UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERIA DE SISTEMAS

DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIO EN LA EMPRESA CAÑAR NET, CAÑAR – ECUADOR.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA DE SISTEMA

AUTOR: MIRIAM MARIBEL ALLAICO CHIMBORAZO

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES, MGS.

CAÑAR - ECUADOR

2021

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCAG

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERIA DE SISTEMAS

DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIO EN LA EMPRESA CAÑAR NET, CAÑAR - ECUADOR

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA DE SISTEMA

AUTOR: MIRIAM MARIBEL ALLAICO CHIMBORAZO

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES, MGS.

CAÑAR - ECUADOR

2021

DIOS, PATRIA, CULTURA Y DESARROLLO

DEDICATORIA

Primeramente, dedico a Dios que siempre me guía por el mejor camino, a mis padres, Nora Chimborazo y Vicente Allaico, y hermanas que han sido el pilar fundamental para poder cumplir una de las muchas metas en mi vida, y a mi ángel de la eternidad María del Carmen (+) que siempre me apoyaba, me aconsejaba, en donde este sé que estará muy orgullosa de mí.

AGRADECIMIENTO

Quiero agradecer a Dios por darme la capacidad y fortaleza de ir cumpliendo mis sueños, a mis padres, hermanas y sobrinos por el apoyo incondicional.

A esta prestigiosa casa de estudio y a sus catedráticos que día a día nos impartieron con sus sabios conocimientos, además de sus sanos consejos.

Al Ing.Cristhian Flores Urgilés mi tutor que con su apoyo y conocimiento me acompaño incondicionalmente para culminar de mi trabajo de Titulación.

DECLARATORIA DE AUTORIA Y

RESPONSABILIDAD

Yo, Miriam Maribel Allaico Chimborazo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Católica de Cuenca extensión Cañar puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y la Normativa actual de la institución.

_____

Miriam Maribel Allaico Chimborazo

C.I: 0302747886

RESPONSABILIDAD

“La responsabilidad del contenido de esta tesis de grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Universidad Católica de Cuenca extensión Cañar”.

Miriam Maribel Allaico Chimborazo

C.I: 0302747886

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por la Est. Miriam Maribel Allaico Chimborazo, bajo mi supervisión.

_____

Ing. Cristhian Flores Urgilés, Mgs

DIRECTOR DELTRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA

APROBACIÓN DE TRIBUNAL DE GRADO

El tribunal designado por el honorable consejo directivo de la Universidad Católica de Cuenca Extensión Cañar, Facultad de Ingeniería de Sistemas instalado para receptar la sustentación del trabajo final de investigación con el tema: “DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIO EN LA EMPRESA CAÑAR NET.”, transcurrido el tiempo reglamentario procede a consignar la calificación de (_____/100).

Cañar, _____de_____ del 2020

PRESIDENTE	**DIRECTOR**
DELEGAGO	**SECRETARIO**

RESUMEN

Un plan de continuidad de negocio es una estrategia que las empresas adoptan para recuperar y restaurar sus funciones críticas en base a procedimientos que ayuden a determinar una solución alternativa para evitar interrupciones de los servicios o procesos que se ejecutan en la organización. La continuidad de negocio en el área informática es una metodología para la gestión de un buen manejo y administración de las TIC's para tener un buen funcionamiento de la organización. El presente trabajo de investigación, plantea un "Diseño de un plan de continuidad de negocio para la empresa Cañar Net". Iniciando con una revisión bibliográfica de trabajos realizados anteriormente en los distintos ISP en donde aplican metodologías similares y brindan validez a las utilizadas en este proyecto. Posteriormente continuamos con las definiciones más relevantes para el desarrollo de un plan de continuidad. Por otro lado, también se realizó una comparativa de los distintos estándares y normativas para la elaboración de un BCP, de la misma manera una comparativa de las distintas metodologías para el análisis de riesgos. Se realizó el levantamiento de información, se especificó y selecciono la norma ISO 22301 para la elaboración del BCP (Business Continuity Plan) y la metodología Magerit para el análisis y gestión de riesgos. Finalmente se puntualiza el resultado de la aplicación de la metodología Magerit y se desarrolla la propuesta de un plan de continuidad de negocio que servirá como referencia para la empresa.

Palabras claves: plan de continuidad, bcp, isp, tic´s, riesgos.

ABSTRACT

A Business Continuity Plan is a strategy that enterprises take on in order to recover and restore their critical functions based on a process that aids to define an olternative solution to avoid the interruption of the services or processes that are carried out within the Enterprise. The business continuty in the technoligical field is a methodology for the well mansgement of the ICT in order to obtain the well-functioning of the Enterprise. This research proposes a business continuity plan fr the Net Cañar Enterprise. It starts with an analtsis of the studies carried out before in the different ISP where similar methodologies are applied, and they validate the ones used in this Project. Then the most relevant definitions for the development of the business continuity plan are presented. On the other hand, a comparison of the dofferent standards and normative for the elaboration of the BCP was aslo conducted. Similarly, a Comparison beyween the different methodologies for the risk analyses. The gathering of information was done, the norm ISO 22301 is selected and specified for the elaboration of the BCP and the Magerit methdology for the analysis and risk management. Finally, the application outcome ot the magerit methodology is pointed out and the proposal of a business continuity plan that will be the reference for the Enterprise is developed.

Keywords: continuity plan, bcp, isp, ICT, risks

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

Cañar Net es una empresa proveedora de internet dedicada a brindar servicio en los cantones: Cañar, El Tambo, Suscal con sus respetivas parroquias de acuerdo a la disponibilidad de cobertura. Esta empresa ofrece servicio de internet banda ancha ilimitada, para tener acceso a internet no necesita de una línea telefónica, el servicio es ilimitado 24/7, sin restricciones de navegación, descargas ilimitadas, la velocidad y correcto funcionamiento del servicio contratado puede variar de acuerdo a: capacidad y configuración del computador, las características del rendimiento de cada uno de los componentes de la red, y la cantidad de usuarios conectados simultáneamente al internet.

En la actualidad la demanda del servicio de internet cada vez es mayor y es una oportunidad para dar a conocer otro mecanismo que ofrezca este importante y necesario servicio en este mundo globalizado y moderno. Toda empresa proveedora de internet necesita ser eficiente y estar regulado por las mejores prácticas, normas, políticas, procedimientos y metodologías agiles que permitan restaurar el servicio de sus actividades y equipos a la hora de presentar alguna interrupción o falla.

En base a lo antes expuesto el presente trabajo investigativo ha sido fundamentado en la necesidad de la empresa Cañar Net de resguardar la información proveniente de las diferentes aplicaciones informáticas del área de TI considerando a esta información como los activos esenciales de la empresa, por otro lado, se pretende también realizar un BCP que permita mitigar los riesgos de la empresa.

El plan de continuidad facilitara la solución para un problema que afecte a la empresa, mejorando así la eficiencia y desarrollo de la misma. Las empresas experimentan situaciones de emergencia, directa o indirectamente, las cuales necesitan respuestas inmediatas. El Plan de Continuidad del Negocio (BCP) permite establecer los procedimientos para asegurar la

continuidad de una empresa en caso de que esta se viera sometida a una interrupción no deseada de su negocio. El presente trabajo está orientado al desarrollo del Plan de Continuidad del Negocio en la empresa Cañar Net, dentro de una empresa de servicios de Seguros de Vida por la factibilidad de conocer sus procesos y tener la apertura para este plan. El desarrollo está basado en la norma ISO 22301 “Sistema de Gestión de la Continuidad del Negocio”, siguiendo sus fases el trabajo incluye una breve descripción de la empresa Cañar Net, se evalúa los posibles riesgos y amenazas a las que está expuesta, se realiza un Análisis de Impacto del Negocio(BIA) que es el punto de partida para crear las estrategias de continuidad, se define un conjunto de equipos para el restablecimiento de operaciones y los procedimientos a utilizarse, y se definió objetivamente los procesos críticos de la compañía que apoya a la toma de decisiones empresariales

CAPÍTULO I

MARCO REFERENCIAL

1.1 Planteamiento del problema

En la actualidad las organizaciones sufren diferentes cambios en el mercado ya sean estos organizacionales, tecnológicos, competitivos, sociales, y culturales por tal motivo se considera poco pertinente seguir realizando las actividades bajo el mismo rumbo tradicional.

