdida de clientes potenciales	El servicio no opera como lo esperaban	Catastrófico	Probable	E
	Falta de soluciones a necesidades	Catastrófico	Probable	E
Interrupción de servicio crítico	Falta de mantenimiento	Moderado	Posible	H
	Error humano crítico	Moderado	Improbable	M
Errores humanos	Falta de capacitación al personal	Mayor	Posible	E
	Mala configuración de equipos	Menor	Casi certeza	H
Incumplimiento de normas		Menor	Casi certeza	H
Incendios	Cableado eléctrico	Moderado	Raro	M
Sismos	Región sísmica	Moderado	Raro	M
Robos	Personal mal intencionado	Moderado	Raro	M
Daños al equipo	Mala manipulación	Menor	Improbable	L
Pérdidas humanas	Accidentes fatales de trabajo	Catastrófico	Improbable	E
	Enfermedades terminales	Catastrófico	Raro	H
	Pandemias	Catastrófico	Probable	E
Accidentes laborales y enfermedades	No seguimiento de procedimientos de seguridad	Catastrófico	Improbable	E
	Incapacidades	Catastrófico	Raro	H

Ausencia de personal	Situaciones personales de colaboradores	Catastrófico	Raro	H
Incumplimiento de legislaciones		Menor	Improbable	L
Demandas externas		Menor	Improbable	L
Mala calidad		Menor	Improbable	L
Especificaciones erróneas	Error humano en solicitudes de activos	Menor	Improbable	L

Fuente: elaboración propia.

En la figura anterior se puede identificar cuáles son los riesgos presentes en la empresa y las fuentes que pueden llegar a materializar ese riesgo, seguidamente se indican los resultados de impacto y probabilidad, para lo cual se tomó como base la tabla 16 y al unir estos resultados y tomando como base la tabla 17 se define la clasificación del riesgo, esto quiere decir que magnitud de pérdida tendrá la empresa si se llega a materializar el riesgo, por ende indica a cuales riesgos se les debe dar prioridad de atención para disminuir su impacto en la empresa.

5.2.5 **Análisis de riesgos para el área de TI**

Una interrupción de los procesos de TI afecta considerablemente a las operaciones e imagen de la empresa, pudiendo ocasionar pérdidas irremediables si la interrupción es por un tiempo superior al tiempo máximo de tolerancia del proceso. Con el diagnostico obtenido en el capítulo anterior, se deja en evidencia los riesgos a los que se enfrenta la organización con respecto a la continuidad de los servicios, por lo que se confecciona un listado de riesgos con el apoyo de la ISO 22301; a cada uno de los riesgos se le coloco un “ID”, esto con el fin de realizar una mejor interpretación y para que el mapa de calor sea más eficiente:

- R1: Corte de energía prolongado.
- R2: Caída de los sistemas automatizados.
- R3: Suspensión de servicios de proveedor de internet.
- R4: Incendio o sismo en el edificio del centro de cómputo.
- R5: Robo de información.

- R6: Pérdida de información por ataque informático.
- R7: Manipulación sensible sin autorización.
- R8: Falla en bases de datos.
- R9: Vencimiento de licencias de software.
- R10: Personal no capacitado para sus funciones.
- R11: Caídas de los equipos informáticos o medios de comunicación principales que conectan a la cooperativa (dispositivos de red, central telefónica, servidores, UPS).
- R12: Pérdida de credibilidad en los servicios de TI debido a que no se han definido los servicios críticos de TI.
- R13: Pérdidas económicas importantes debido a la no realización de mantenimientos preventivos.

5.2.5.1 Escalas de probabilidad

Está escala define los rangos en los que se pueden manifestar los riesgos. Consta de una escala de probabilidad de ocurrencia que va desde altamente probable a muy poco probable, que cuantitativamente corresponden a un rango de 5 a 1 respectivamente. Cada uno de estos rangos están definidos por lapsos inferiores a una semana hasta lapsos superiores de cinco años. Además, se tienen cinco colores (rojo, anaranjado, amarillo, verde y verde claro) los cuales son utilizados para clasificar la probabilidad en código de color, lo que es útil en la creación del mapa de calor.

Tabla 38 – Escala de probabilidad

Probabilidad de ocurrencia	Calificación cuantitativa	Calificación cualitativa	Código de colores
Altamente probable	5	Puede ocurrir en la mayoría de las veces. Cuando la amenaza puede presentarse en periodos inferiores a 1 semana.	Rojo
Muy probable	4	Puede ocurrir varias veces en el futuro. Cuando la amenaza puede presentarse en periodos inferiores a 2 meses.	Anaranjado
Probable	3	Puede ocurrir alguna vez en el futuro. Cuando la amenaza puede presentarse en periodos inferiores a 1 año.	Amarillo

Poco probable	2	Puede ocurrir alguna vez, pero es muy poco probable. Cuando la amenaza puede presentarse en periodos inferiores a 5 años.	Verde
Muy poco probable	1	Puede ocurrir en circunstancias excepcionales. Cuando la amenaza puede presentarse en periodos superiores a 5 años.	Verde claro

Fuente: elaboración propia.

5.2.5.2 **Escalas de impacto**

Se desarrollan para definir el impacto materializado que se puede tener si se llegan a presentar los riesgos. Consta de una escala de impacto que va desde muy alto a muy bajo, las mismas son evaluadas cuantitativamente en un rango de 5 a 1 según corresponda. Además, se tiene cinco colores (rojo, anaranjado amarillo, verde y verde claro) los cuales son utilizados para clasificar el impacto en código color, lo que es de mucha utilizada en la aplicación del mapa de calor.

Tabla 39 – Escala de impacto

Impacto	**Calificación**	**Calificación cualitativa**	**Código de colores**
Muy alto	5	No existen controles suficientes, por lo que se puede dar una interrupción completa en los servicios y pérdidas muy considerables.	Rojo
Alto	4	Existen pocos controles, por lo que se puede dar una interrupción en los servicios y pérdidas considerables.	Anaranjado
Medio	3	Existen algunos controles, por lo que se pueden dar interrupciones parciales en los servicios y algunas pérdidas menores.	Amarillo

Bajo	2	Existen pocas actividades sin controles, por lo que se puede dar una interrupción parcial en los servicios.	Verde
Muy bajo	1	Existen controles suficientes, por lo que pueden presentarse avisos, pero sin interrupción ni daños.	Verde claro

Fuente: elaboración propia.

5.2.5.3 **Escalas nivel de riesgo**

Una vez que se han realizado los riesgos según las escalas de probabilidad e impacto, se efectúa una operación entre el valor de la probabilidad por el valor del impacto obtenido de cada riesgo y este resultado da el valor del nivel de riesgo inherente que se procede a clasificar de la siguiente manera.

Tabla 40 – Escala de nivel de riesgo inherente

Color	Nivel de riesgo	Escala de medición por puntos
Rojo	Muy alto	16 – 25
Anaranjado	Alto	11 – 15.9
Amarillo	Medio	7 – 10.9
Verde	Bajo	5 – 6.9
Verde claro	Muy bajo	1 – 4.9

Fuente: elaboración propia.

Tabla 41 – Matriz de exposición

(Mapa de calor)			**Muy alto**	**Alto**	**Medio**	**Bajo**
Probabilidad	Estimación	Valor	5	4	3	2
Muy alta (MA) – Altamente probable	>90% y <100%	5	Muy alto	Muy alto	Alto	Medio
Alta (A) – Muy probable	>70% y <90%	4	Muy alto	Muy alto	Alto	Medio
Media (M) – Probable	>40% y <70%	3	Alto	Alto	Medio	Bajo

Baja (B) – Poco probable	>10% y <40%	2	Medio	Medio	Bajo	Muy bajo
Muy baja (MB) – Muy poco probable	>0% y <10%	1	Bajo	Muy bajo	Muy bajo	Muy bajo

Fuente: elaboración propia.

5.2.5.4 **Valoración de los riesgos**

Los riesgos se evalúan con las escalas que se proponen y según el valor obtenido del impacto y del riesgo, se efectúa un cálculo para obtener el resultado del nivel del riesgo inherente, el cual consiste en una multiplicación entre ambos resultados (Valor del impacto * Valor de la probabilidad = Valor del riesgo), con él que se puede clasificar el nivel del riesgo inherente.

Tabla 42 – Valoración de riesgos

		Cálculos			Valoración del riesgo		
ID	**Riesgo**	**Valor del impacto**	**Valor de la probabilidad**	**Valor del nivel del riesgo**	**Probabilidad**	**Impacto**	**Nivel de riesgo inherente**
R1	Corte de energía prolongado.	5	3	15	Probable	Muy alto	Alto
R2	Caída de los sistemas automatizados.	5	4	20	Muy probable	Muy alto	Muy alto
R3	Suspensión de servicios de proveedor de internet.	5	2	10	Poco probable	Muy alto	Medio
R4	Incendio o sismo en el edificio.	4	2	8	Poco probable	Alto	Medio
R5	Robo de información.	5	4	20	Muy probable	Muy alto	Muy alto
R6	Pérdida de información por ataque informático.	5	3	15	Probable	Muy alto	Alto
R7	Manipulación sensible sin autorización.	5	4	20	Muy probable	Muy alto	Muy alto
R8	Falla en bases de datos.	4	4	16	Muy probable	Alto	Muy alto
R9	Vencimiento de licencias de software.	3	5	15	Altamente probable	Medio	Alto
R10	Personal no capacitado para sus funciones.	4	4	16	Muy probable	Alto	Muy alto
R11	Caídas de los equipos informáticos (dispositivos de red, central telefónica, servidores, UPS).	5	5	25	Altamente probable	Muy alto	Muy alto
R12	No se han definido los servicios críticos de TI.	5	4	20	Muy probable	Muy alto	Muy alto
R13	No realización de mantenimientos preventivos.	3	5	15	Altamente probable	Medio	Alto

Fuente: elaboración propia.

5.2.5.5 **Mapa de calor**

De acuerdo con la valoración de riesgos anterior, se obtienen los siguientes resultados:

R1 – Valor de nivel del riesgo = 15

R2 – Valor de nivel del riesgo = 20

R3 – Valor de nivel del riesgo = 10

R4 – Valor de nivel del riesgo = 8

R5 – Valor de nivel del riesgo = 20

R6 – Valor de nivel del riesgo = 15

R7 – Valor de nivel del riesgo = 20

R8 – Valor de nivel del riesgo = 16

R9 – Valor de nivel del riesgo = 15

R10 – Valor de nivel del riesgo = 16

R11 – Valor de nivel del riesgo = 25

R12 – Valor de nivel del riesgo = 20

R13 – Valor de nivel del riesgo = 15

En el siguiente mapa de calor se ubica cada código de riesgo en la celda que le corresponda según los resultados de la tabla 24, además se ordenan ascendentemente los riesgos según su impacto en la cooperativa esto con el fin de obtener un panorama más claro y sencillo acerca de los riesgos más críticos en la empresa CENECOOP R.L en cuanto al plan de continuidad de negocio se refiere.

Tabla 43 – Mapa de calor

Matriz de exposición (Mapa de calor)			Impacto			
			Muy alto	Alto	Medio	Bajo
Probabilidad	Estimación	Valor	5	4	3	2
Muy alta (MA) – Altamente probable	>90% y <100%	5	R11		R9, R13	
Alta (A) – Muy probable	>70% y <90%	4	R2, R5, R7, R12	R8, R10		
Media (M) – Probable	>40% y <70%	3	R1, R6			
Baja (B) – Poco probable	>10% y <40%	2	R3	R4		
Muy baja (MB) – Muy poco probable	>0% y <10%	1				

Fuente: elaboración propia.

Tabla 44 – Riesgos ordenados ascendentemente

ID	Riesgo	Valor obtenido	Nivel de riesgo inherente
R11	Caídas de los equipos informáticos (dispositivos de red, central telefónica, servidores, UPS).	25	Muy alto
R2	Caída de los sistemas automatizados.	20	Muy alto
R5	Robo de información.	20	Muy alto
R7	Manipulación sensible sin autorización.	20	Muy alto
R12	No se han definido los servicios críticos de TI.	20	Muy alto
R8	Falla en bases de datos.	16	Muy alto
R10	Personal no capacitado para sus funciones.	16	Muy alto
R1	Corte de energía prolongado.	15	Alto
R6	Pérdida de información por ataque informático.	15	Alto
R9	Vencimiento de licencias de software.	15	Alto

R13	No realización de mantenimientos preventivos.	15	Alto
R3	Suspensión de servicios de proveedor de internet.	10	Medio
R4	Incendio o sismo en el edificio.	8	Medio

Fuente: elaboración propia.

5.3 Servicios críticos según norma ISO 22301

En este apartado lo que se busca es determinar cuáles son los servicios críticos de la empresa que de llegar a verse interrumpidos por alguna circunstancia provocaría la interrupción de las operaciones del Centro de Estudios y Capacitación Cooperativa y por ende no se podría aplicar la continuidad del negocio.

5.3.1 Servicios críticos que brinda CENECOOP R.L.

Según las encuestas realizadas a todos los funcionarios de los departamentos de la cooperativa se pudo obtener la información de todos los servicios que brinda la empresa, mismos que se resumen en la tabla 27.