Las organizaciones proveedoras de internet que existen en el cantón Cañar de alguna manera u otra han sufrido algún incidente ya sea esto provocado por el hombre o por la naturaleza teniendo como resultado la perdida de servicio, perdida de equipos informáticos, pérdidas económicas etc., esto debido a que no cuentan con un plan de continuidad de negocios bien estructurado.

El plan de continuidad de negocio es una disciplina que prepara a la organización a mantener la continuidad en sus negocios durante un desastre, a través de la implementación de la misma. Este plan es adaptable en cualquier tipo de organización, es importante debido a la prioridad que proporciona al servicio de los clientes

No importa el tamaño de la empresa o las medidas de seguridad implantadas, toda empresa necesita de un plan de continuidad de servicio, ya que tarde o temprano se encontrará con una incidencia de seguridad que pongan en riesgos a los servidores, o algún evento que detenga totalmente la operación de la empresa.

La empresa Cañar Net, en la actualidad es una importante entidad que proporciona internet a la provincia del Cañar y sus parroquias, y gracias a los beneficios que ofrece, maneja una gran cantidad de clientes. El Problema surge cuando sus redes de distribución y la gran cantidad de información que manejan sus servidores aumenta, ocasionando fallos en su

correcto funcionamiento debido a la sobrecarga de información, evitando así su normal funcionamiento y sostenibilidad de la empresa.

Por este motivo la elaboración de un plan de continuidad, es creado con el objetivo de dar solución a algunos problemas que puedan afectar a la empresa, el cual tiene como finalidad promocionar una guía, para que la empresa pueda superar cierto problema que afecte en su desarrollo.

1.2 Formulación del problema

¿Cuáles son los principales problemas que afectan a la empresa Cañar Net?

¿Sera posible dar una solución aceptable a dichos problemas?

¿Cuál sería el estándar de continuidad de negocio más adecuado para aplicar en la empresa Cañar Net?

¿En qué medida mejorara la recuperación de los procesos de TI al implementar de un plan de continuidad de negocios?

1.3 Antecedentes de la investigación

En la actualidad el avance tecnólogo ha jugado un papel fundamental en el desarrollo de la sociedad, proporcionando una fuente de información, entretenimiento y aprendizaje mediante diferentes medios, entre los cuales tenemos el internet el cual desde sus inicios ha ido evolucionando, volviéndose así parte fundamental del desarrollo social, llegando incluso a considerarse como una herramienta necesaria para poder vivir.

En los tiempos modernos el internet es un medio necesario para todos, jugando un papel importante en la vida cotidiana proporcionando una fuente de información, educación, y entretenimiento para todos quienes tienen acceso a esta herramienta, teniendo esto en cuenta muchas empresas que proveen este medio han surgido y una de estas empresas es Cañar Net.

Esta institución además de tener la mejor tecnología debe garantizar la seguridad y confidencialidad de los datos ante la presencia de incidentes o desastres que pudieran afectar la correcta funcionalidad de las actividades.

Por ello es conveniente tener elaborado una propuesta de Plan de Continuidad de Negocio en donde se incluya las pautas necesarias a seguir ante la pérdida de un servicio que pueda ocasionar la perdida de información.

Con un tema similar se tiene una investigación en la Universidad Autónoma de Occidente, Facultad de ingeniería departamento de Operaciones y Sistemas Programa de Ingeniería Informática Santiago de Cali, realizado por Carlos Andrés Tellez Mondragon el tema: DISEÑAR UN PLAN DE CONTINUIDAD DE NEGOCIOS EN EL PROCESO DE ADMINISTRACIÓN DE RECURSOS DE TI DE LA OFICINA DE INFORMÁTICA Y TELEMÁTICA DE LA ALCALDÍA DE SANTIAGO DE CALI, en el presente trabajo investigativo detalla el procedimiento para la realización de un BCP, partiendo desde la identificación de los procesos críticos posteriormente se realiza el análisis de impacto y tiempos críticos de recuperación, posteriormente se realiza un análisis de riesgos y en base a ello se determina el tratamiento de los riesgos bajo la Norma ISO 22301. (MONDRAGON, 2015)

Por otra parte se tiene se han encontrado estudios similares realizados en la Escuela Politécnica Nacional, Facultad de Ciencias Administrativas, trabajo de titulación previo a la obtención del título de ingeniero en administración de procesos realizado por Boris Alcides Garaicoa Martínez, tema: DIAGNOSTICO DE VULNERABILIDADES DE LAS EMPRESAS PROVEEDORAS DE SERVICIOS PORTADORES DE TELECOMUNICACIONES CON BASE EN QUITO, ANTE EVENTOS NATURALES QUE PROVOQUEN UNA SUSPENSIÓN DE SUS OPERACIONES MEDIANTE UN PLAN DE CONTINUIDAD DE NEGOCIOS, donde propone diseñar y desarrollar un Plan

de continuidad de negocios empezando con el levantamiento de información de la empresa posterior a eso se realiza la evaluación de riesgos finalmente se establece un plan de acciones en donde se determina el equipo de trabajo y sus responsabilidades. (MARTÍNEZ, 2017)

De la misma manera se encontró una investigación realizada en la Escuela Superior Politécnica Del Litoral, Facultad de Ciencias Naturales y Matemáticas, Proyecto Integrador titulado: DISEÑO DE UN MODELO DE GESTIÓN POR PROCESOS APLICADO A UNA EMPRESA PROVEEDORA DE SERVICIOS DE INTERNET, UBICADO EN LA CIUDAD DE BABAHOYO. Realizado por: Cinthia Isabel Piguave Ibarra & Sally Denisse Mera Panta para obtener el título de Ingeniería en auditoria y contabilidad pública autorizada. Este trabajo investigativo servirá como muestra par el diseño de procesos de una empresa proveedora de internet y el plan de direccionamiento estratégico.(IBARRA & MERA, 2017)

1.4 Justificación de la investigación

De acuerdo con las necesidades y posibles problemas que puedan surgir en la empresa, los cuales afecten su funcionamiento, la creación de un plan de continuidad, permitirá que la posible pérdida de información y problemas en la disponibilidad del servicio, tengan una posible solución en caso de que esto ocurra. Además de proporcionar una metodología la cual ayudara a reducir los riesgos enlazados con la integridad, confiabilidad y disponibilidad de los centros de datos.

Obviamente la empresa debe priorizar en mantener la continuidad en la distribución de sus servicios para que esto no afecte a sus clientes, dicha continuidad puede ser por la falta de planificación en caso de que un problema aparezca, por este motivo la creación de un modelo que pueda restablecer o mantener la continuidad de los servicios, es algo que la empresa necesita emplear.

Desde un punto de vista estratégico, un plan de continuidad proporciona un alto apoyo en la elaboración de una solución para un problema que se presente en la empresa.

Con este proyecto, la entidad tendrá resultados favorables y provechosos para su crecimiento ya que podrán ocurrir situaciones inesperables que paralicen los servicios que esta ofrece, que gestionan su activo principal (como por ejemplo que se produzca una falla en un servidos de archivo), pero estará preparada para reaccionar y establecer sus operaciones en tiempos óptimos que no le generen perdida de información y lo más importante de dinero.

1.5 Objetivos

1.5.1 Objetivo general

Diseñar un Plan de Continuidad de negocio en la empresa Cañar Net. Mediante la utilización de estándares reconocidos para garantizar la provisión de los servicios que brinda a sus clientes.

1.5.2 Objetivo específico

- Realizar un estudio teórico de las normativas del plan de continuidad de negocio.
- Identificar los riesgos internos que presenta la empresa Cañar Net. Y que generen interrupciones en el servicio mediante el análisis del entorno.
- Elaborar el plan de continuidad de negocio para la empresa Cañar Net. Como herramienta preventiva que garantice la continuidad del proceso ante un incidente existente.

1.6 Limitaciones

Este estudio no contempla la fase de implementación de la propuesta del plan de continuidad de servicio.

1.7 Delimitaciones

El proyecto se llevará a cabo en el área de TI de la empresa proveedor de servicio de internet Cañar Net.” Ubicada en el Cantón Cañar.

CAPITULO II

MARCO TEORICO

2.1.RIESGOS INFORMÁTICOS

Se entiende por riesgo la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización. El nivel de riesgo dependerá del análisis previo de vulnerabilidad del sistema, de las amenazas y del posible impacto que estas puedan tener en el funcionamiento de la empresa.

Según (Solarte Solarte , Enriquez Rosero, & Benavides Ruano, 2015) dice que los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas informáticos tanto físico como lógico. Si no se tienen las medidas las medidas adecuadas para salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento, por lo tanto, los riesgos se pueden clasificar en: Riesgos de integridad, riesgos de relación, riesgos de acceso, riesgos de utilidad, riesgos de infraestructura.

2.1.1 Identificación de Riesgos

La identificación del riesgo es una de las tareas más importantes a realizar durante la gestión de riesgos dentro de una organización. Consistirá en especificar detalladamente las amenazas reales dentro de un plan de proyecto, las estimaciones, la planificación temporal, los recursos, el presupuesto entre otras. (Garreta, 2003)

Para que el proceso de identificación del riesgo sea más simple es necesario realizar un mapa de riesgos que permita tener identificados los riesgos de mayor importancia, que necesiten ser tratados en el menor tiempo posible, la descripción detallada de la misma y las consecuencias que estas puedan tener.

2.1.2 Evaluación de Riegos

Luego de haber identificado y clasificado los riegos se desarrolla un análisis cualitativo que permita determinar el impacto en base a la probabilidad de ocurrencia que llegará a presentarse en la organización.

Para realizar el análisis cualitativo de riesgo podemos utilizar diferentes herramientas o métodos que ayudaran a evaluar la probabilidad y sus consecuencias, estos podrían ser: entrevistas, FODA[1], o lluvia de ideas, etc. todos estos procesos y métodos ayudan al gerente a tomar buenas decisiones ante la presencia de un riesgo.(Brand et al., 2013)

2.1.3 Matriz de riesgos

Una matriz de riesgo es una herramienta que permite tener un control adecuado para identificar los procesos más importantes en una organización, así como también los tipos y el nivel de riesgo inherentes a estas actividades. (sigweb, s.f)

La matriz de riesgos ayuda a la evaluación de la efectividad de gestión y administración de los riesgos visualizando el impacto que tendría en los resultados y los objetivos que tiene la organización.

Tabla 1: Matriz de Riesgo. Autor: Desarrollador de la tesis. Fuente: (CARAZO, 2016)

CONSECUENCIAS	PROBABILIDAD				
	Raro	Improbable	Posible	Probable	Casi seguro
Insignificante	Bajo	Bajo	Bajo	Medio	Medio
Menor	Bajo	Bajo	Medio	Medio	Medio
Moderado	Medio	Medio	Medio	Alto	Alto
Mayor	Medio	Medio	Alto	Alto	Muy alto
Extremo	Medio	Alto	Alto	Muy alto	Muy alto

[1] Fortalezas, Oportunidades, Debilidades y Amenazas

Tabla 2: Probabilidad. Autor: Desarrollador de la tesis. Fuente: (Nieto Muñoz, 2015)

Raro	Poco probable que ocurra, pero posible
Improbable	Improbable, pero pueda que se produzca
Posible	Ocurra varias veces
Probable	Ocurra con frecuencia
Casi seguro	Continuamente con experiencia

Tabla 3: Impacto. Autor: Desarrollador de la tesis. Fuente: (Nieto Muñoz, 2015)

Insignificante	Las consecuencias se manejan con procedimientos de rutina
Menor	La consecuencia podría amenazar la eficiencia o efectividad de algunos aspectos de la organización, pero estas pueden ser resueltas internamente por el área afectada con esfuerzo adicional.
Moderado	Las consecuencias no amenazan a la organización, pero podrían implicar una revisión o cambio importante en las operaciones de una o varias áreas afectadas, con recursos significativos.
Mayor	Las consecuencias amenazarían la operatividad efectiva de una o varias áreas. Estos daños pueden afectar la imagen, reputación o confianza
Extremo	Las consecuencias amenazan la continuidad de las operaciones de la organización en todos sus procesos.

2.2. ANÁLISIS Y GESTIÓN DE RIESGOS EN UN SISTEMA INFORMÁTICO

El análisis y gestión de riesgos son métodos que permite investigar riesgos de sistemas de información y recomendar medidas adecuadas para controlar estos riesgos en la organización. Utilizar métodos de análisis y gestión de riesgos implica una evaluación del impacto que una violación de seguridad tendría en la empresa señalando de esta manera los riesgos existentes, identificando las amenazas que afecte al SI y la determinación de vulnerabilidad del sistema a dicha amenaza. (Heredero C. , 2006)

A continuación, se presenta los principales conceptos a la hora de estudiar el análisis y gestión de riesgos en una organización según el libro titulado Enciclopedia de la seguridad informática 2º edición (Vieites, 2011).

2.2.1. Amenazas

Es considerado 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. Las amenazas se califican de la siguiente manera:

Amenazas naturales: Hace referencia a los desastres naturales como inundaciones, incendio, tormenta, fallo electrónico, explosión etc.

Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc.

Amenazas de agentes internos: Los empleados descuidados con una formación inadecuado o descontento, errores en la utilización de las herramientas del sistema.

2.2.2. Vulnerabilidades

Según Álvaro Vieites, (2011) “Se considera vulnerabilidad a cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir perdidas en la empresa”.

Estas vulnerabilidades pueden originarse por fallos en los sistemas físicos o lógicos, también estos defectos pueden darse por ubicación, instalaciones, configuraciones y mantenimiento de los equipos, procedimientos mal definidos o sin actualizar, ausencia de políticas de seguridad, etc.

El objetivo de un análisis y gestión de riesgos informáticos es facilitar los componentes de un sistema que requiere protección, sus vulnerabilidades que debilitan el sistema y las amenazas que ponen en peligro ayudando de esta manera a minimizar perdidas en la organización.

2.2.3. Incidentes de seguridad

Según Vieites, 2011 un incidente de seguridad es cualquier evento que tenga o pueda tener como resultado la interrupcion de servicios suministrados por un sistema informatico o

posibles perdidas fisicas, de activos o financieras. En resumen el incidente es la materializacion de una amenaza. (Vieites, 2011)

2.2.4. Impactos

Es la medicion y valoracion del daño que podria producir a la organización un incidente de seguridad. Para valorar el impacto es necesario tener en cuenta tanto los daños tangibles como la estimacion de los daños intangibles en donde se incluye la información. (Vieites, Enciclopedia de la Seguridad Informática. 2ª edición, 2011)

Para calificar el impacto del daño se puede emplear una escala tanto cuantitativa o cualitativa que ha continuacion se detalla:

Tabla 4: Escala propuesta para medir el impacto del daño en la organización. Fuente: (Vieites, 2011)

Alto	• Perdida o inabilitacion de recursos criticos • Interrupcion de los procesos de negocios daño en la imagen y reputacion de la organización. • Robo o revelacion de información estratégica o especialmente protegida.
Medio	• Perdida o inabilitacion de recursos críticas pero que cuenta con elementos de respaldo. • Caída notable en el rendimiento de los procesos de negocio o en la actividad normal de la organización. • Robo o revelacion de información Confidencial, pero no considerada estratégica.
Bajo	• Pérdida o inhabilitacíon de recursos secundarios. • Disminución del rendimientode los procesos de negocio. • Robo o revelacion de información interna no publicada.

2.3.GESTIÓN DE RIESGOS INFORMÁTICOS

La gestión de riesgo es un proceso separado que utiliza los resultados del análisis de riesgos para seleccionar e implementar las medidas de seguridad (salvaguarda) adecuadas para controlar los riesgos identificados. (Maldonado Mariño, 2013)

La administración de riesgo es un proceso continuo, dado que es necesario evaluar periódicamente si los riesgos identificados fueron correctamente reducidos por medio de políticas, reglas y procedimiento implementados.