Tabla 45 – Servicios que brinda CENECOOP R.L.

Departamento	Servicios críticos brindados	Descripción
TI	1. Diseño gráfico para cursos virtuales 2. Desarrollo y mantenimiento de software 3. Sitio web de la entidad 4. Seguridad informática 5. Comunicaciones (acceso local a internet) 6. Soporte de averías a empleados 7. Licenciamiento	1. Se hacen etiquetas para la plataforma Moodle de cursos virtuales. 2. Constante actualización de los sistemas utilizados por los departamentos. 3. Capa de presentación para página web. 4. Capacidad de retener ataques informáticos. 5. Soporte a fallas en la red. 6. Mantenimiento de equipos, correos, software y hardware del personal. 7. Compras e instalación se licencias según necesidades requeridas.
Proyectos	1. Venta de servicios	1. Búsqueda constante de nuevos clientes para la venta de servicios.

	2. Control y seguimiento de proyectos	2. Se mantiene contacto con los clientes con proyectos en desarrollo.
IyD	1. Estudio y análisis de la actualidad en necesidad requerida	1. Planificar, dirigir y coordinar actividades de IyD para crear procedimientos o mejorarlos.
Contabilidad	1. Facturación 2. Cobros 3. Reportes 4. Pago a proveedores 5. Proveeduría 6. Declaración de impuestos	1. Se emiten facturas de los servicios brindados. 2. Se realizan los cobros a clientes y cooperativas. 3. Se realizan los reportes según solicitudes de altos mandos. 4. Se realiza la solicitud de dinero para pago a proveedores. 5. Contratación administrativa. 6. Se realizan las declaraciones pertinentes y pagos correspondientes.
Académico	1. Seguimiento a charlas u otras actividades académicas 2. Realización de certificados 3. Venta de cursos virtuales	1. Velar por el buen funcionamiento y convocatorias a actividades académicas. 2. Impresión de certificados físicos y actualización de digitales en plataforma Moodle. 3. Vender cursos libres a cooperativas o estudiantes.
Comunicación	1. Mercadeo en general 2. Servicio al cliente 3. Recursos humanos	1. Marketing digital en redes sociales, sitio web y plataforma educativa. 2. Solución de problemas a estudiantes y clientes. 3. Reclutamiento de personal y mantenimiento de un plantel laboral.
Auditoría	1. Analizar la información financiera	1. Auditar la información financiera y contable de la empresa.

	2. Establecer normas y políticas	2. Auditar a todos los departamentos y analizas informes.
Gerencia	1. Desarrollo de planes de gestión 2. Apoyo en la elaboración de informes a CGR 3. Colaborar en labores de planeamiento para actividades 4. Formular mecanismos de control	1. Desarrollar las actividades asignadas de acuerdo con los planes de gestión con el fin de contribuir al logro de las estrategias, misión, visión y objetivos institucionales. 2. Apoyar a los integrantes del equipo de trabajo del área en la elaboración de informes de mediana y alta complejidad. 3. Organización y desarrollo de eventos cooperativos que requieren presencia del CENECOOP R.L. 4. Garantizar la entrega y comunicación oportuna de los asuntos competencias de la gerencia.
Asesoría legal	1. Autorización de documentos importantes 2. Seguimiento de procesos judiciales	1. Brindar asesoría respecto a contratos que éste deba suscribir en el ejercicio de sus diferentes actividades y proyectos. 2. Atender procesos judiciales que sean asignados por la gerencia o el consejo de administración.

Fuente: elaboración propia.

Todas los servicios y actividades que se detallaron en la tabla 27 tienen su interrelación, debido a que todos los departamentos de una u otra manera necesitan los servicios de TI para su funcionamiento por esta razón es importante identificar los servicios más críticos para posteriormente estimar los tiempos de recuperación, en razón a las posibles alteraciones de los procesos considerados de alta prioridad para el funcionamiento de la infraestructura de TI.

Hay dos departamentos claves en la organización como lo son el financiero y la gerencia, el primero de ellos depende de todos los departamentos anteriores para poder generar el flujo económico de la empresa y el gerencial es el que acata las indicaciones de primera mano brindadas por el Consejo de Administración y el Comité de Vigilancia. Por tanto, una falla en alguno de estos tres departamentos va a afectar significativamente el flujo normal de trabajo de las demás áreas de la empresa.

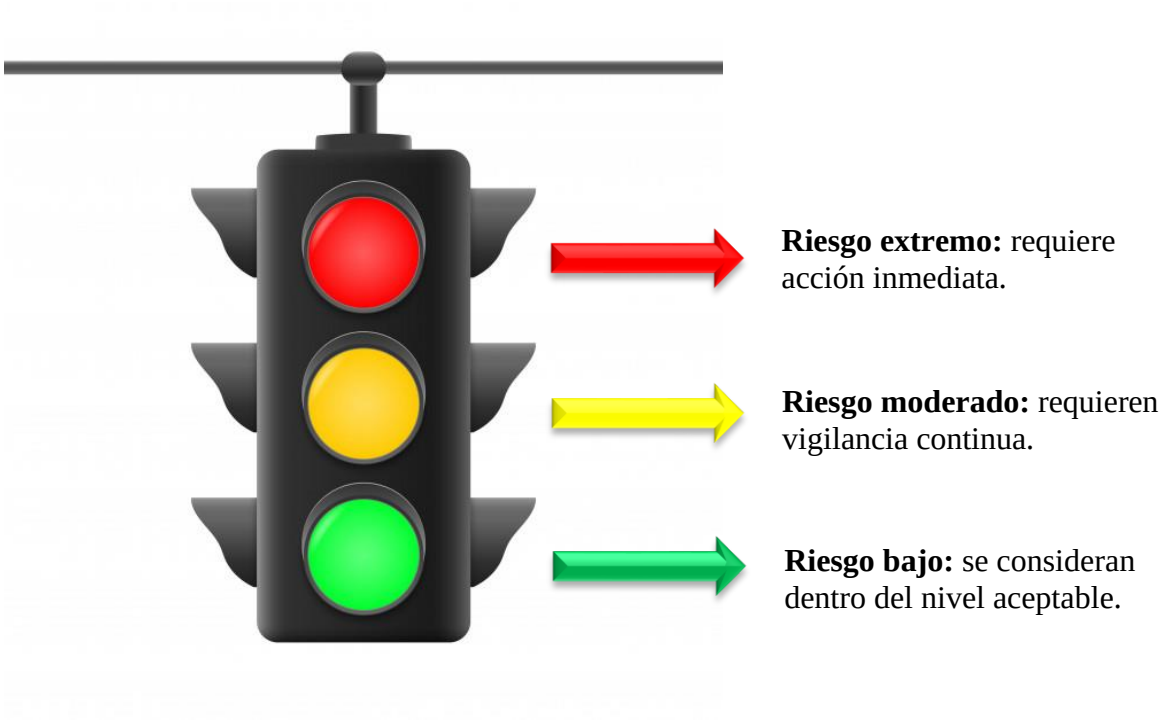
Una vez que se han obtenido cuáles son los servicios más críticos de la cooperativa, se procede a realizar una clasificación de los riesgos para determinar cuáles son los riesgos que deberá atacar CENECOOP R.L y cuales podrá aceptar y así tener un panorama más amplio de hacia donde se debe dirigir los recursos de la empresa para evitar la eventual interrupción de los servicios.

La clasificación de riesgos se realizó mediante entrevistas y discusiones guiadas con las jefaturas de cada uno de los departamentos de la empresa. En la siguiente figura se muestran los riesgos de los servicios críticos de la organización clasificados según la metodología de semáforo de riesgos.

5.3.2 **Semáforo de servicios críticos**

El semáforo se utiliza para realizar la clasificación de los servicios críticos de la organización contra los riesgos. La escala de los riesgos se da en extremo, moderado y bajo, siguiendo los lineamientos que se muestran en la figura 13.

Figura 16 – Descripción de la clasificación de riesgos en el semáforo



Fuente: elaboración propia.

Tabla 46 – Matriz de la herramienta semáforo de riesgos para CENECOOP R.L.

	TI	Proyectos	IyD	Contable	Académico	Comunicación	RRHH	Auditoría	Gerencia	Legal
Seguridad informática	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🔴	🔴	🔴
Acceso local a internet	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Soporte de averías a empleados	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Desarrollo y mantenimiento de sistemas	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🟢
Venta de servicios	🔴	🔴	🟡	🔴	🔴	🔴	🟡	🟡	🔴	🔴
Control y seguimiento de proyectos	🟡	🔴	🟡	🟢	🟡	🟢	🟢	🟢	🟢	🟢
Estudio y análisis de la actualidad en necesidad requerida	🟡	🔴	🔴	🟡	🟢	🟢	🟢	🟢	🟢	🟢
Facturación	🟢	🟢	🟡	🔴	🟡	🟢	🟢	🟡	🔴	🔴
Cobros	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Pago a proveedores	🔴	🟢	🟢	🔴	🟢	🟢	🟢	🟡	🔴	🟢
Seguimiento a charlas u otras actividades académicas	🔴	🟢	🟢	🟢	🔴	🟡	🟢	🟢	🟢	🟢
Venta de cursos virtuales	🔴	🟢	🟡	🔴	🔴	🟡	🟡	🟡	🔴	🟡
Servicio al cliente	🟡	🔴	🟢	🟢	🔴	🔴	🟢	🟢	🟢	🟢
Recursos humanos	🟢	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🟡	🟢
Analizar la información financiera	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🔴	🔴	🟡
Establecer normas y políticas	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🔴	🔴	🔴
Desarrollo de planes de gestión	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🟡
Formular mecanismos de control	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🔴	🟢
Autorización de documentos importantes	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🔴
Seguimiento de procesos judiciales	🟡	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🔴

Fuente: elaboración propia.

En la figura anterior (14) se observa cuales servicios representan para los departamentos de la empresa un riesgo extremo, moderado y bajo, dando una perspectiva de los servicios a los que la cooperativa deba darle una atención inmediata para solventarlos y evitar que se vuelvan incontrolables e incluso provoquen la no continuidad del negocio para CENECOOP R.L, se refleja además cuales servicios se pueden llegar a aceptar, manteniendo siempre una constante vigilancia para visualizar cualquier cambio que pueda modificar el estatus de la valoración.

Se observa también que los servicios extremos del departamento de TI que se definen en la tabla 27 afectan directamente a todos los departamentos de la empresa, el cual es el que tiene el mayor efecto en los empleados pues una vez que el servicio crítico falle los empleados de dicho departamento automáticamente no pueden seguir laborando.

5.3.3 Procedimiento que establece Good Practice Guidelines

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA. Los tiempos de recuperación se describen en capítulo 2, específicamente en el análisis de impacto BIA de la norma ISO 22301.

En cuanto a los procedimientos establecidos por la guía de buenas prácticas es importante señalar que el Business Continuity Institute, en su código de buenas prácticas para la gestión de continuidad del negocio, especifica algunas herramientas que se ajustan a cada etapa del ciclo de vida de la gestión de continuidad del negocio, las cuales son:

- El establecimiento de parámetros como el recovery time objetive (RTO), recovery point objetive (RPO) así como el maximum tolerable period of disruption (MTPD) para la determinación de las estrategias.
- El business impact analisys (BIA). (Business Continuity Institute, 2013)

Se procede a identificar el período máximo de inactividad que puede tolerar una organización de un servicio crítico antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del servicio. Esto indica que si un proceso tiene un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a los de mayor tolerancia.

Tabla 47 – Prioridades de recuperación de procesos críticos

Departamento	Servicio crítico (proceso)	MTD (en días)	Prioridad de recuperación
TI	Diseño gráfico para cursos virtuales	3 días	4
	Desarrollo de software	2 días	3
	Sitio web de la entidad	2 días	3
	Seguridad informática	0.5 días	1
	Comunicaciones (acceso local a internet)	1 día	2
	Soporte de averías a empleados	0.5 días	1
	Licenciamiento	1 día	2
Proyectos	Venta de servicios	1 día	2
	Control y seguimiento de proyectos	2 días	3
IyD	Estudio y análisis de la actualidad en necesidad requerida	3 días	4
Contabilidad	Facturación	1 día	2
	Cobros	0.5 días	1
	Reportes	3 días	4
	Pago a proveedores	2 días	3
	Proveeduría	1 día	2
	Declaración de impuestos	5 días	6
Académico	Seguimiento a charlas u otras actividades académicas	2 días	3
	Realización de certificados	5 días	6
	Venta de cursos virtuales	1 día	2
Comunicación	Mercadeo en general	2 días	3
	Servicio al cliente	0.5 días	1
	Recursos humanos	1 día	2
Auditoría	Analizar la información financiera	0.5 días	1
	Establecer normas y políticas	2 días	3
Gerencia	Desarrollo de planes de gestión	1 día	2
	Apoyo en la elaboración de informes a CGR	0.5 días	1

	Colaborar en labores de planeamiento para actividades	1 día	2
	Formular mecanismos de control	1 día	2
Asesoría legal	Autorización de documentos importantes	0.5 días	1
	Seguimiento de procesos judiciales	1 día	2

Fuente: elaboración propia.