2.3.1. Proceso de gestión de riesgo

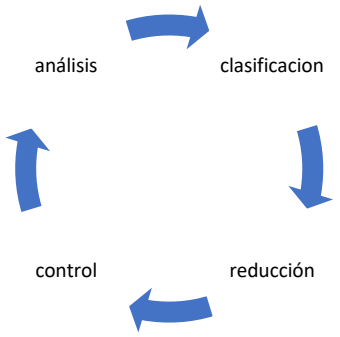


Ilustración 1: proceso de gestión del riesgo. Fuente: (Maldonado Mariño, 2013)

Análisis: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.

Clasificación: Determina si los riesgos encontrados y los riesgos restantes son aceptables.

Reducción: Define e implementa las medidas de protección. Además, sensibiliza y capacita los usuarios conforme a las medidas.

Control: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento. (Maldonado Mariño, 2013)

2.4.METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS

Para la elaboración del análisis y gestión de riesgos existen diferentes metodologías que se puede utilizar, cada una de ellas detallan de manera sistemática las etapas a seguir. (Maldonado Mariño, 2013). Estas metodologías se definen a continuación:

2.4.1 Metodología MAGERIT

Magerit es una metodología ha sido elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del consejo Superior de Informático. Magerit toma como referencia:

Los criterios ITSEC (Information Technologies Security Evaluation Criteria), objeto de una recomendación del Consejo de la Unión Europea de 7/4/1995.

"Los criterios comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información, criterios elaborados por la Unión Europea, EE. UU Y Canadá". (Corrales, 2005)

Magerit estudia a los riesgos que soportan un sistema de información y el entorno asociable con él, entendiéndose por riesgos la posibilidad de que suceda un daño o perjuicio. Esta metodología recomienda algunas medidas que son apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos. (Bances & Vasquez, 2018)

Ilustración 2: Proceso de la Metodología Magerit Fuente: (Ferruzola Gómez et al., 2019)

Objetivos de Magerit

Esta metodología propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes identificando las amenazas que acechan al sistema de información y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.

Estos resultados permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlare los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. Esta metodología permite:

- Aporta racionalidad en el conocimiento del estado de seguridad de los sistemas de Información y en la introducción de las medidas de seguridad.
- Ayuda a garantizar una adecuada cobertura en extensión, de forma que no hay elementos del sistema de información.
- Asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos.

Estructura de Magerit

Según el Libro de Ayudantes técnicos Opción informática. (Corrales, 2005) dice que la metodología Magerit se apoya tres submodelos: El Submodelo de Elementos proporciona los componentes que el Submodelo de Eventos va a relacionar entre sí, mientras que el Submodelo de Procesos será la descripción funcional (el esquema explicativo) del proyecto de seguridad a construir.

Submodelo de Elementos

Este submodelo de elementos de Magerit comprende seis entidades básicas caracterizada por ciertos atributos y relacionadas entre sí:

- Activos
- Amenazas
- Vulnerabilidades
- Impactos
- Riesgos
- Salvaguardas (Funciones, Servicios y mecanismos)

Submodelo de Eventos

Una vez que el submodelo de elementos ha proporcionado los componentes para el análisis y gestión de riesgos, el submodelo de eventos será el encargado de reaccionarlos entre sí. Magerit ofrece tres vistas de este último submodelo para ayudar a automatizar la metodología.

- Vista estática relacional
- Vista dinámica de tipo organizativo
- Vista dinámica de tipo físico.

Submodelos de Procesos

En este submodelo de procesos comprende 4 etapas las cuales son:

- Planificación del Proyecto de Riesgos
- Análisis de riesgos
- Gestión de riesgos
- Selección de salvaguardas

La metodología Magerit fue diseñada para que las organizaciones sean capaces de adoptar sus tareas a los procesos de evaluación, certificación, auditoria o acreditación necesarias, según el caso, para conseguir mantener unos estándares de calidad de sus actividades.

Estructura de las guías Magerit

Las guías Magerit ofrecen un marco de trabajo para que las diferentes empresas sean capaces de gestionar sus riesgos eficientemente. La Metodología Magerit está formada por tres guías las cuales se detalle a continuación:

Libro 1 Método: Este libro se considera el volumen principal de la metodología Magerit, ya que se explica con detalle cómo desarrollarla.

Libro 2 Catalogo de elementos: Es un complemento del libro 1 y en este se incluyen ejemplos y tipos de elementos que pueden ser activos, salvaguardas, amenazas y vulnerabilidades. También se incluyen dimensiones de valoración y criterios de valoración.

Libro 3 Guía de técnicas: De la misma manera es un complemento del libro 1 y en él se describe algunas técnicas que pueden utilizarse en cada fase del proceso de análisis y gestión de riesgo. (Tejada, 2015).

Ilustración 3: Catálogos de Magerit: Autor: Propio.

2.4.2 Metodología OCTAVE

OCTAVE, metodología del SEI (Software Engineering Institute) que desde un punto de vista organizativo y técnico analizo los riesgos y propone un plan de mitigación. (Heredero, Dirección y gestión de los sistemas de información en la empresa, 2006).

La metodología Octave es una evaluación que se basa en riesgos y planeación técnica de seguridad computacional. Es un proceso interno de la organización, significa que las personas de la empresa tienen la responsabilidad de establecer la estrategia de seguridad una vez que se realice dicha evaluación, esta metodología se basa en el conocimiento del personal de la empresa para capturar el estado actual de la seguridad de esta manera es más fácil determinar los riesgos críticos. (Veiga, 2020).

Esta metodología está enfocada a los riesgos organizacionales, temas estratégicos relacionados con la práctica, es flexible y puede aplicarse a la medida para la mayoría de las organizaciones. Es necesario que la organización maneje el proceso de la evaluación y tomen las decisiones para proteger la información. El equipo de análisis, integrado por personas de

los departamentos de TI, de negocios lleva acabo la evaluación, debido a que todas las perspectivas son cruciales para controlar los riesgos de seguridad computacional. (Veiga, 2020)

La metodología OCTAVE cuenta con tres fases las cuales son:

Fase 1 Build asset-based threat profiles: En esta etapa se desarrolla perfiles de amenazas basados en los activos, en el cual se identifica los bienes, las amenazas, practicas actuales, vulnerabilidades y los recursos de seguridad de la organización.

Fase 2 Identify infrastructure vulnerabilities: Por otra parte, en esta fase se identifica las vulnerabilidades de la infraestructura, se basa en los componentes clave y sus correspondientes vulnerabilidades técnicas.

Fase 3 Develop security strategy and plans: Finalmente en esta fase se desarrolla las estrategias y planes de seguridad, con base a los riesgos, la estrategia de protección y los planes de mitigación. (Hurtado, 2018).

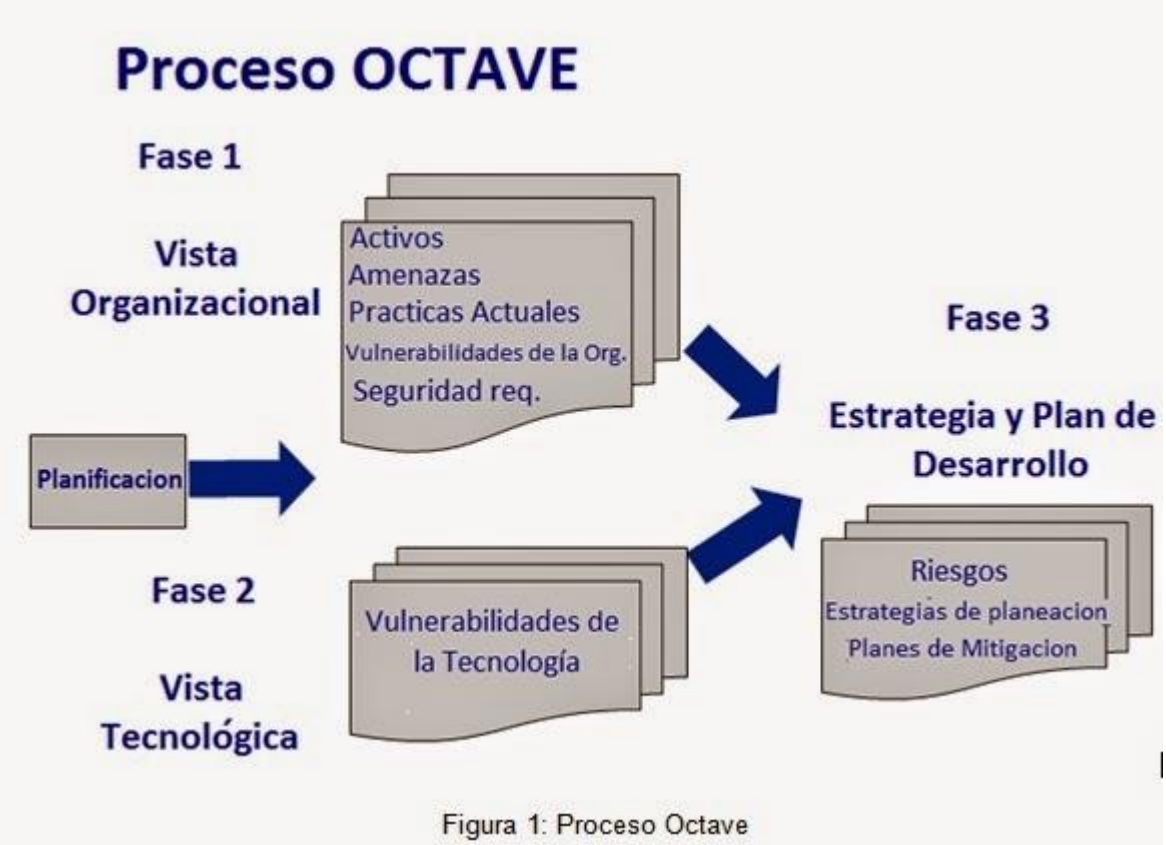


Ilustración 4: Metodología OCTAVE. Fuente: (Hurtado, 2018)

Proceso de la metodología OCTAVE visión de la organización

1. **Identificar el conocimiento de la empresa.** Se identifica la perspectiva que tienen los directivos, en esta fase del proceso se identifica el conocimiento de la empresa ilustra las entradas que necesitan para obtener las salidas. Se pueden definir como entradas a los cuestionarios de activos, perfiles genéricos de las amenazas, catálogo de amenazas, catálogos de prácticas de la organización, técnicas y entrenamiento, datos organizacionales y finalmente leyes y regulaciones que la compañía se encuentre obligada a cumplir.

2. **Identificar el conocimiento del área operativa.** De acuerdo al conocimiento actual de los gerentes del área operacional, un cuestionario de activos, perfil genérico de amenazas, cuestionario de la estrategia de protección datos organizacionales, leyes y regulaciones que se deban cumplir y la lista despreciando las prioridades de los

activos de la empresa con sus respectivos valores relativos, que los jefes de área operativa proporcionen, corresponden a las entradas de esta parte de la metodología.

3. **Identificar el conocimiento del personal.** Detalla las entradas y las salidas que pertenecen a esta parte. En las entradas se tiene el conocimiento actual del personal, cuestionario de activos, perfil genérico de amenazas, cuestionario de la estrategia de protección actual, catálogo de las prácticas de la organización, técnicas y de capacitación, datos organizacionales, leyes y regulaciones que la compañía está obligada a cumplir, lista priorizada de activos, lista de activos del área operacional y el mapa de cruce de activos. Posteriormente se obtiene la lista de activos que el personal identifica, mapa de los activos del área de la empresa comparado con los activos del área operacional y los del personal. (Hurtado, 2018)

4. **Creación de perfiles de amenaza.** En este proceso integra toda la información contenida en los procesos anteriores y procede a crear un conjunto de perfiles de amenaza para los activos en estado crítico, por lo general este tipo de procedimientos suele gestionar por el equipo de análisis. (Hurtado, 2018)

Metodología OCTAVE visión tecnológica

1. **Identificar componentes claves.** En este proceso para cada activo critico encontrado hay que identificar los componentes claves que se deben evaluar para las vulnerabilidades de la tecnología. El equipo de análisis realiza esta actividad, con ayuda del personal de TI esto dependiendo de la necesidad.

2. **Evaluación de componentes seleccionados.** Se identifica las principales vulnerabilidades de los componentes críticos. El equipo de análisis y los miembros de equipo suplementarios evalúan cada uno de los componentes de la infraestructura de

tecnología, identificando las vulnerabilidades de estos. Para esta parte del procese se necesita utilizar herramientas de evaluación de vulnerabilidades.

Metodología OCTAVE Planificación de las medidas y reducción de riesgos

1. **Realizar un análisis de riesgos.** En esta etapa se identifica los riesgos que se podrían dar sobre los activos críticos de una empresa. Para la realización de este proceso se utiliza la información de los procesos 1 al 6 para crear los perfiles de riesgo para los activos críticos con cada una de las descripciones de los impactos encontrados, se crean criterios de valoración y finalmente se evalúan los resultados. (Hurtado Samaniego Diego Fernando, 2019)

2. **Desarrollo de estrategias de protección.** Finalmente, en este proceso se define una serie de acciones, estrategias y planes para proteger los activos críticos los cuales deberán ser estudiados y aprobados para su ejecución. (Hurtado Samaniego Diego Fernando, 2019)

2.4.3 Metodología CRAMM

CRAMM (CCTA Risk Analysis and Management Method) fue desarrollada por la agencia CCTA (Central Computer and Telecomunications Agency) del gobierno del Reino Unido en 1985.

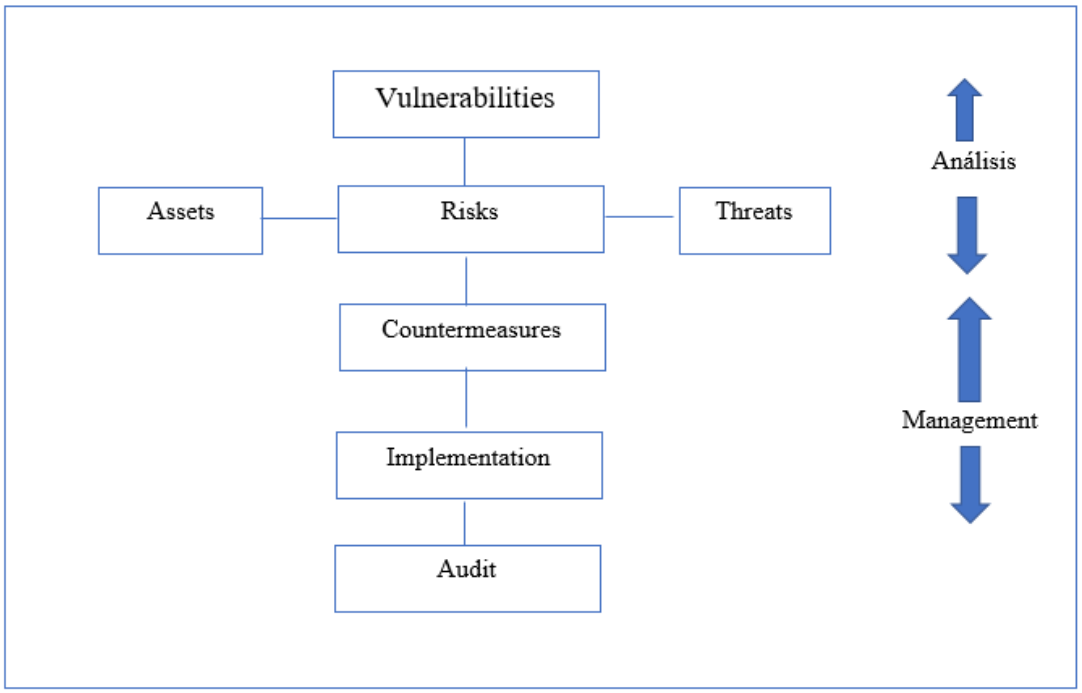


Ilustración 5: Esquema CRAMM. Fuente: (Vieites, 2011)