Según los resultados que se muestran en la tabla 28 se determina que hay 7 servicios críticos que la organización no puede esperar más de un día para solucionarlos, ya que tienen prioridad uno (1), además se evidencia que los departamentos que tienen está prioridad de recuperación inmediata son: TI, Contabilidad, Comunicación, Gerencia y Asesoría Legal.

Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los servicios críticos del negocio; por esta razón es clave la identificación de recursos críticos del área de Tecnologías de Información que permitan tomar acciones para medir el impacto del negocio, ya que de acuerdo con los datos obtenidos se puede visualizar que el departamento de TI es el que tiene el período de recuperación en dos servicios críticos que tienen la prioridad uno.

La siguiente tabla representa la identificación de recursos críticos del departamento del Tecnologías de la Información.

Tabla 48 – Identificación de servicios críticos de TI según GPG

Categoría (Función crítica)	**Servicio crítico (Proceso)**	**MTD (en días)**	**Prioridad de recuperación**	**Descripción**
Aplicativos	Sistema financiero	0.5 días	1	Facilitan la gestión y administración de la cooperativa del día a día, el buen funcionamiento es clave en la continuidad del negocio.
	Sistema académico	1 día	2	
	Sistema de facturación	0.5 días	1	
	Comercio electrónico	1 día	2	
	Sitio web	2 días	3	
	Licenciamiento	3 días	4	

	Intranet interna	1 día	2	
Seguridad de la información	Firewall	0.5 días	1	Velar por el cumplimiento de la seguridad informática e impedir todo tipo de ataque cibernético.
	Seguridad en la red	0.5 días	1	
	Seguridad en las computadoras	1 día	2	
	Seguridad de invitados	2 días	3	
Comunicaciones	Conexión a internet	1 día	2	El control de la comunicación es de vital importancia en la empresa.
	Central telefónica	0.5 días	1	
Soporte	Soporte a estudiantes	1 día	2	Se da un soporte a los empleados y estudiantes virtuales en horario de oficina.
	Averías a empleados	0.5 días	1	
	Sistema de respaldos	3 días	4	

Fuente: elaboración propia.

De acuerdo con la tabla 29 se evidencia que son quince los servicios críticos del departamento de Tecnología de la Información que requieren de atención y cuidado, es por está razón que se procede a realizar el impacto de análisis sobre el negocio (BIA) en la cooperativa CENECOOP R.L, la forma de utilización fue con entrevistas guiadas a las jefaturas de los departamentos, de está forma se determinaron y se obtuvieron los servicios más críticos que dependían del departamento de TI.

Con la siguiente tabla, determina las necesidades temporales (RTO), limitaciones de pérdida de datos (RPO) para cada uno de los procesos de la empresa desde el punto de vista de la continuidad del negocio, para estas valoraciones se utilizan las tablas 3 y 4 del capítulo II, referentes a RTO y RPO.

Tabla 49 – Análisis de impacto en el negocio según guía de buenas prácticas

Departamento	Servicio crítico (proceso)	Depende de TI	RTO	RPO	¿Cubre los requisitos del negocio?
TI	Diseño gráfico para cursos virtuales	Sí	4	3	Pobremente
	Desarrollo de software	Sí	3	2	Pobremente
	Sitio web de la entidad	Sí	1	1	Completamente
	Seguridad informática	Sí	1	1	Completamente
	Comunicaciones (internet)	Sí	2	1	Pobremente
	Soporte de averías a empleados	Sí	2	2	Completamente
	Licenciamiento	Sí	3	3	Completamente
Proyectos	Venta de servicios	Sí	1	1	Completamente
	Control y seguimiento de proyectos	No	2	2	Completamente
IyD	Estudio y análisis de la actualidad en necesidad requerida	No	3	3	Completamente
Contabilidad	Facturación	Sí	2	1	Pobremente
	Cobros	Sí	1	1	Completamente
	Reportes	Sí	3	2	Pobremente
	Pago a proveedores	No	3	3	Completamente
	Proveeduría	Sí	2	2	Completamente
	Declaración de impuestos	No	3	2	Pobremente

Académico	Seguimiento a charlas u otras actividades académicas	Sí	3	4	Completamente
	Realización de certificados	No	2	2	Completamente
	Venta de cursos virtuales	Sí	1	1	Completamente
Comunicación	Mercadeo en general	No	2	2	Completamente
	Servicio al cliente	No	2	2	Completamente
	Recursos humanos	No	2	1	Pobremente
Auditoría	Analizar la información financiera	No	2	1	Pobremente
	Establecer normas y políticas	No	3	3	Completamente
Gerencia	Desarrollo de planes de gestión	Sí	2	2	Completamente
	Apoyo en la elaboración de informes a CGR	No	3	3	Completamente
	Colaborar en labores de planeamiento para actividades	No	3	3	Completamente
	Formular mecanismos de control	No	2	2	Completamente
Asesoría legal	Autorización de documentos importantes	No	3	2	Pobremente
	Seguimiento de procesos judiciales	No	2	1	Pobremente

Fuente: elaboración propia.

Según los resultados que se muestran en la tabla anterior se puede observar que los servicios críticos de CENECOOP R.L deben mejorar en algunos puntos, en especial brindar una mayor atención en los servicios que presentan un tiempo de recuperación permitido en uno (1) según el análisis de BIA efectuado en la tabla 30.

El departamento de tecnología de información toma un papel trascendental en este proceso, ya que si bien es cierto todas las áreas de la cooperativa son importantes, la que más repercute en los servicios críticos de cada una de ellas es TI, reportando ser un área operativa pese a que se le ha caracterizado a lo largo de la historia por ser un poco estratégica. Además, se debe de prestar atención al departamento de contabilidad, donde sus servicios dependen enormemente del área tecnológica y es debido a la gran cantidad de sistemas que poseen en dicha unidad.

5.4 Implementación de Plan de Continuidad de Negocio (BCP)

En este apartado se realiza la propuesta del plan de continuidad de negocio para la empresa CENECOOP R.L, una vez efectuado el diagnóstico y análisis de la organización. Para la implementación del plan de continuidad, se analizan los resultados y se ejecuta una evaluación de aceptación, colaboración y cumplimiento de los objetivos del plan.

En la realización del plan de continuidad de negocio para CENECOOP R.L, una vez que se ha efectuado el diagnóstico y análisis de la organización, se recoge la información necesaria, se crean nuevas plantillas, de acuerdo con lo estipulado en la ISO 22301 y el COBIT. Para la implementación del plan, se usan los criterios de los entregables de este documento, los cuáles son explicados y entregados a los encargados de la organización. A continuación, se detallan los entregables:

- Diagnóstico y análisis de la situación actual.
- Diseño de la metodología y plantillas a considerar.

Ahora bien, los pasos para la implementación del plan de continuidad de negocio para la cooperativa son:

1. Diagnosticar y analizar la situación actual de la institución, este punto se desarrolla en la sección 5.2 de este documento. Se debe tomar en cuenta:
    - ✓ Análisis de impacto.
    - ✓ Análisis de riesgos.
    - ✓ Identificación de riesgos.
    - ✓ Evaluación de los riesgos.
2. Diseñar la metodología y definir las necesidades de la organización. Se realiza en la sección 3 del documento, este punto se desarrolla según diagnostico hecho en la cooperativa y se toma como referencia el marco de trabajo y la ISO 22301.
3. Cuando se llega a este punto la situación de CENECOOP R.L, posee un panorama más claro, al ya tener conocimiento sobre todos los riesgos, identificación de servicios críticos para la institución en caso de una interrupción de servicios. Se determinan los riesgos relevantes que pueden generar una brecha importante en la organización en caso de ocurrir y se determina la estrategia a utilizar. La ISO 22301 menciona las operaciones a seguir para implementar los procedimientos:

a) Establecer protocolo de comunicación interna y externa.
b) Ser específicos a las medidas inmediatas que deben tomarse durante caída del servicio.
c) Ser flexible para poder responder a amenazas imprevistas y cambiantes.
d) Centrarse en el impacto de los eventos que podrían generar una mayor pérdida en las operaciones de CENECOOP R.L.
e) Desarrollar en base a los supuestos establecidos.
f) No lo indica la norma, pero considero realmente de mucha utilidad la creación de una base del conocimiento para el manejo del plan de continuidad del negocio.

5.4.1 **Fase I – Recopilación de datos**

En esta sección se reúnen los datos necesarios tales como: actividades, activos y medidas de defensa de cada proceso que es tomado en cuenta para el caso de aplicación.

En la tabla 31 re resume una ficha técnica con información de la empresa CENECOOP R.L y el departamento de TI.

Tabla 50 – Ficha técnica CENECOOP R.L.

Nombre de la empresa	Centro de Estudios y Capacitación Cooperativa R.L (CENECOOP R.L.)
Línea de negocio	Capacitación
Empresas relacionadas	6
Empresa del caso de estudio	San Pedro (CENECOOP R.L.)
Dirección	Edificio Cooperativo, detrás del Mall San Pedro
Teléfono	2528-5820
Gerente general	Rodolfo Navas Alvarado
Número de empleados	27
Número de personal del departamento de TI	4
Número de laptops instaladas	17
Número de desktops instaladas	7

Número de servidores	4
Número de aplicaciones	10
Servicios críticos de TI	• Corte de energía prolongado. • Caída de los sistemas automatizados. • Suspensión de servicios de proveedor de internet. • Incendio o sismo en el edificio. • Robo de información. • Pérdida de información por ataque informático. • Manipulación sensible sin autorización. • Falla en bases de datos. • Vencimiento de licencias de software. • Personal no capacitado para sus funciones. • Caídas de los equipos informáticos (dispositivos de red, central telefónica, servidores, UPS). • No se han definido los servicios críticos de TI. • No realización de mantenimientos preventivos.

Fuente: elaboración propia.

5.4.1.1 **Corte de energía prolongado**

Tabla 51 – Corte de energía prolongado

CENECOOP R.L.	**Servicio crítico:** corte de energía prolongado				Versión 1.0
Persona responsable:	Rodolfo Navas Alvarado				
Puesto:	Gerente general				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	El edificio es antiguo, debe mejorar en infraestructura física en todos sus pisos.			
Aplicaciones	■	Aplicaciones de recuperación y restauración de datos.			
Operaciones	■	Mínimo mantenimiento a las UPS e inclusive actualmente la fuente de corriente principal está dañada.			
Personal	■	Directrices con recursos humanos.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				
☐ Irrecuperable ☑ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☐ > 24 horas	1. Verificar estado del generador eléctrico en la cooperativa. 2. Velar por el funcionamiento de las UPS. 3. Revisar que la falla sea externa y no un tema de toma corrientes de la institución. 4. Coordinar con ICE para que solucione a la brevedad.				
¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?			

☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 100.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
Todos los equipos físicos de la institución.	201.198.XXX.XXX	2 horas.
Tiempo total de recuperación del proceso	3 ☑ horas ☐ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.1.2 **Caída de los sistemas automatizados**

Tabla 52 – Caída de los sistemas automatizados

CENECOOP R.L.	**Servicio crítico:** caída de los sistemas automatizados			Versión 1.0	
Persona responsable:	Alonso Salazar Céspedes				
Puesto:	Coordinador de TI				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	Equipo de empleados que utilizan los sistemas están obsoletos.			
Aplicaciones	■	Aplicaciones con poco mantenimiento.			

Operaciones	■	No se brinda un mantenimiento a las bases de datos ni a los archivos de los sistemas automatizados.
Personal	■	Requisitos de seguridad, empleados reportan problema hasta que sistema deja de funcionar.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☑ 8-24 horas ☐ > 24 horas	1. Reportar incidente al departamento de TI. 2. Asignar un técnico al problema reportado. 3. El técnico asignado revisa la falla y soluciona, en caso de que no pueda solucionar lo reporta al coordinador. 4. Coordinador resuelve y se hacen las pruebas para verificar el funcionamiento.

¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?
☐ 2-5 horas ☐ 5-12 horas ☑ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 50.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.

Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
Departamento afectado de acuerdo con el sistema crítico caído.	201.198.XXX.XXX	15 horas.
Tiempo total de recuperación del proceso	24 ☑ horas ☐ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.1.3 **Suspensión de servicios de proveedor de internet**

Tabla 53 – Suspensión de servicios de proveedor de internet

CENECOOP R.L.	**Servicio crítico:** suspensión de servicios de proveedor de internet			Versión 1.0	
Persona responsable:	Alonso Salazar Céspedes				
Puesto:	Coordinador de TI				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	El equipo físico de red de la cooperativa no se renueva desde el año 2012, no se hacen mantenimientos.			
Aplicaciones	■	No aplica directamente con el servicio crítico.			
Operaciones	■	Dependencia de un solo proveedor.			
Personal	■	Conocimiento de seguridad, directrices por parte de TI.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				
☐ Irrecuperable ☑ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☐ > 24 horas	1. Reportar incidente al departamento de TI. 2. Asignar un técnico al problema reportado por el empleado. 3. El técnico asignado revisa la falla y soluciona, en caso de que no pueda solucionar lo reporta al coordinador. 4. Coordinador llama al proveedor de servicios de internet, por ser una línea empresarial el problema debería de resolverse en las primeras 2 horas, de no ser algún problema con cableado externo de la organización.				
¿Tiempo en recibir pérdidas económicas?	Importancia de los datos		¿Hay pérdidas económicas en dinero?		

☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 250.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio y por cantidad de empleados.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
Todos los equipos físicos conectado a la red de CENECOOP R.L.	201.198.XXX.XXX	2 horas
Tiempo total de recuperación del proceso	3 ☑ horas ☐ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.1.4 **Desastre natural en el edificio cooperativo**

Tabla 54 – Desastre natural en el edificio cooperativo

CENECOOP R.L.	**Servicio crítico:** desastre natural en el edificio cooperativo (incendios, inundaciones o terremotos)				Versión 1.0
Persona responsable:	Evelyn Obando Pereira				
Puesto:	Comunicación e imagen				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			

Infraestructura	■	El edificio es antiguo, debe mejorar en infraestructura física en todos sus pisos.
Aplicaciones	■	No aplica directamente con el servicio crítico.
Operaciones	■	Velar por el cumplimiento en todos los departamentos en las medidas de seguridad impuestas por la comisión de brigadistas.
Personal	■	Se debe mejorar en los requisitos e instrucciones de seguridad en todos los pisos del departamento.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☑ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☐ > 24 horas	1. Reportar el desastre al equipo de brigadistas que lo conforma la compañera Evelyn Obando junto con los demás integrantes de las cooperativas del mismo edificio. 2. Iniciar proceso de evacuación y control del desastre. 3. Verificar que todas las personas se encuentren bien, posteriormente revisar las instalaciones. 4. Reportar al departamento de TI los posibles fallos en equipos o sistemas. 5. Realizar las reparaciones de los equipos de ser posible.

¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?
☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 250.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.

Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
Infraestructura física de CENECOOP R.L.	–	3 días
Infraestructura físico y lógica de la red en la cooperativa.	201.198.XXX.XXX	2 días
Tiempo total de recuperación del proceso	6 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.1.5 **Robo de información**

Tabla 55 – Robo de información

	Servicio crítico: robo de información				Versión 1.0
Persona responsable:	Alonso Salazar Céspedes				
Puesto:	Coordinador de TI				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	Mejorar el equipo de red de la institución.			
Aplicaciones	■	Las computadoras de los empleados no cuentan con software especializado para la prevención de pérdida de datos, además no hay cortafuegos en equipos de red.			
Operaciones	■	Cifrar la información confidencial que viaja a través de la red, mantener siempre actualizadas las aplicaciones que usa la organización.			

Personal	▪	El personal de la institución no se ha capacitado en aspectos de seguridad de la información, deben conocer la información sensible que gestiona CENECOOP R.L.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☑ > 24 horas	1. Reportar o anticipar el incidente al departamento de TI. 2. El coordinador analiza el caso. 3. Examina el tipo de robo de información tecnológica para identificar criticidad de la institución. 4. Definir acciones tanto preventivas como correctivas para evitar este tipo de operaciones.

¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?
☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☑ > 2 días	☐ Irremplazables ☑ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 25.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.

Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
PC o servidor	PC: 201.198.XXX.XXX Servidor en la nube: 192.252.XXX.XXX	3 días

Tiempo total de recuperación del proceso	3 ☐ horas ☑ días ☐ semanas ☐ meses

Fuente: elaboración propia.

5.4.1.6 **Pérdida de información por ataque informático**

Tabla 56 – Pérdida de información por ataque informático

CENECOOP R.L.	**Servicio crítico:** pérdida de información por ataque informático			Versión 1.0	
Persona responsable:	Alonso Salazar Céspedes				
Puesto:	Coordinador de TI				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	El equipo de red es bastante obsoleto.			
Aplicaciones	■	Actualización de equipo de red y software en servidores.			
Operaciones	■	No realización de copias de seguridad en computadoras de los empleados de la compañía.			
Personal	■	No se advierte al personal de posibles peligros informáticos, no poseen restricciones de páginas web o enlaces sospechosos.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☑ 8-24 horas ☐ > 24 horas	1. Reportar o anticipar el incidente al departamento de TI. 2. Todo el departamento de TI se reúne y responden lo más rápido posible ante el ataque. 3. Examina el tipo de robo de información tecnológica para identificar criticidad de la institución. 4. Definir acciones tanto preventivas como correctivas para evitar este tipo de operaciones. 5. Iniciar restauración en servidores o computadoras atacadas con base en respaldos realizados.				

¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?
☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 42.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
PC o servidor	PC: 201.198.XXX.XXX Servidor en la nube: 192.252.XXX.XXX	2 días
Tiempo total de recuperación del proceso	3 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.1.7 **Manipulación sensible sin autorización**

Tabla 57 – Manipulación sensible sin autorización

CENECOOP R.L.	**Servicio crítico:** manipulación sensible sin autorización				Versión 1.0
Persona responsable:	Alonso Salazar Céspedes				
Puesto:	Coordinador de TI				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	No aplica directamente con el servicio crítico.			

Aplicaciones	▪	Se puede mejorar en aspectos de software especializado de auditoría informática para la información.
Operaciones	▪	Informar a los empleados acerca documentos sensibles.
Personal	▪	Mínimas directrices del departamento de Tecnologías de la Información.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☐ Irrecuperable ☑ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☐ > 24 horas	1. Reportar o anticipar el incidente al departamento de TI. 2. Verificar que el empleado sin autorización no haya reenviado la información confidencial. 3. Suprimir la información de la persona sin autorización. 4. Crear política para garantizar la no transferencia de información consideradas como confidenciales sin autorización previa.

¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?
☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☑ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 100.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.

Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
Cualquier dispositivo móvil o computador de donde salió la información	201.198.XXX.XXX	1 hora

Tiempo total de recuperación del proceso	1 ☑ horas ☐ días ☐ semanas ☐ meses

Fuente: elaboración propia.

5.4.1.8 **Falla en bases de datos**

Tabla 58 – Falla en base de datos

CENECOOP R.L.	**Servicio crítico:** falla en base de datos				Versión 1.0
Persona responsable:	Alonso Salazar Céspedes				
Puesto:	Coordinador de TI				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	No aplica en el proceso ya que los motores de bases de datos en CENECOOP R.L se encuentran en la nube.			
Aplicaciones	■	Se debe actualizar las bases de datos SQL y MySQL, además de darle un mantenimiento constante a cada una de ellas.			
Operaciones	■	No se realizan respaldos a todas las bases de datos de la institución.			
Personal	■	Mínima capacitación a empleados sobre la utilización de sistemas de la cooperativa.			
¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?				
☑ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas	1. Reportar la falla al departamento de TI. 2. Asignar un técnico al problema para que revise la falla. 3. El técnico reporta la falla al coordinador.				

☑ 8-24 horas ☐ > 24 horas	4. El coordinador repara la falla en la base de datos en caso de no ser así obtener respaldos para proceder con la restauración de la base de datos. 5. Hacer pruebas para comprobar que el problema ha sido solventado.	
¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?
☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 100.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
Servidor	192.252.XXX.XXX	8 horas
Servidor	198.38.XXX.XXX	8 horas
Tiempo total de recuperación del proceso	1 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.1.9 **Vencimiento de licencias de software**

Tabla 59 – Vencimiento de licencias de software

CENECOOP R.L.	**Servicio crítico:** vencimiento de licencias de software	Versión 1.0
Persona responsable:	Mauriel Cabalceta Calderón	
Puesto:	Asistente de TI	
Simbología		

Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■

Listado de medidas de defensa	Estado	Actividad del proceso
Infraestructura	■	Algunas computadoras de empleados obsoletas por lo que es difícil la actualización de sistemas.
Aplicaciones	■	Escasa actualización del personal de TI en los sistemas administrativos instalados en las computadoras de los empleados.
Operaciones	■	El personal de TI debe tener un mayor control sobre el software que se instala en CENECOOP R.L, además es necesario la implementación de un software para limitar la descarga de programas en la red interna de la cooperativa.
Personal	■	Poca capacitación al personal, para que alerte del tema y conozca de los peligros.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☑ 8-24 horas ☐ > 24 horas	1. Reportar o anticipar el incidente al departamento de TI. 2. Asignar un técnico a la computadora o servidor con licencia caducada o próxima a vencer y revisar la información de esta. 3. Solicitar al coordinador boleta para adquisición de compra de licenciamiento al departamento financiero. 4. Instalación de software y verificación que problema sea resuelto.

¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?

☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☑ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 50.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
Cualquier computador de CENECOOP R.L.	201.198.XXX.XXX	1 hora
Servidores	198.38.XXX.XXX 192.252.XXX.XXX	12 horas
Tiempo total de recuperación del proceso	2 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.1.10 **Personal no capacitado para sus funciones**

Tabla 60 – Personal no capacitado para sus funciones

CENECOOP R.L.	**Servicio crítico:** personal no capacitado para sus funciones			Versión 1.0	
Persona responsable:	Evelyn Obando Pereira y Alonso Salazar Céspedes				
Puesto:	Coordinadora de recursos humanos y Coordinador de TI.				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	No aplica directamente con el servicio crítico.			
Aplicaciones	■	No aplica directamente con el servicio crítico.			

Operaciones	■	Escasa planificación, directrices y políticas de capacitaciones de los altos mandos de CENECOOP R.L.
Personal	■	Falta de preparación ante cualquier eventualidad al departamento de TI. Mínima o nula capacitación al personal nuevo. El personal de TI no cuenta con un proceso que le permita identificar si se encuentra ante una situación relacionada a contingencia.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☑ > 24 horas	1. El técnico debe reportar al coordinador de TI su inexperiencia en la tarea asignada. 2. El jefe del departamento debe reunir al personal de TI para realizar una estructura de entrenamiento para los involucrados. 3. Es responsabilidad del departamento mantener actualizados los entrenamientos del área. 4. El técnico debe lograr resolver el inconveniente inicial.

¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?
☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☑ > 2 días	☐ Irremplazables ☐ Importantes ☑ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: (sin estimación), multiplicado por la cantidad de horas que no hubo servicio.

Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración

Computadoras del departamento de TI	201.198.XXX.XXX	15 días
Tiempo total de recuperación del proceso	1 ☐ horas ☐ días ☐ semanas ☑ meses	

Fuente: elaboración propia.

5.4.1.11 **Caídas de los equipos informáticos**

Tabla 61 – Caídas de los equipos informáticos

CENECOOP R.L.	**Servicio crítico:** caídas de los equipos informáticos			Versión 1.0	
Persona responsable:	Alonso Salazar Céspedes				
Puesto:	Coordinador de TI				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	El edificio es antiguo, por lo que hay mucha humedad y polvo que cae en los equipos de CENECOOP R.L.			
Aplicaciones	■	Mínima actualización de software en los equipos de red y computadoras que pueden repercutir en el fallo de equipos informáticos.			
Operaciones	■	Este es el principal problema de las caídas, el último mantenimiento que realizó el departamento de TI al equipo de red fue en el año 2014, por lo que las caídas son constantes en la red.			
Personal	■	El personal de Tecnología de la Información no está comprometido con el cargo, ya que estos problemas son continuos y solamente lo resuelven momentáneamente.			

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?	
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☑ 8-24 horas ☐ > 24 horas	1. Reportar el daño al departamento de TI. 2. Asignar un técnico al problema reportado. 3. El técnico asignado revisa el equipo y reporta el tipo y la gravedad del daño. (Verificar si el equipo posee garantía) 4. Si no aplica la garantía el técnico de TI puede reparar el equipo o el proveedor lo repara con un costo adicional. 5. Hacer pruebas para verificar que la falla sea resuelta.	
¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?
☑ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☐ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 250.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
Equipos de red	201.198.XXX.XXX	1 día
Tiempo total de recuperación del proceso	3 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.1.12 **No se han definido los servicios críticos de TI**

Tabla 62 – No se han definido los servicios críticos de TI

CENECOOP R.L.	**Servicio crítico:** no se han definido los servicios críticos de TI	Versión 1.0

Persona responsable:	Alonso Salazar Céspedes				
Puesto:	Coordinador de TI				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■

Listado de medidas de defensa	Estado	Actividad del proceso
Infraestructura	■	No aplica directamente con el servicio crítico.
Aplicaciones	■	No aplica directamente con el servicio crítico.
Operaciones	■	No se tienen definidos los servicios críticos vinculados con la continuidad del servicio.
Personal	■	El personal de TI no le ha dado la atención que requiere los servicios críticos de la institución.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☑ > 24 horas	1. Los altos mandos deben programar una reunión con todo el personal de la cooperativa CENECOOP R.L. 2. Se le indica a cada coordinador que se reúna internamente con las personas del área para que cada departamento determine los servicios críticos que desarrollan. 3. Programar una reunión general y el auditor interno debe generar un documento formal con todos los riesgos descritos por cada uno de los departamentos. 4. Cada área debe dar seguimiento a sus respectivos servicios críticos.

¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?

☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☑ > 2 días	☑ Irremplazables ☐ Importantes ☐ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 200.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.
Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración
Cualquier computador de CENECOOP R.L.	201.198.XXX.XXX	No aplica
Tiempo total de recuperación del proceso	7 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.1.13 **No realización de mantenimientos preventivos**

Tabla 63 – No realización de mantenimientos preventivos

CENECOOP R.L.	**Servicio crítico:** no realización de mantenimientos preventivos			Versión 1.0	
Persona responsable:	Mauriel Cabalceta Calderón				
Puesto:	Asistente de TI				
Simbología					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Listado de medidas de defensa	Estado	Actividad del proceso			
Infraestructura	■	No aplica directamente con el servicio crítico.			
Aplicaciones	■	Algunas aplicaciones utilizadas por la cooperativa son obsoletas por lo que su mantenimiento se vuelve engorroso.			

Operaciones	▪	Debido al mínimo mantenimiento muchos equipos presentan fallos que pudieron haberse reparado con el soporte adecuado.
Personal	▪	El personal de TI no saca el tiempo adecuado para actualizar equipos físicos tanto de empleados, como red interna ni mucho menos una limpieza o actualización en las versiones.

¿Tiempo estimado en la recuperación de la información?	¿Cómo se procede para combatir el servicio crítico?
☐ Irrecuperable ☐ 0-4 horas ☐ 4-8 horas ☐ 8-24 horas ☑ > 24 horas	1. El coordinador de informática debe organizar una reunión con todo el personal del departamento. 2. Comunicarles acerca de la necesidad de los riesgos por la no realización de mantenimiento en CENECOOP R.L. 3. Asignar a un responsable por semana (incluido el coordinador) para la ejecución de cada uno de los mantenimientos propuestos (impresoras, computadoras, equipo de red, servidores). 4. Informar al coordinador de la labor completada para que sea anotada en bitácora.

¿Tiempo en recibir pérdidas económicas?	Importancia de los datos	¿Hay pérdidas económicas en dinero?
☐ 2-5 horas ☐ 5-12 horas ☐ 12-24 horas ☐ 1-2 días ☑ > 2 días	☐ Irremplazables ☐ Importantes ☑ Algo importante ☐ Sin importancia	☑ Sí ☐ No Sí la respuesta es afirmativa, indique el monto aproximado de pérdida económica: 150.000 colones por hora, multiplicado por la cantidad de horas que no hubo servicio.

Recursos tecnológicos que soportan este proceso: (Información se completa con ayuda de personal de TI)		
Nombre de equipos	IP del equipo	Tiempo de restauración

Cualquier computador de CENECOOP R.L.	201.198.XXX.XXX	4 horas
Equipos de red	201.198.XXX.XXX	1 día
Tiempo total de recuperación del proceso	2 ☐ horas ☑ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

Tabla 64 – Autorización servicios críticos de TI

Revisión		
	Nombre	**Firma**
Realizado por:	Fabián Soto Bogantes	
Revisado por:	Coordinador de TI	
Autorizado por:	Gerente general	

Fuente: elaboración propia.

5.4.2 Fase II – Aplicación del plan de continuidad del negocio

Los procesos críticos identificados tienen medidas de defensa que necesitan ser mejoradas y en otros casos implementadas debido a la nula existencia según menciona el marco de trabajo COBIT en su sección DS4, en el punto 5.4.3 se describen las medidas de defensa que se deben tomar en cuenta.

5.4.3 Medidas de defensa para garantizar la continuidad del servicio (DS4)

El objetivo de este apartado del documento es emitir un criterio al área de Tecnología de Información sobre el cumplimiento de los controles en el proceso de COBIT 5, específicamente en su sección DS4, además de recomendar oportunidades de mejora y agregar valor, para garantizar de manera razonable la efectividad, eficiencia y disponibilidad de los servicios críticos del Centro de Estudios y Capacitación Cooperativa R.L. A continuación de detalla cada uno de los objetivos de control del marco de gestión de TI donde se señala la recomendación o estructura de plantilla que se debe tomar en cuenta para una efectiva aplicación del plan de continuidad de negocio.

5.4.3.1 **DS4.4 – Mantenimiento del Plan de Continuidad de TI**

Según la norma COBIT en el apartado DS4.4 se deben realizar mantenimientos de forma constante y clara, el marco de gestión de TI lo define como: "exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna" (p. 114)

El propósito de mantener actualizada la documentación cada vez que se produce un cambio importante en la organización a nivel de infraestructura, operaciones, personal, aplicaciones de TI o de cualquier otro proceso implicado en los procesos críticos de la cooperativa. Esto permite que la documentación se utilice ante una situación de crisis que refleje la información de distintos actores involucrados en los procesos que se deben tener en cuenta en una situación de contingencia.

Tabla 65 – Mantenimiento de los servicios críticos

CENECOOP R.L.	**Actualización de servicio crítico:**				Fecha y hora:
Persona responsable:					
Equipo responsable:					
Puesto:					
Diagnóstico del servicio					
Cumple las mejores prácticas	■	Necesita mejorar	■	Carencias severas	■
Impacto en la organización	Estado	Causa		Solución	
Infraestructura					
Aplicaciones					
Operaciones					
Personal					
¿El servicio se encuentra detenido actualmente?				☐ Sí ☐ No	

¿Se han reportado fallas en el servicio crítico recientemente?			☐ Sí ☐ No
Recursos tecnológicos que soportan este proceso:			
Nombre de equipos	IP del equipo	Tiempo de restauración	
Tiempo total de recuperación del proceso		☐ horas ☐ días ☐ semanas ☐ meses	

Fuente: elaboración propia.

5.4.3.2 **DS4.5 – Pruebas del Plan de Continuidad de TI**

Según la norma COBIT en el apartado DS4.5 se realiza la estructura del plan de pruebas, según la norma se define como: "probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta apunta y en pruebas integradas con el proveedor." (p. 114)

Se aplica la plantilla para la documentación del plan de pruebas, se conforma por datos generales, participantes, detalles de pruebas, programación, revisión y autorización; estos campos son los sugeridos por la empresa CENECOOP R.L para su implementación.

- Datos generales: se le debe poner un id a cada prueba, registro de fecha de creación, alcance que consiste en lo que se va a realizar, donde y para qué.
- Recursos necesarios: son los recursos necesarios que dependen de la prueba, puede ser desde una computadora hasta un servidor.
- Participantes del equipo: es el punto más importante de la plantilla se completa el nombre del personal o proveedor y documentar las funciones del empleado durante la ejecución de la prueba.
- Detalles de la prueba: objetivo principal de la prueba, fecha y hora de inicio, tipo de prueba y la existencia de alguna condición para el cumplimiento de la prueba (opcional) y en caso de que haya cierta observación.

- Programación: listado de actividades para realizar en cada prueba, fecha y hora, el responsable de la ejecución de cada actividad y en caso de que haya alguna observación.
- Revisión: quién revisa y autoriza.

Tabla 66 – Diseño del plan de pruebas

CENECOOP Crecemos Juntos	**Datos generales**	
ID	Fecha de creación	Alcance
Recursos necesarios		
Recursos necesarios para la prueba	Descripción	
Participantes		
Nombre completo	**Empleado o proveedor**	**Actividades por ejecutar**
Detalles de la prueba		
Objetivo de la prueba		
Fecha y hora programada		
Hora de retorno		
Tipo de prueba		
Condiciones para cancelar prueba		
Observaciones		
Programación de actividades		
Nombre de actividad	Fecha de inicio	Responsable	Observaciones
Revisión		
	Nombre	Firma
Realizado por:		
Revisado por:		

Autorizado por:		

Fuente: elaboración propia.

5.4.3.3 **DS4.6 – Entrenamiento del Plan de Continuidad de TI**

En el apartado DS4.6 de los objetivos de control del COBIT señala: “asegurarse de que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.” (p. 114)

Se muestra la estructura de la plantilla para los servicios de capacitación en CENECOOP R.L.

Tabla 67 – Propuesta de capacitación a la continuidad de los servicios tecnológicos

CENECOOP Crecemos Juntos	**Datos generales**		
Expositor	Fecha de creación		Duración
Datos de capacitación			
ID	Objetivo capacitación	Área	Método de capacitar
Contenidos			
Listado de contenidos	1.		
Asistencia			
Área	Nombre	Firma	Observaciones
Revisión			
	Nombre		Firma
Realizado por:			
Revisado por:			
Autorizado por:			

Fuente: elaboración propia.

5.4.3.4 **DS4.7 – Distribución del Plan de Continuidad de TI**

Según la norma COBIT en el apartado DS4.7 se define la distribución del plan de continuidad de TI en: "determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre." (p. 114)

Para el caso de CENECOOP R.L al existir solamente 4 personas en el departamento de TI, cada uno de los miembros debe cumplir con varias tareas por lo que el equipo se distribuye de la siguiente manera:

- Equipo de administración de crisis: Rodolfo Navas Alvarado.
- Equipo de notificación: Evelyn Obando Pereira.
- Coordinador de la continuidad del negocio: Alonso Salazar Céspedes.
- Equipo de recuperación de backups: Mauriel Cabalceta Calderón.
- Equipo de coordinación de soporte: Guillermo Hidalgo Blanco / Mauriel Cabalceta Calderón.
- Equipo de redes y telecomunicaciones: Mauriel Cabalceta Calderón.
- Equipo de respuesta de emergencia: Marco Aurelio Salazar.
- Equipo de aplicaciones: Alonso Salazar Céspedes.
- Equipo de evaluación y daños: Guillermo Hidalgo Blanco / Mauriel Cabalceta Calderón
- Equipo de recuperación de respaldos de registros críticos: Mauriel Cabalceta Calderón.
- Equipo de integración y pruebas: Mauriel Cabalceta Calderón / Alonso Salazar Céspedes.
- Equipo de controles de seguridad: Alonso Salazar Céspedes.
- Equipo de logística y suministro de recursos: Evelyn Obando Pereira / Marco Aurelio Salazar.
- Equipo de coordinación y soporte: Mauriel Cabalceta Calderón.

Tabla 68 – Distribución de roles por actividades de negocio

CENECOOP Crecemos Juntos	**Conformación de roles**	
Riesgo crítico	**Equipos responsables**	**Personas responsables**

Corte de energía prolongado.	Equipo de administración de crisis. Equipo de notificación. Coordinador de la continuidad del negocio. Equipo de recuperación de backups.	Rodolfo Navas Alvarado. Alonso Salazar Céspedes. Evelyn Obando Pereira. Mauriel Cabalceta Calderón.
Caída de los sistemas automatizados.	Equipo de administración de crisis. Equipo de notificación. Coordinador de la continuidad del negocio. Equipo de coordinación de soporte Equipo de aplicaciones	Rodolfo Navas Alvarado. Alonso Salazar Céspedes. Evelyn Obando Pereira. Guillermo Hidalgo Blanco.
Suspensión de servicios de proveedor de internet.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de notificación. Equipo de redes y telecomunicaciones.	Rodolfo Navas Alvarado. Alonso Salazar Céspedes. Evelyn Obando Pereira. Mauriel Cabalceta Calderón.
Incendio o sismo en el edificio.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de notificación. Equipo de respuesta de emergencia Equipo de evaluación y daños	Rodolfo Navas Alvarado. Alonso Salazar Céspedes. Evelyn Obando Pereira. Marco Aurelio Salazar. Mauriel Cabalceta Calderón.
Robo de información.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de controles de seguridad Equipo de integración y pruebas. Equipo de recuperación de respaldos de registros críticos. Equipo de evaluación y datos	Rodolfo Navas Alvarado. Alonso Salazar Céspedes. Evelyn Obando Pereira. Mauriel Cabalceta Calderón. Guillermo Hidalgo Blanco. Marco Aurelio Salazar.
Pérdida de información por ataque informático.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de controles de seguridad Equipo de integración y pruebas.	Rodolfo Navas Alvarado. Alonso Salazar Céspedes. Evelyn Obando Pereira. Mauriel Cabalceta Calderón. Guillermo Hidalgo Blanco.

	Equipo de recuperación de respaldos de registros críticos. Equipo de evaluación y daños	Marco Aurelio Salazar.
Manipulación sensible sin autorización.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de controles de seguridad Equipo de evaluación y daños	Rodolfo Navas Alvarado. Alonso Salazar Céspedes. Mauriel Cabalceta Calderón. Marco Aurelio Salazar.
Falla en bases de datos.	Equipo de administración de crisis. Coordinador de la continuidad del negocio. Equipo de evaluación y daños Equipo de recuperación de backups de registros críticos y datos.	Alonso Salazar Céspedes. Mauriel Cabalceta Calderón. Guillermo Hidalgo Blanco.
Vencimiento de licencias de software.	Equipo de notificación. Equipo de coordinación y soporte Equipo de integración y pruebas	Evelyn Obando Pereira Guillermo Hidalgo Blanco. Mauriel Cabalceta Calderón.
Personal no capacitado para sus funciones.	Coordinador de la continuidad del negocio. Equipo de notificación. Equipo de logística y suministro de recursos.	Alonso Salazar Céspedes. Evelyn Obando Pereira. Marco Aurelio Salazar.
Caídas de los equipos informáticos (dispositivos de red, central telefónica, servidores, UPS).	Coordinador de la continuidad el negocio. Equipo de notificación. Equipo de controles de seguridad. Equipo de evaluación y riesgos. Equipo de sistemas de backups. Equipo de integración y pruebas.	Alonso Salazar Céspedes. Evelyn Obando Pereira. Mauriel Cabalceta Calderón. Guillermo Hidalgo Blanco.
No se han definido los servicios críticos de TI.	Coordinador de la continuidad del negocio. Equipo de notificación. Equipo de logística y suministro de recursos.	Rodolfo Navas Alvarado. Alonso Salazar Céspedes. Evelyn Obando Pereira.