La metodología CRAMM abarca de forma compleja todas las fases de la gestión de riesgos, desde el análisis real de los riesgos hasta la propuesta de contramedidas, incluida la generación de resultados para la documentación de seguridad (planificación de emergencia y aseguramiento de la continuidad) Cramm es apoyado simultáneamente por la aplicación del mismo nombre que ayuda en la recopilación de datos, así como en el cálculo y procesamiento del informe de gestión de riesgos. (Numpaque Pineda)

Ayuda también a demostrar la eficiencia del costo invertido en la administración de riesgos, la seguridad y la planificación de emergencias. Cuenta con una amplia biblioteca única de contramedidas de seguridad. Esta metodología permite a que la organización se certifique de acuerdo con la ISO 27001. (Numpaque Pineda, pág. 7)

2.4.4 Metodología MEHARI

Esta metodología es también conocido como un método de análisis de riesgo armonizado, es una metodología desarrollada en el año 1995 por CLUSIF(club de la Securite de Information Francais) con la finalidad de que los responsables de la seguridad informática evalúen cuantitativamente los principales factores de riesgos que puede percibir la empresa, para ello se requiere que la entidad establezca previamente una política de seguridad y mantenimiento de riesgos a un nivel convenido esto servirá como referencia para que el acople de los objetivos estratégicos existentes sea de acorde a los nuevos métodos de funcionamiento de la empresa. (GARCÍA., 2018)

Existen dos enfoques para la gestión de riesgos el primer enfoque consiste en identificar todos los tipos de riesgos y analizar cada situación de riesgo identificando y tomando las decisiones específicas para cada uno a continuación se visualiza el proceso que se lleva a cabo para la identificación, análisis y evaluación de riesgos: (GARCÍA., 2018)

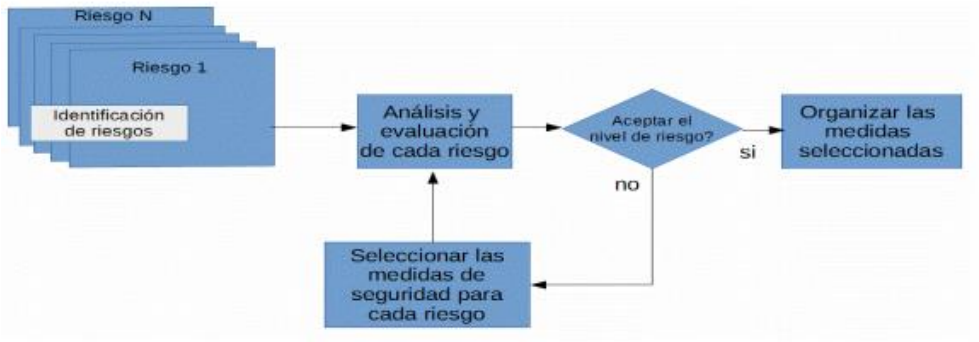


Ilustración 6: Enfoque individual para la gestión del riesgo; Fuente: (GABRIELA, 2017).

Esta metodología adopta un enfoque para un análisis directo e individual de cada una de las situaciones de riesgos, en resumen, esto quiere decir que cada riesgo debe ser identificado y descrito por los escenarios que contienen cierto número de elementos precisos y específicos. Cada escenario de riesgos puede ser evaluado cuantitativamente y esta evaluación considera lo siguiente: (GARCÍA., 2018)

- El impacto específico del escenario de riesgo que refleja el nivel de consecuencia de la ocurrencia en la ausencia de cualquier medida de seguridad.

- La probabilidad específica del escenario que refleja la probabilidad de ocurrencia en ausencia de cualquier tipo de mecanismo de seguridad.

- Los factores de reducción de riesgo basados en las medidas de seguridad, categorizada por el tipo de efecto que ellos tienen sobre el impacto o la probabilidad de las medidas de riesgo y la calidad de esas medidas.

El proceso que se sigue para la evaluación de cada escenario permite seleccionar medidas de seguridad, con objetivos cualitativos por cada medida para que el riesgo pueda ser mantenido por debajo de un nivel aceptable por la empresa.

La metodología MEHARI sostiene una estructura de gestión del riesgo que a continuación se visualiza en la siguiente ilustración 8:

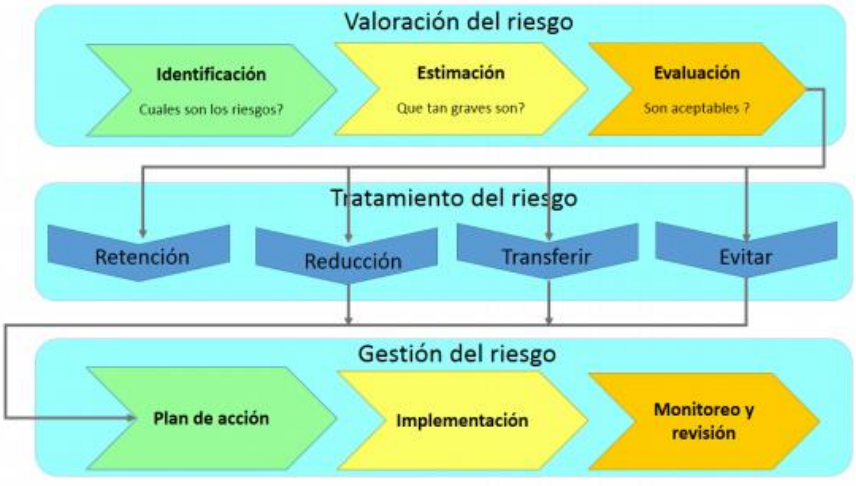


Ilustración 7: Proceso de valoración, tratamiento y gestión del riesgo según MEHARI; Fuente: (GABRIELA, 2017).

2.5. CUADRO COMPARATIVO DE LAS METODOLOGÍAS DE ANÁLISIS DE RIESGO

Luego de haber realizado una investigación sobre las metodologías para la elaboración del análisis y gestión de riesgos se procedió a la elaboración de una tabla comparativa que a continuación de detalla:

Tabla 5: Análisis del ámbito de aplicación y procesos metodológicos. Fuente (VARGAS, s.f.)

Metodología	Ámbito de aplicación	Etapas/ fases que se llevan a cabo
MAGERIT	Uso preferente en la administración pública española, pero puede adaptarse a cualquier tipo de organización. Y está adaptada a los sistemas informáticos.	1. Análisis de riesgos 2. Caracterización de los activos • Caracterización de las amenazas • Caracterización de las salvaguardas • Estimación del estado del riesgo 3. Gestionar los riesgos
OCTAVE	Cualquier organización pública o privada. También está orientada a los sistemas informáticos.	**Fase 1.- Construir perfiles de amenazas basados en los activos** Proceso 1: Identificar el conocimiento de los altos directivos. Proceso 2: Identificar el conocimiento de los directivos de áreas operativas. Proceso 3: Identificar el conocimiento del personal operativo

		Proceso 4: Crear perfiles de amenazas. **Fase 2.- Identificar vulnerabilidades en la infraestructura** Proceso 5: Identificar componentes claves Proceso 6: Evaluación de componentes seleccionados **Fase 3.- Desarrollar estrategias y planes de seguridad** Proceso 7: Realizar un análisis de riesgos Proceso 8: Desarrollar estrategias de protección
CRAMM	Uso preferente en la administración pública británica, pero puede ser adaptada a cualquier entidad pública o privada.	1. Definir marco de gestión de riesgo 2. Identificar riesgos 3. Identificar propietarios de los riesgos 4. Evaluar riesgos 5. Definir niveles aceptables de riegos