No realización de mantenimientos preventivos.	Equipo de coordinación y soporte. Equipo de evaluación y daños.	Mauriel Cabalceta Calderón.

Fuente: elaboración propia.

5.4.3.5 **DS4.8 – Recuperación y Reanudación de los Servicios de TI**

Según la norma COBIT en el apartado DS4.8 se define lo siguiente: "planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio." (p. 114)

Se crea una plantilla donde el coordinador del área de Tecnología de la Información avala el procedimiento.

Tabla 69 – Recuperación y reanudación de los servicios de TI

CENECOOP Crecemos Juntos	**Reanudación de servicio**	
Puesto	Encargado	Sustituto
Revisión de lista (cuando un servicio falla)		
Se activa procedimiento de respaldo		☐ Sí ☐ No
Se comunica a los equipos respectivos de la continuidad		☐ Sí ☐ No
Empleados continúan utilizando el servicio caído		☐ Sí ☐ No
Se reanuda el servicio de manera correcta		☐ Sí ☐ No

Fuente: elaboración propia.

5.4.3.6 **DS4.9 – Almacenamiento de Respaldos**

Según la norma COBIT en el apartado DS4.9 se define lo siguiente: "almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido

de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.” (p. 114)

Se crea una estructura de plantilla para la restauración de respaldos, ya que tanto COBIT como la ISO 22301 mencionan la importancia de este proceso. Se recomienda tomar en cuenta los siguientes aspectos:

- Nombre del encargado del puesto.
- Mencionar el tipo de respaldo, puede ser de configuración de equipos o de base de datos, también es importante tomar en cuenta el ambiente en el cual se aplica el respaldo, ya sea de producción o desarrollo, tiempos calculados para efectuar dicha acción.

Tabla 70 – Restauración de respaldos

CENECOOP Crecemos Juntos	**Restauración de respaldos**	
Puesto	Encargado	Sustituto
Diccionario		
Tipo de respaldo		
Ambiente destino		
Tiempo de restauración		
Descripción		
Observaciones		
Revisión		
	Nombre	Firma
Realizado por:		
Revisado por:		

Autorizado por:		

Fuente: elaboración propia.

5.4.3.7 **DS4.10 – Revisión Post Reanudación**

Según la norma COBIT en el apartado DS4.10 se define lo siguiente: "Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia." (p. 114)

Se crea una plantilla donde el coordinador del área de Tecnología de la Información (Alonso Salazar Céspedes) se encarga de distribuir la información y hacer una revisión de lista donde se colocan los servicios y procesos que brinda CENECOOP R.L, para verificar que la entidad se encuentre en un correcto funcionamiento.

Tabla 71 – Reanudación de servicio

CENECOOP Crecemos Juntos	**Reanudación de servicio**	
Puesto	Encargado	Sustituto
Revisión de lista		
Los servicios que brinda el área de TI están arriba		☐ Sí ☐ No
Los datos que brinda el área de TI están arriba		☐ Sí ☐ No
Validación con los interesados del funcionamiento del equipo		☐ Sí ☐ No

Fuente: elaboración propia.

Tabla 72 – Autorización aplicación y mantenimiento del plan de continuidad del negocio

Revisión		
	Nombre	**Firma**
Realizado por:	Fabián Soto Bogantes	
Revisado por:	Coordinador de TI	
Autorizado por:	Gerente general	

Fuente: elaboración propia.

5.4.4 Fase III – Análisis de resultados

Una vez aplicado el plan de continuidad del negocio se procede a aplicar las respectivas pruebas, ejercicios y ensayos, para analizar los resultados de acuerdo con el factor tiempo, financiero y factor organizacional.

5.4.4.1 Factor tiempo

Tabla 73 – Factor tiempo

Parámetro	Valor
Tiempo promedio que un servicio pasa detenido	120 minutos
Tiempo que toma en reportar un incidente	5 minutos
Tiempo de revisión de los equipos para determinar el problema	30 minutos
Tiempo que tarde el proveedor de los equipos para dar una solución (solo en caso de que aplique)	180 minutos
Tiempo que tarda el técnico del departamento de TI en dar una solución	120 minutos
Tiempo necesario para conseguir un servidor de características similares al equipo que presenta problemas	20 minutos
Tiempo necesario para instalar y configurar las aplicaciones del servidor	210 minutos
Tiempo necesario de instalación y configuración de servicios y aplicaciones críticas de TI	240 minutos
Tiempo necesario para reiniciar un servidor e iniciar la aplicación	10 minutos
Tiempo necesario para verificar que el estado de los servicios sean óptimos para los usuarios	10 minutos
Tiempo necesario para levantar el internet en caso de fallo interno	60 minutos
Tiempo aproximado de imprevistos	30 minutos
Tiempo promedio de fallas	**86.25 minutos**

Fuente: elaboración propia.

En base con el factor tiempo el parámetro que representa un mayor problema es el tiempo que se necesita para instalar y configurar las aplicaciones en el servidor lo que implica restaurar las

aplicaciones tomaría mínimo 4 horas. Los demás parámetros son tiempos asequibles para el Centro de Estudios y Capacitación Cooperativa R.L, el tiempo promedio de una falla es de 86.25 minutos.

5.4.4.2 **Factor financiero**

Tabla 74 – Factor financiero

Parámetro	Valor
Costo de almacenamiento en la nube	₡80.000 mensuales
Costo adquisición de un servidor con características similares al servidor dañado.	₡550.000 mensuales
Costo promedio por servicio crítico detenido	₡130.583 por detención
Costo asesoría de un proveedor	₡300.000 mensuales
Costo de capacitación al personal	₡800.000 mensuales
Costo promedio de fallas	**₡372.116 mensuales**

Fuente: elaboración propia.

El análisis de costos se detallan los valores de forma mensual, tomando en cuenta el tiempo de uso de los equipos. El costo promedio de las fallas es de ₡372.116 colones mensuales.

5.4.4.3 **Factor organizacional**

En el factor organizacional se define el recurso humano que es necesario para la implementación del plan de continuidad del negocio. El equipo de gestión de riesgos está conformado por un miembro del departamento de TI.

Es importante aclarar que la implementación de un sistema de salud y seguridad ocupacional es importante en el Edificio Cooperativo, ya que en CENECOOP R.L no poseen nada al respecto, con el fin de tener un nivel de operación aceptable y seguro de las actividades dentro de la organización y de esta manera prevenir los riesgos para garantizar la integridad de los empleados de la cooperativa; se debe involucrar a todo el personal para la capacitación constante.

Para la implementación del sistema de salud y seguridad ocupacional se puede utilizar la Norma OHSAS 18001 que puede ser aplicada a cualquier tipo de empresa, porque ayuda a fomentar ambiente laborales seguros, estables y confortables. Con dicha norma, se garantiza una respuesta ante situaciones de emergencia como:

- ✓ Creación de una política de salud ocupacional.
- ✓ Identificar riesgos de salud.
- ✓ Análisis, evaluación y mejora del sistema de salud y seguridad ocupacional.

Tabla 75 – Autorización análisis de resultados

Revisión		
	Nombre	**Firma**
Realizado por:	Fabián Soto Bogantes	
Revisado por:	Coordinador de TI	
Autorizado por:	Gerente general	RODOLFO ARTURO NAVAS ALVARADO (FIRMA) Firmado digitalmente por RODOLFO ARTURO NAVAS ALVARADO (FIRMA) Fecha: 2020.10.07 12:36:04 -06'00'

Fuente: elaboración propia.

Al identificar los procesos críticos que contribuyen más a la misión de CENECOOP R.L, se analiza el impacto que podría tener cualquiera de estos eventos que impida el correcto funcionamiento y pérdidas potenciales que podría acarrear esa interrupción. Como resultado, se desarrolla las tres fases: análisis de servicios críticos, aplicación del plan y análisis de resultados. Se identifican los servicios y se establece la magnitud de los impactos potenciales tanto operativos como financieros.

El BCP involucra acciones complejas ante los servicios críticos mencionados anteriormente que son salvavidas ante eventualidades en la empresa, es de vital importancia que la empresa conozca su naturaleza de negocio para la recuperación, de esto depende la identificación acertada de los riesgos para establecer las estrategias más eficientes para su implementación, permitiendo de está manera la correcta estimación de recursos. Además de esto los altos mandos deben demostrar su compromiso con el proceso, pues la implementación de la administración de la continuidad de servicios de TI es compleja y costosa sin un retorno de inversión.

CAPITULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1 **Conclusiones**

Con los análisis FODA, PESTEL y CAME se identificaron las debilidades y fortalezas, tanto de la organización como del departamento de Tecnologías de la Información; adicionalmente, se concluyó que la empresa no contaba con ningún tipo de plan de continuidad de negocio, siendo necesario su desarrollo para garantizar su permanencia. La metodología propuesta consideró estándares y normas internacionales, para la mitigación de vulnerabilidades y riesgos, entre ellos la norma ISO y el COBIT.

Se identificaron satisfactoriamente los servicios críticos que pueden materializarse, tanto a nivel general (todos sus departamentos en forma general) como los enfocados en el tipo tecnológico, a los que está expuesto el Centro de Estudios y Capacitación Cooperativa R.L., además se identificaron los riesgos altamente potenciales (R1 a R13), mediante matrices para la determinación de riesgos (análisis de riesgos cualitativo, escala de probabilidad, escala de impacto, nivel de riesgo inherente, valoración de riesgos y semáforo de riesgos), lo cual asegura la prevención de daños, así como las posibles pérdidas que pueden traer consigo la ocurrencia de desastres en la empresa, tanto materiales, como humanos, generando una ventaja sobre los competidores.

Se desarrolló el plan de continuidad aplicando los procedimientos necesarios para dar una solución breve, ante cualquier tipo de incidente, reduciendo el impacto sobre la organización, lo que implicaría una inversión por parte de CENECOOP R.L. Se definió una guía que permite aplicar diferentes pasos o procedimientos, en caso de ser requeridos ante cualquier contingencia; esta guía permite identificar cada uno de los riesgos a los que se enfrenta la entidad cooperativa y con base en ellos se elaboró un plan de acción para mitigar dichos riesgos. Además, a través del marco de trabajo, específicamente en el apartado DS4 de objetivos de control, se confeccionaron plantillas para atacar vulnerabilidades específicas, tales como: respaldos, mantenimiento del plan, roles y responsables, capacitaciones y post reanudación de servicios críticos.

Se concluye que la organización no está exenta a sufrir incidentes que afecten el funcionamiento de sus servicios más críticos, como ya ha ocurrido en ocasiones, generando pérdidas económicas y dañando levente la imagen del Centro de Estudios y Capacitación Cooperativa R.L. Finalmente la empresa está anuente a mejorar y ofrecer a su cartera de clientes la continuidad en sus servicios, sin embargo, hasta el momento no contaba con un plan de continuidad, por lo que al ocurrir un

acontecimiento grave no se podrían levantar los servicios en un tiempo óptimo, lo que repercute en clientes insatisfechos con respecto a los servicios brindados por la organización.

6.2 Recomendaciones

1) Se recomienda llevar a cabo la implementación del plan de continuidad de negocio, tomando como referencia la propuesta elaborada y utilizando como base las plantillas entregadas, ya que se encuentran enfocadas en la organización y alineada a los estándares ISO 22301 y COBIT en su apartado DS4.

2) Invertir en respaldo de servidor web, base de datos, proveedor de internet y planta para suministro de fluido eléctrico, con esto se favorece enormemente la cooperativa, pues si en algún momento se presenta un incidente relacionado a estos aspectos, se puede mantener la continuidad del servicio e incluso para el cliente no es perceptible el acontecimiento.

3) Se aconseja a la empresa CENECOOP R.L. contratar los servicios de un técnico o empresa certificada en telecomunicaciones, para que realice una reestructuración de redes y cableado estructurado, además que verifique la topología actual, para garantizar el buen funcionamiento de la red y que la seguridad de la información sea integra, esté disponible y sea confidencial.

4) Mantener el plan de continuidad de negocio en constante actualización, para esto será necesario actualizar la valoración de riesgos al menos una vez al año, con el fin de determinar que los cambios ocurridos no afecten el proceso.

5) El coordinador de TI debe velar porque la Gerencia esté comprometida con el plan, buscando la asignación de responsables ante nuevos riesgos de la compañía, además, se aconseja implementar políticas de control asociadas al plan, siendo el auditor interno de CENECOOP R.L quien debe dar el seguimiento oportuno.

6) Se requiere la capacitación del personal involucrado en el modelo del plan de continuidad, para fortalecer los resultados obtenidos e instruir adecuadamente a los empleados.