		6. Identificar respuestas adecuadas al riesgo 7. Implantar respuestas 8. Obtener garantías de la efectividad 9. Monitorizar y revisar.
	Cualquier organización pública o privada.	1. Establecer el contexto 2. Identificar riesgos 3. Analizar riesgos 4. Evaluar riesgos 5. Tratar riesgos 6. Monitorear y revisar 7. Comunicar y consultar
AS/ NZS ISO 31000	Estándar de carácter genérico orientado a una amplia gama de actividades, operaciones, procesos, funciones, proyectos, productos, servicios, activos.	
MEHARI	Gobiernos, organismos, Empresas medianas y grandes, compañías comerciales, sin fines de	**Fase 1.- Valoración del riesgo** - Identificación del riesgo - Estimación de riesgos - Evaluación de riesgos

lucro (Educación, salud, servicios públicos, organizaciones no gubernamentales) Orientada a los sistemas de información.	**Fase 2.- Tratamiento del riesgo (**decidir entre las siguientes alternativas) - Retener el riesgo - Reducir el riesgo - Transferir el riesgo - Evitar el riesgo **Fase 3.- Gestión del riesgo** - Desarrollo de planes de acción - Implementación de planes de acción - Monitoreo

Tabla 6: Análisis de los aspectos propios del análisis de riesgo. Fuente:

Metodología /Estándar	Tipos de análisis	Caracterización y valoración de activos	Caracterización y valoración de amenazas	Caracterización y valoración de vulnerabilidades	Caracterización y valoración de salvaguardas	Estimación de riesgos	Tratamiento de riesgos
MAGERIT	Análisis cuantitativos y cualitativos	Detalla la forma de caracterizar activos y hace su valoración, provee de ejemplos y sugiere técnicas	Detalla la forma de caracterizar amenazas y hace su valoración, provee de ejemplos y sugiere técnicas	No se considera explícitamente	Detalla la forma de caracterizar salvaguardas y hace su valoración, provee de ejemplos y sugiere técnicas	Detalla la forma de estimar el impacto del riesgo, estimar el riesgo e interpretar los resultados, provee de ejemplos y sugiere técnicas.	Provee un proceso detallado para la gestión de riesgos.
OCTAVE	Análisis cuantitativos y cualitativos	Detalla la forma de caracterizar activos, provee guías y ejemplos	Detalla la forma de caracterizar amenazas, provee guías y ejemplos	Detalla la forma de caracterizar vulnerabilidades, provee guías y ejemplos	No se considera explícitamente	Se identifican los riesgos y se evalúa el impacto en términos de una escala predefinida (alto, medio, bajo)	Se basa en el desarrollo de: - Estrategias de protección - Planes de mitigación y lista de acciones
CRAMM	Análisis cuantitativos o cualitativos	Describe procedimientos para la identificación y valoración de activos	Describe procedimientos para la evaluación de amenazas.	Describe procedimientos para la evaluación de vulnerabilidades	No se considera explícitamente	Describe el procedimiento para la estimación del riesgo.	No se considera explícitamente.

AS/ NZS ISO 31000	Cualitativo Semicuantitativo Cuantitativo	No se define explícitamente un método de identificación y valoración de activos.	No se define explícitamente un método de identificación y valoración de amenazas.	No se define explícitamente un método de identificación y valoración de vulnerabilidades	No se define explícitamente un método de identificación y valoración de salvaguardas.	Se sugieren métodos cualitativos y cuantitativos que pueden ser aplicados. No detalla alguna técnica en particular.	Estrategias: - Evitar el riesgo - Reducir la probabilidad de ocurrencia. - Reducir las consecuencias. - Transferir los riesgos. - Retener los riesgos
MEHARI	Análisis cuantitativos y cualitativos	Describe procedimientos para la identificación de activos	Describe procedimientos para la identificación de amenazas.	Describe procedimientos para la identificación de vulnerabilidades	No se considera explícitamente.	Describe procedimientos para la estimación del riesgo.	- Retención del riesgo - Reducción del riesgo - Evitar el riesgo - Transferencia del riesgo

2.6. CONTINUIDAD DE NEGOCIO

El termino BCP2, según la definición antes descrita es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona estrategias que debe seguir al momento de presentar interrupción en las funciones o actividades que viene realizando la empresa tomando en cuenta las medidas de prevención ante la criticidad de los procesos y el tiempo de recuperación. (Gaspar Martínez, 2004)

A continuación, se presenta algunos conceptos que ayudara a entender de mejor manera un plan de continuidad de negocio según el criterio de varios autores que definen a un BCP como:

> Según el Glosario de Términos de seguridad de las Tecnologías de la Información, de Arturo Ribagorda, editado por Ediciones Coda (1997) podemos entender como Plan de Contingencia: "la definición de acciones a realizar, recursos a utilizar y personal a emplear caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización". (Navarro, Ramos Gonzáles , Del Peso Ruiz , & Del Peso Ruiz , 2012)

Y según varios autores definen el plan de continuidad de negocios de la siguiente manera:

> Gonzales Zubieta define "El Plan de Contingencias como una estrategia planificada constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por la paralización total o parcial de la capacidad operativa de la empresa" (Navarro, Manual de outsourcing informático: (análisis y contratación), 2003, pág. 78)

> Para Ramos Gonzáles el Plan de contingencias o Plan de Continuidad es uno de los puntos que nunca se deberían pasar por alto en una auditoria de seguridad, por las

2 Bussiness Continuity Plan o plan de continuidad de negocio

consecuencias que puede tener no haberlo revisado; es imprescindible conocer si funcionaría con las garantías necesarias y cubriría los requerimientos en un tiempo inferior al fijado y con una duración suficiente. (Navarro, Manual de outsourcing informático: (análisis y contratación), 2003, pág. 78)

En base a lo que manifiesta los autores Ribagorda, Gonzales y Ramos podemos concluir que un plan de continuidad de negocio es tener una visión a futuro a reducir el número y la magnitud de decisiones que tomen en un periodo determinado al momento de que se presente la interrupción de los procesos normales.

Las interrupciones en los procesos de la organización pueden suceder por varios factores ya sean estos provocados por el hombre o desastres naturales tales como; incendios, inundaciones, terremotos, etc. Si la organización desea elaborar un Plan de continuidad de negocio es necesario seguir una serie de etapas que Caballero Gonzáles & Clavero García, 2016 definen:

- **Diseño del plan y establecimiento de la política de continuidad de negocio.**

En esta etapa se identifican las actividades a realizarse antes de iniciar con el desarrollo o implementación de un BCP. (Caballero Gonzáles & Clavero García, pág. 96)

- **Conocimiento de los procesos de negocio de la organización y el análisis de riesgos que impactan en las actividades del negocio.**

Es una de las etapas más esenciales ya que se definen los productos o servicios más primordiales de la organización, de la misma manera se deben definir los elementos claves para que la empresa funcione y los riesgos a las que está expuesta. (pág. 96)

- **Medidas preventivas**

Se establecen las medidas de seguridad preventivas y proactivas esto con el fin de evitar que se produzca incidentes graves. (pág. 97)

- **Estrategias de recuperación**

Se da prioridad a las actividades que se llevan a cabo dentro de la organización se brinda mayor importancia a las que hay que salvaguardar. (pág. 97)

- **Desarrollo e implementación del plan**

En la penúltima etapa se establecen un conjunto de prácticas y procedimientos que se llevaran a cabo al momento de la recuperación del sistema y establecer la continuidad del negocio una vez que se ha producido un incidente. (pág. 97)

- **Mantenimiento del plan**

En la etapa final se difunde, revisa, actualiza y prueba que el plan es el adecuado para el negocio. (pág. 97)

Luego de haber definido un plan de continuidad de negocios, el proceso que se debe seguir a la hora de elaborar un BCP se procede a la identificación y selección de las metodologías y estándares adecuados a utilizar en este presente proyecto.

2.7.METODOLOGÍAS Y ESTÁNDARES PARA LA CONSTRUCCIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO.