7) Una vez que el plan sea implementado, será necesario evaluar el desempeño, eficiencia y funcionalidad de éste, para revisar su operación y hacer los ajustes necesarios.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Álvarez, L. F. V., Rodas, R. M., Trujillo, M. E., & Farmacéuticos, Q. PLAN DE CONTINGENCIA Y PLAN DE RESPUESTA DE LA FACULTAD DE CIENCIAS QUÍMICAS Y FARMACIA, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, ANTE LA OCURRENCIA DE DESASTRES NATURALES Y/O PROVOCADOS POR EL HOMBRE.

Arbós, L. C., & Babón, J. G. (2017). Gestión integral de la calidad: implantación, control y certificación. Profit editorial.

Arias Galicia, L. F. (2007). Metodología de la investigación. Editorial Trillas.

Balmaceda Torres, G. A. (2020). Marco para la Gestión de Riesgos TI en el Entorno Bancario.

Bautista, M. (2014). Marco de Referencia para la Formulación de un Plan de Continuidad de Negocio para TI, un caso de estudio. Revista Técnica" energía", 10(1), 200-207.

Brand, K., & Boonen, H. (2007). IT governance based on CobiT® 4.1-A management guide. Van Haren.

Business Continuity Institute. (2013). ISO 22301: Guía de buenas prácticas 2013. Recuperado de: http://normaiso22301.com/bci-business-continuity-institute-ha-publicado-la-ultima-edicion-de-la-guia-de-buenas-practicas-gpg/

Casares, I. S. A. B. E. L. (2013). Proceso de Gestión de Riesgos y Seguros en las empresas. España: Molinuevo, Gráficos, SL.

Centro de Estudios y Capacitación Cooperativa R.L. (2015). Organigrama. Recuperado de: https://www.cene.coop/organigrama/

Chapman, A. (2004). Análisis DOFA y análisis PEST. Accesible en: http://www.degerencia.com/articulos.php.

Díaz Montaña, P. A., Mariño Martínez, O. L., & Sierra Sánchez, F. V. (2016). Elaboración del análisis de impacto al negocio (BIA) como parte fundamental del plan de continuidad de negocio de la cadena radial (Bachelor's thesis, Universidad Piloto de Colombia).

HERNÁNDEZ SAMPIERI, R. O. B. E. R. T. O. (2006). Fundamentos de Metodología de la Investigación. Tercera Edición McGraw-Hill.

Huerta, A. V. Códigos de buenas prácticas de seguridad. UNE-ISO/IEC.

ISACA. (2012). COBIT 5: A business framework for the governance and management of enterprise IT. ISACA.

ISO, B. (2012). 22301: 2012. Societal security. Business continuity management systems. Requirements. British Standards Institute, London, 15-19.

López Ortiz, J. E., & Mayorga Cáceres, E. J. (2017). Diseño, documentación e implementación del sistema de gestión para la continuidad de negocio en Cotrascal SAS con base en la Ntc ISO 22301: 2012 (Doctoral dissertation, Universidad Industrial de Santander, Escuela De Estudios Industriales Y Empresariales).

López-Roldán, P., & Fachelli, S. (2015). Metodología de la investigación social cuantitativa.

Martínez, J. G. (2010). El plan de continuidad de negocio: Una guía práctica para su elaboración. Ediciones Díaz de Santos.

Martínez Ortiz, Á. C., Soler Moreno, S. P., & Carreño Lizarazo, F. (2018). Propuesta de un modelo de plan de continuidad de negocio para la empresa Roldan y Cía.

Melo, V., & Hernando, A. (2008). El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. Revista de derecho, (29), 333-366.

Mendoza, M. Á. (2014). Business Impact Analysis (BIA) y la importancia de priorizar procesos. Recuperado de https://www. welivesecurity. com/laes/2014/11/06/business-impact-analysis-bia.

National Fire Protection Association. (2007). NFPA 1600 Norma sobre el Manejo de Desastres, Emergencias y Programas para la Continuidad de los Negocios, Edición 2007.

Susanto12, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECSIJENS, 11(5), 23-29.

Obando E. (2015). ¿Quiénes somos? Centro de Estudios y Capacitación Cooperativa R.L. Recuperado de: https://www.cene.coop/quienes-somos/

Posada Escobar, J. C. (2013). Modelo de negocio prototipo para una empresa especializadas en BCM y mitigación de riesgo en la división midstream del sector oil & gas (Master's thesis, Bogotá-Uniandes).

Puerto Jiménez, D. N. (2011). La gestión del riesgo en salud en Colombia (Doctoral dissertation, Universidad Nacional de Colombia).

Rodríguez Valencia, J. (2001). Cómo aplicar la planeación estratégica a la pequeña y mediana empresa. México: Thomson learning.

Sáez, V. (2013). Modelo Integral para la implementación de un Plan de Continuidad de Negocio en Chile.

Sampieri, H., Fernández, C., & Baptista, L. (2014). Metodología de la Investigación. Sexta edición. Editorial McGRAW-HILL.

Scherkenbach, W. W. (1994). La ruta Deming hacia la mejora continua (No. D10 200).

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica-ESPOL, 28(5).

Vallejo Peralta, C. B. (2017). Desarrollo e implementación de un plan de continuidad de negocio y de recuperación de desastre en la empresa Agripac SA (Master's thesis, Espol).

Vieites, Á. G. (2011). Enciclopedia de la seguridad informática (Vol. 6). Grupo Editorial RA-MA.

APÉNDICES

1.1 **Entrevista a jefaturas de CENECOOP R.L.**

1. ¿Cuántas sucursales tiene el Centro de Estudios y Capacitación Cooperativa?

   ◯ Solo una.

   ◯ Dos sucursales.

   ◯ Más de dos.

2. ¿Considera que es el plan de continuidad del negocio para TI es la mejor opción para la productividad en caso de una interrupción en la organización?

   ◯ Sí.

   ◯ No.

3. ¿Tiene la empresa (sucursales) un plan de continuidad del negocio?

   ◯ Sí.

   ◯ No.

4. ¿Qué tan probable un servicio falla a la semana en la empresa CENECOOP R.L.?

   ◯ Muy probable.

   ◯ Probable.

   ◯ Poco probable.

   ◯ Nunca.

5. ¿Cuánto tiempo espera generalmente al momento de interrupción en algún servicio crítico de la organización?

   ◯ De 10 a 30 minutos.

◯ De 31 a 59 minutos.

◯ De 1 a 3 horas.

◯ Más de 3 horas.

6. ¿Marque con una “X” de acuerdo con la escala que se brinda más adelante la disponibilidad de los servicios del Centro de Estudios según considere? (siendo 1 la más baja y 10 la más alta)

1	2	3	4	5	6	7	8	9	10

1.2 **Encuesta efectuada a colaboradores de la empresa.**

CENECOOP R.L. Crecemos juntos	**Encuesta "Plan de Continuidad del Negocio"**

Buenos días (tardes):

El objetivo de este formulario es recopilar las opiniones de los trabajadores acerca del plan de continuidad del negocio.

Conteste este cuestionario con la mayor sinceridad posible. Las respuestas serán confidenciales.

Marque con X el espacio en blanco según la pregunta o conteste de manera amplia lo que se le pregunta.

Fecha: _____

Puesto: _____

1) ¿Ha escuchado hablar sobre un plan de continuidad del negocio?

◯ Sí.

◯ No, pase a la pregunta 3.

2) ¿Qué significa para usted un plan de continuidad del negocio?

_____

_____

_____

3) ¿En su empresa o departamento hay implementado un plan de continuidad del negocio?

◯ Sí.

◯ No.

4) ¿Existen procedimientos o actividades de respaldo que realicen en caso de que sus procedimientos normales fallen, son procedimientos establecidos por la empresa?

◯ Sí.

◯ No.

Justifique su respuesta:

_____

_____

_____

5) ¿Cuáles de sus funciones considera usted críticas, que en caso de no realizarse los demás procesos de la organización se pueden ver afectados, de ser este el caso que departamentos podrían ser afectados?

_____

_____

_____

6) ¿La interrupción en el funcionamiento normal de su departamento generaría alguna implicación legal en caso de que se interrumpa dicha actividad?

_____

_____

_____

7) ¿Con cuáles herramientas (software) necesita para desarrollar sus funciones? ¿En caso de que éstos fallen, se tiene un plan B para solucionarlo? ¿Cuáles son los servicios que brinda su departamento?

_____

_____

_____

8) ¿Hace cuántos años tiene su equipo de cómputo?

◯ De 1 a 3 años.

◯ De 4 a 6 años.

◯ De 6 o más años.

1.3 **Índice de Gestión Institucional (IGI) del área tecnológica**

Las preguntas que se anotan a continuación consisten en una medición efectuada por la Contraloría General de la República con el fin de valorar el establecimiento de factores formales tendentes a potenciar la gestión en la organización, en este caso, para efectos de la investigación se toma en cuenta solamente el área de tecnologías de información.

1. ¿La institución ha establecido una estructura formal del departamento de TI, que contemple el establecimiento de los roles y las responsabilidades de sus funcionarios?
2. ¿Existen en la institución funcionarios formalmente designados para que conformen una representación razonable que como parte de sus labores, asesoren y apoyen al jerarca en la toma de decisiones estratégicas en relación con el uso y el mantenimiento de tecnologías de información?
3. ¿La institución cuenta con un plan estratégico de tecnologías de información vigente que al menos cumpla los siguientes requisitos?:
    a. Describir la forma en que los objetivos estratégicos de TI están alineados con los objetivos estratégicos de la institución.
    b. Disponer de un mecanismo para evaluar el impacto de TI en los objetivos estratégicos de la institución.
    c. Incluir fuentes de financiamiento, estrategias de adquisiciones y un presupuesto que esté vinculado con el presupuesto institucional que se presenta ante la CGR.

    (LA RESPUESTA AFIRMATIVA REQUIERE QUE EL PLAN CONTEMPLE LOS TRES PUNTOS, COMO MÍNIMO.)

4. ¿La institución cuenta con un modelo de arquitectura de la información que:
    a. ¿Sea conocido y utilizado por el nivel gerencial de la institución?
    b. ¿Caracterice los datos de la institución, aunque sea a nivel general?

    (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE CUMPLAN AMBOS PUNTOS.)
5. ¿La institución cuenta con un modelo de plataforma tecnológica que defina los estándares, las regulaciones y las políticas para la adquisición, operación y la administración de la capacidad tanto de hardware como de software de plataforma?
6. ¿La institución cuenta con un modelo de aplicaciones (software) que defina los estándares para su desarrollo y/o adquisición?
7. ¿La institución cuenta con un modelo de entrega de servicio de TI que defina los acuerdos de nivel de servicio con los usuarios?
8. ¿Se ha oficializado en la institución un marco de gestión para la calidad de la información?
9. ¿La institución cuenta con directrices (o políticas) orientadas a lo siguiente?:
    a. La identificación de información en soporte digital, gestionada por la institución, que deba ser compartida con otras instituciones o que deba ser del conocimiento de la ciudadanía en general.
    b. La implementación de mecanismos tecnológicos para comunicar dicha información a sus destinatarios.

    (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE CUMPLAN AMBOS PUNTOS.)
10. ¿La institución ha oficializado lineamientos o políticas para la seguridad (tanto física como electrónica) de la información, así como procesos de administración y operación asociados a ellos, sustentados en un documento vinculado al Plan Estratégico de TI, que identifique al menos de manera general lo siguiente:
    a. Requerimientos de seguridad
    b. Amenazas
    c. Marco legal y regulatorio relacionado con seguridad de la información, que la entidad debe cumplir

    (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE IDENTIFIQUEN LOS TRES ASUNTOS, COMO MÍNIMO.)

11. ¿La institución ha definido, oficializado y comunicado políticas y procedimientos de seguridad lógica?
    (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE CUMPLAN AMBOS TIPOS DE REGULACIÓN HAYAN SIDO DEFINIDOS, OFICIALIZADOS Y COMUNICADOS.)
12. ¿Se han definido e implementado procedimientos para otorgar, limitar y revocar el acceso físico al centro de cómputo y a otras instalaciones que mantienen equipos e información sensibles?
13. ¿Se aplican medidas de prevención, detección y corrección para proteger los sistemas contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento, etc.)?
14. ¿Se aplican políticas oficializadas que garanticen que la solicitud, el establecimiento, la emisión, la suspensión, la modificación y el cierre de cuentas de usuario y de los privilegios relacionados se hagan efectivas por el administrador de cuentas de usuario de manera inmediata?
15. ¿Existe un plan formal que asegure la continuidad de los servicios de tecnologías de información en la organización?
16. ¿Las políticas de TI se comunican a todos los usuarios internos y externos relevantes?
    (LA RESPUESTA AFIRMATIVA REQUIERE QUE SE CONSIDERE A LOS USUARIOS TANTO INTERNOS COMO EXTERNOS, SEGÚN CORRESPONDA.)

ANEXOS

1.1 Cronograma del proyecto

Tabla 76 – Cronograma del Plan de Continuidad del Negocio en CENECOOP R.L.

Etapa 1

Name	Task owner	Status	Task Timeline - Start	Task Timeline - End	Priority
Inicio de propuesta del proyecto	Fabián Soto	Done	2019-10-07	2019-11-30	Medium
Aprobación de propuesta	Fabián Soto	Done	2019-12-20	2019-12-20	High
Charla dirección de carrera	Fabián Soto	Done	2020-02-13	2020-02-13	Medium
Inicio de diagnóstico en CENECOOP R.L.	Fabián Soto	Done	2020-02-14	2020-02-23	High
Inicio del documento	Fabián Soto	Done	2020-02-24	2020-02-24	High
			2019-10-07	**2020-02-24**	

Etapa 2

Name	Task owner	Status	Task Timeline - Start	Task Timeline - End	Priority
Fase I - Análisis de la situación actual	Fabián Soto	Done	2020-02-25	2020-03-29	High
Fase II - Determinación de riesgos	Fabián Soto	Done	2020-03-30	2020-05-16	High
Fase III - Desarrollo del BCP	Fabián Soto	Done	2020-05-17	2020-06-11	High
Fase IV - Verificación y control	Fabián Soto	Done	2020-06-12	2020-06-29	High
Fase V - Mantenimiento del BCP	Fabián Soto	Done	2020-06-30	2020-07-19	High
			2020-02-25	**2020-07-19**	

Cierre

Name	Task owner	Status	Task Timeline - Start	Task Timeline - End	Priority
Fase VI - Cierre de documento	Fabián Soto	Done	2020-07-20	2020-08-12	High
Presentación de documento a CENECOOP	Fabián Soto	Done	2020-08-14	2020-08-23	Medium
Aprobación de la información del proyecto	Fabián Soto	Future steps	2020-08-14	2020-08-27	High
Defensa de tesis	Fabián Soto	Future steps	2020-11-01	2020-11-30	High
			2020-07-20	**2020-11-30**	

Fuente: elaboración propia.

1.2 **Anexo de encuestas realizadas a CENECOOP R.L.**

Figura 17 – Resultados de encuestas a empleados de CENECOOP R.L.

ID	Hora de inicio	Hora de finalización	Nombre	Language	Fecha	¿Ha escuchado hablar sobre un plan de continuidad del negocio?
1	7/1/20 7:56:24	7/1/20 7:58:02	anonymous	English	7/1/2020	Sí
2	7/1/20 7:58:04	7/1/20 7:58:44	anonymous	English	7/1/2020	Sí
3	7/1/20 7:58:45	7/1/20 7:59:51	anonymous	English	7/1/2020	No
4	7/1/20 7:59:53	7/1/20 8:00:55	anonymous	English	7/1/2020	Sí
5	7/1/20 8:01:52	7/1/20 8:03:06	anonymous	English	6/30/2020	Sí
6	7/1/20 8:03:08	7/1/20 8:04:30	anonymous	English	7/1/2020	Sí
7	7/1/20 8:04:32	7/1/20 8:05:45	anonymous	English	7/1/2020	Sí
8	7/1/20 8:06:00	7/1/20 8:08:06	anonymous	English	7/1/2020	Sí
9	7/1/20 8:08:10	7/1/20 8:09:26	anonymous	English	7/1/2020	Sí
10	7/1/20 8:09:28	7/1/20 8:13:29	anonymous	English	7/1/2020	Sí
11	7/1/20 8:13:37	7/1/20 8:15:29	anonymous	English	7/1/2020	No
12	7/1/20 8:15:30	7/1/20 8:17:11	anonymous	English	7/1/2020	No
13	7/1/20 8:17:13	7/1/20 8:19:31	anonymous	English	7/1/2020	No
14	7/1/20 8:19:36	7/1/20 8:20:51	anonymous	English	7/1/2020	No
15	7/1/20 8:21:16	7/1/20 8:23:05	anonymous	English	7/1/2020	Sí
16	7/3/20 9:17:34	7/3/20 9:19:37	anonymous	English	7/3/2020	Sí
17	7/3/20 9:19:48	7/3/20 9:22:29	anonymous	English	7/3/2020	No
18	7/3/20 9:31:16	7/3/20 9:33:40	anonymous	English	7/3/2020	No
19	7/3/20 10:15:32	7/3/20 10:17:35	anonymous	English	7/3/2020	No
20	7/3/20 10:15:31	7/3/20 10:17:40	anonymous	English	7/3/2020	Sí
21	7/3/20 10:18:30	7/3/20 10:30:05	anonymous	English	7/3/2020	No
22	7/3/20 10:47:35	7/3/20 10:48:39	anonymous	English	7/3/2020	No
23	7/3/20 13:53:55	7/3/20 13:55:38	anonymous	English	7/3/2020	Sí
24	7/3/20 13:54:02	7/3/20 13:55:44	anonymous	English	7/3/2020	Sí
25	7/3/20 13:56:18	7/3/20 13:58:31	anonymous	English	7/3/2020	Sí
26	7/3/20 13:56:19	7/3/20 14:00:09	anonymous	English	7/3/2020	No
27	7/3/20 14:30:42	7/3/20 14:33:11	anonymous	English	7/3/2020	Sí

ID	¿En su empresa o departamento hay implementado un plan de continuidad del negocio?	¿Existen procedimientos o actividades de respaldo que realicen en caso de que sus procedimientos normales fallen?	¿Hace cuántos años tiene su equipo de cómputo?	¿Cómo evalua el servicio de internet en su puesto de trabajo?
1	No	No	De 4 a 6 años.	Regular
2	No	No	De 4 a 6 años.	Regular
3	No	No	De 4 a 6 años.	Malo
4	No	No	De 6 o más años.	Malo
5	No	No	De 1 a 3 años.	Bueno
6	No	No	De 1 a 3 años.	Bueno
7	No	Sí	De 1 a 3 años.	Bueno
8	No	No	De 4 a 6 años.	Bueno
9	No	No	De 6 o más años.	Bueno
10	No	Sí	De 6 o más años.	Bueno
11	No	No	De 4 a 6 años.	Regular
12	No	No	De 4 a 6 años.	Bueno
13	No	No	De 4 a 6 años.	Bueno
14	No	No	De 6 o más años.	Bueno
15	No	No	De 1 a 3 años.	Bueno
16	No	No	De 6 o más años.	Regular
17	No	No	De 4 a 6 años.	Malo
18	No	No	De 6 o más años.	Bueno
19	No	Sí	De 4 a 6 años.	Bueno
20	No	Sí	De 4 a 6 años.	Malo
21	No	No	De 1 a 3 años.	Bueno
22	No	No	De 1 a 3 años.	Malo
23	No	Sí	De 4 a 6 años.	Bueno
24	No	No	De 6 o más años.	Bueno
25	No	No	De 4 a 6 años.	Bueno
26	No	No	De 4 a 6 años.	Regular
27	No	No	De 4 a 6 años.	Bueno

ID	¿Cuáles de sus funciones considera usted críticas, que en caso de no realizarse los demás procesos de la organización se pueden ver afectados, de ser este el caso que departamentos podrían ser afe...
1	Analizar la información financiera, brindada por el departamento financiero, afecta a todos los departamentos.
2	La digitalización de los documentos al sistema, por lo que si no se realiza las otras funciones se paralizarán.
3	Confección de certificados.
4	Actualización de información contable (sistemas), declaraciones de impuestos y afectan a todos los empleados del CENECOOP.
5	La relación con nuestros clientes. El servicio al cliente. La imagen de la empresa (Comunicación e imagen).
6	Control y seguimiento a proyectos en marcha. Afecta CyI, Académico, Proyectos y Mercadeo.
7	-Disminución de matrícula.-No vender servicios.-Toda la empresa se ve perjudicada
8	Elaborar y actualizar de documentos administrativos del CENECOOP R.L., para la diligencia de información, políticas y normas que contribuyen al respectivo funcionamiento de la entidad, en caso de no ser así, el departamento Gerencial podría presentar inconvenientes y limitaciones en la coordinación. Afecta a todos.
9	Convocatorias a actividades académicas. Departamentos: Académico, comunicación e imagen.
10	Diseño de procesos educativos. Dep: Academico - Proyectos - IyD - Comunicación
11	Llevar un control del área virtual, por ejemplo, el no abrir cursos para el inicio de los períodos. Áreas: TI, mercadeo, finanzas.
12	Desarrollo y actualización de sistemas y plataformas educativas que afecta a todos los departamentos de la institución.
13	Diseño gráfico (artes, flyers) ediciones de vídeo e imagen y se ven perjudicados: Ti,rpyectos, academico, comunicación y mercadeo.
14	Mis funciones no son críticas en la organización
15	Subir contenido a redes sociales (Facebook, Twitter, Instagram, Youtube) Solo implica en comunicación e imagen.
16	Seguimiento a charlas o actividades académicas.
17	Asesoría legal, afecta a todos los departamentos.
18	Desarrollo de actividades en plataforma educativa para juventud cooperativa. Áreas: Juventud, académico, comunicación.
19	Desarrollo de sistemas de software y afectan a todos los empleados de la institución.
20	Soporte remoto a estudiantes sobre plataforma Moodle. Dep: TI, comunicación, académico.
21	Temas de contratación administrativa.
22	Pagos a proveedores, afecta a todos los departamentos.
23	Todo el tema de mercadeo que afectan todas las actividades de CENECOOP.
24	Distribución de recursos para departamento académico. Afecta solamente al área académica.
25	Diferentes actividades tributarias que afecta a toda la organización.
26	Contestar llamadas (secretariado) afecta la gerencia.
27	Actualización de estatus, coordinación con el consejo de administración que afecta a toda la empresa.

ID	¿Que considera usted que debería mejorar el departamento de TI?
1	Todo.
2	Debe haber una jefatura, con un plan de trabajo al cual se le dé seguimiento y se evalúe cumplimiento y brechas.
3	Más sistemas.
4	Mejoramiento de equipo para empleados.
5	Seguimiento y respaldo de información en las computadoras.
6	Equipo y herramientas tecnológicas
7	Planta Eléctrica
8	Considero que todos los integrantes deben de ser tan comprometidos como otros, esto sin duda alguna generaría mayor porcentaje de eficiencia y con esto se lograría un mayor respuesta y desempeño de la gestión del departamento como tal.
9	Mejorar el control y calidad.
10	Respaldos de equipos y servicio al cliente.
11	No salir a comer todos juntos. Tener mayor control de los recursos.
12	Cumplir con todas las normativas de seguridad para mantener el resguardo y en óptimo estado el centro de datos.
13	Respaldos de las actividades y trazabilidad
14	Las cargas de trabajo entre sus miembros de manera que cada uno cuente con una similitud de estas y no se recargue en una persona el trabajo
15	Tener el software licenciado.
16	Actualización constante por parte del personal de TI.
17	Realizar mantenimiento preventivos.
18	Corregir las fallas más rápido a veces tardan mucho tiempo
19	Dedicación al trabajo por todos los de departamento no solo alguno(s).
20	Conexión a internet inestable.
21	Licenciamiento de software.
22	Mejorar el internet, siempre falla mucho
23	Mejorar el servicio al cliente.
24	Mantenimiento en el software desarrollado por ellos mismos.
25	Una impresora independiente para el departamento académico.
26	Que se puedan hacer respaldos en la nube.
27	Mejoras en equipos, la impresoras están viejas y obsoletas.

Fuente: elaboración propia.

De igual forma, ingresando al siguiente enlace se pueden visualizar los gráficos de los 27 resultados de las encuestas realizadas a todos los empleados de la cooperativa CENECOOP R.L.

Enlace: **clic aquí**

1.3 Anexo de entrevistas realizadas a jefaturas

Tabla 77 – Respuestas de entrevistas a jefaturas

Departamento	Fecha y hora	1- Sucursales de CENECOOP R.L.	2- Mejora la productividad un BCP	3- Tiene BCP en sucursales	4- Probabilidad falla de servicios	5- Tiempo promedio de interrupción	6- Promedio disponibilidad de servicio
Comunicación	23/06/20 09:12 a.m	Solo una	Sí	No	Probable	De 31 a 59 minutos	8
IyD	24/06/20 11:40 a.m	Solo una	Sí	No	Muy probable	De 1 a 3 horas	6
Auditoría	23/06/20 09:24 a.m	Solo una	Sí	No	Muy probable	De 1 a 3 horas	6
Gerencia	23/06/20 09:49 a.m	Solo una	Sí	No	Probable	De 31 a 59 minutos	7
Coord. Virtual	23/06/20 02:00 p.m	Solo una	Sí	No	Poco probable	De 10 a 30 minutos	8
Coord. Juventud	23/06/20 10:16 a.m.	Solo una	Sí	No	Probable	De 1 a 3 horas	7
RH	23/06/20 08:50 a.m	Solo una	Sí	No	Probable	De 31 a 59 minutos	8
TI	22/06/20 08:15 a.m	Solo una	Sí	No	Poco probable	De 10 a 30 minutos	9
Finanzas	23/06/20 03:00 p.m	Solo una	Sí	No	Probable	De 31 a 59 minutos	7
Legal	23/06/20 02:20 p.m	Solo una	Sí	No	Probable	De 10 a 30 minutos	8

Fuente: elaboración propia.