Ilustración 8: Metodologías para la ejecución de un Plan de continuidad de Negocio; Fuente: (LossAd Parthners S.A.S., 2021)

Existen varias normativas y estándares que en conjunto aportan a la continuidad de negocio, pero la norma especializada para la creación del plan de continuidad de negocio es la norma ISO 22301 ya que es un estándar certificable y auditable y se utiliza como una guía para establecer un modelo que certifique la seguridad de la información en caso de que se presente un incidente. (Welivesecurity.com, 2014)

A continuación, se describe cada una de las fases de las normas de continuidad del negocio:

2.7.1. BRITISH STANDARDS INSTITUTE (BSI): BS 25999-1 BS 25999-2

Es un estándar británico desarrollado en un inicio como un Plan de Continuidad de Negocio (BCP) y luego expandido a una Administración de Continuidad de Negocio (BCM) creado y mejorado por un grupo de expertos de relevancia mundial en los sectores de la industria. Se trata de una norma certificable; es decir, que entrega una certificación a quienes comprueben conocimiento y práctica de la misma; en el cual se tienen en cuenta tanto los

recursos humanos, como las infraestructuras, la información vital, las tecnologías de información y los equipos que la soportan. (CERDA, 2013, pág. 17)

La norma consiste en una serie de recomendaciones o buenas prácticas para facilitar la recuperación de los recursos antes mencionados en caso de que se presente una crisis, y fue dividida en dos partes:

- BS 25999-1: (2005) Documento orientativo que proporciona las recomendaciones prácticas para el BCM
- BS 25999-2: (2006) Establece los requisitos para un sistema de Administración de Continuidad de Negocio (BCM): es la parte certificable a través de la implementación, auditoría y certificación (CERDA, 2013, pág. 18)

Las etapas que brinda el estándar BS 25999 son los siguientes:

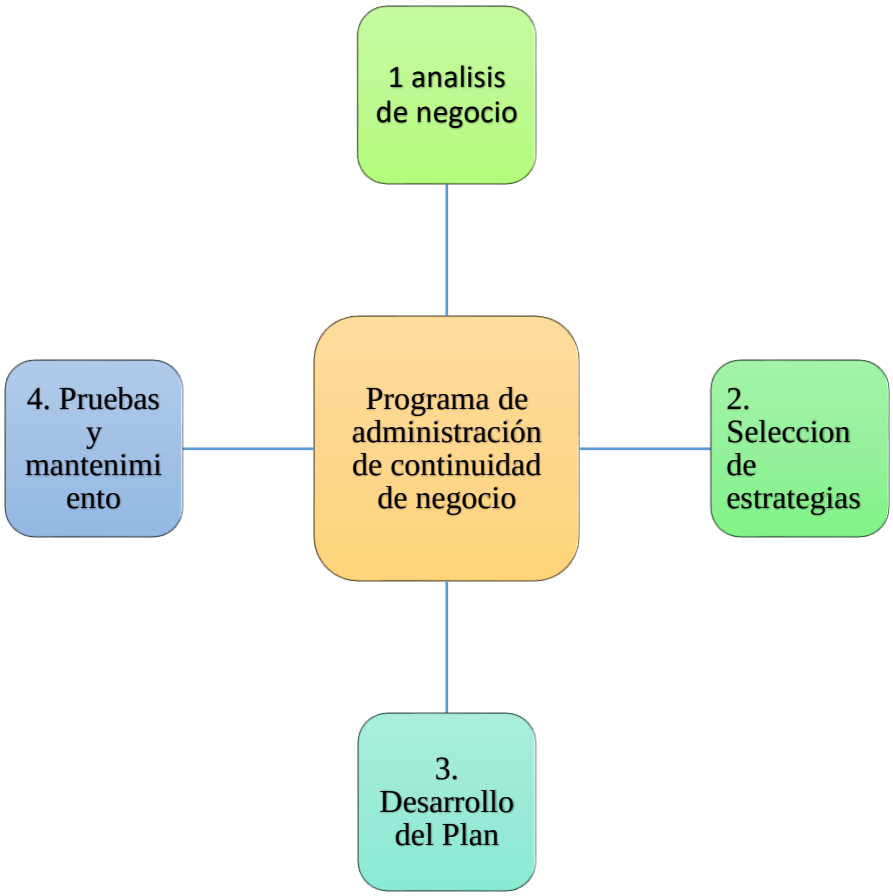


Ilustración 9: Etapas del BS 25999; Fuente: (CERDA, 2013)

Se inicia con la gestión del programa de BCP en donde se podrá establecer una aproximación de la organización a la continuidad de negocio.

La intervención de cada uno de los participantes y la alta dirección es muy importante ya que de esa manera se puede garantizar que el proceso de gestión de continuidad de negocio es el adecuado.

2.7.1.1.Fase 1. Entendimiento de la organización o análisis de negocio

En esta fase se realiza un análisis de negocio, se identifica y entiende los procesos del negocio ya que es la parte fundamentan de la organización y servirá para desarrollar el plan de continuidad de negocio de esta manera se asegura la continuidad de la actividad en caso de que se presente una contingencia. (SÁEZ VARGAS, 2013)

Una vez analizada la organización se procede a la evaluación de los riesgos que es la determinación de vulnerabilidades internas o externas de la organización esto con el fin de tener una visión a futuro de los posibles daños que puede causar al normal proceso operacional de la empresa.(Nieto, 2015)

Según Quevedo, 2012 señala que el entendimiento de la organización esta constituida por el analisis de impacto en el negocio que determina el impacto que puede provocar las posibles interrupciones. Debe incluir:

- Las actividades críticas para dar soporte a los procesos de negocio.
- El impacto que produce la interrupción en las diferentes actividades.
- El tiempo máximo que puede soportar la organización sin que los servicios sufran algún daño grave.
- Identificación de dependencias entre actividades.
- Identificar las actividades más críticas dentro de la organización.
- El tiempo de recuperación para cada una de las actividades criticas identificadas, este tiempo debe estar dentro del límite máximo tolerable de interrupción. (pág. 96)

2.7.1.2.Fase 2. Selección de estrategias

En esta etapa se define cada uno de los pasos a seguir para la recuperación del funcionamiento de las actividades críticas que se presentaron dentro de la organización esto dependerá del periodo de tiempo tolerable de interrupción para que de esta manera no pueda afectar los servicios y las consecuencias no lleve a cabo ninguna acción. Quevedo(2012) refiere que en la determinación de las estrategias de continuidad de negocio la empresa debe definirse a nivel de los diferentes recursos necesarios:

- Uno de los primeros elementos necesarios es el desarrollo y la documentación de una estructura de respuestas ante los incidentes.
- Formar al personal en diversas habilidades y no exclusivas de sus actividades asignadas.
- En el ámbito tecnológico las medidas que deben seguir es el tiempo y nivel de recuperación objetivo (RTO Recovery Time Objective y RPO Recovery Point Objective) para los sistemas que dan soporte a las actividades claves identificadas en el análisis BIA.
- También se debe garantizar la confidencialidad, integridad y disponibilidad de la información esto lo podemos lograr mediante copias de seguridad que se realicen frecuentemente.
- Determinar como la relación de los interesados será administrada durante el tiempo de interrupción.
- Se debe tener muy en cuenta las actividades no definidas como críticas.

2.7.1.3. Fase 3. Desarrollo e implementación de las respuestas BCM

Es la fase en la cual se desarrolla e implementa los planes para garantizar la continuidad de las actividades críticas y la gestión de los incidentes.

Estructurar las respuestas a incidentes: se veden realizar una serie de secuencias de operaciones una vez que se haya presentado el incidente.

Desarrollar los planes de la gestión de continuidad de negocio: en este caso es necesario recuperar las actividades interrumpidas. Y por último el desarrollo de los planes de gestión de incidentes. (Quevedo, 2012)

2.7.1.4. Fase 4. Pruebas y mantenimiento

En esta última fase es necesario realizar diversas pruebas esto con el fin de determinar la eficacia con la que puede continuar la organización ante la presencia de alguna interrupción.

Se tiene que validar cada uno de los planes y procedimientos ya desarrollados, la revisión y el mantenimiento deben realizarse de una manera constante o en tiempos definidos.(Quevedo, 2012)

2.7.2 NORMA ISO 22301

La ISO 22301 es una norma internacional de gestión de continuidad de negocio, fue remplazada a partir de la norma británica original BS 25999-2 en el año 2012 “Seguridad de la sociedad: Sistemas de continuidad de negocio-requisitos”. (ISO, s.f.)

Esta metodología aplica el ciclo Plan-Do-Check-Act (conocido como PDCA por sus siglas en Ingles), esto ayuda a la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de su efectividad.(Zapata, 2015)

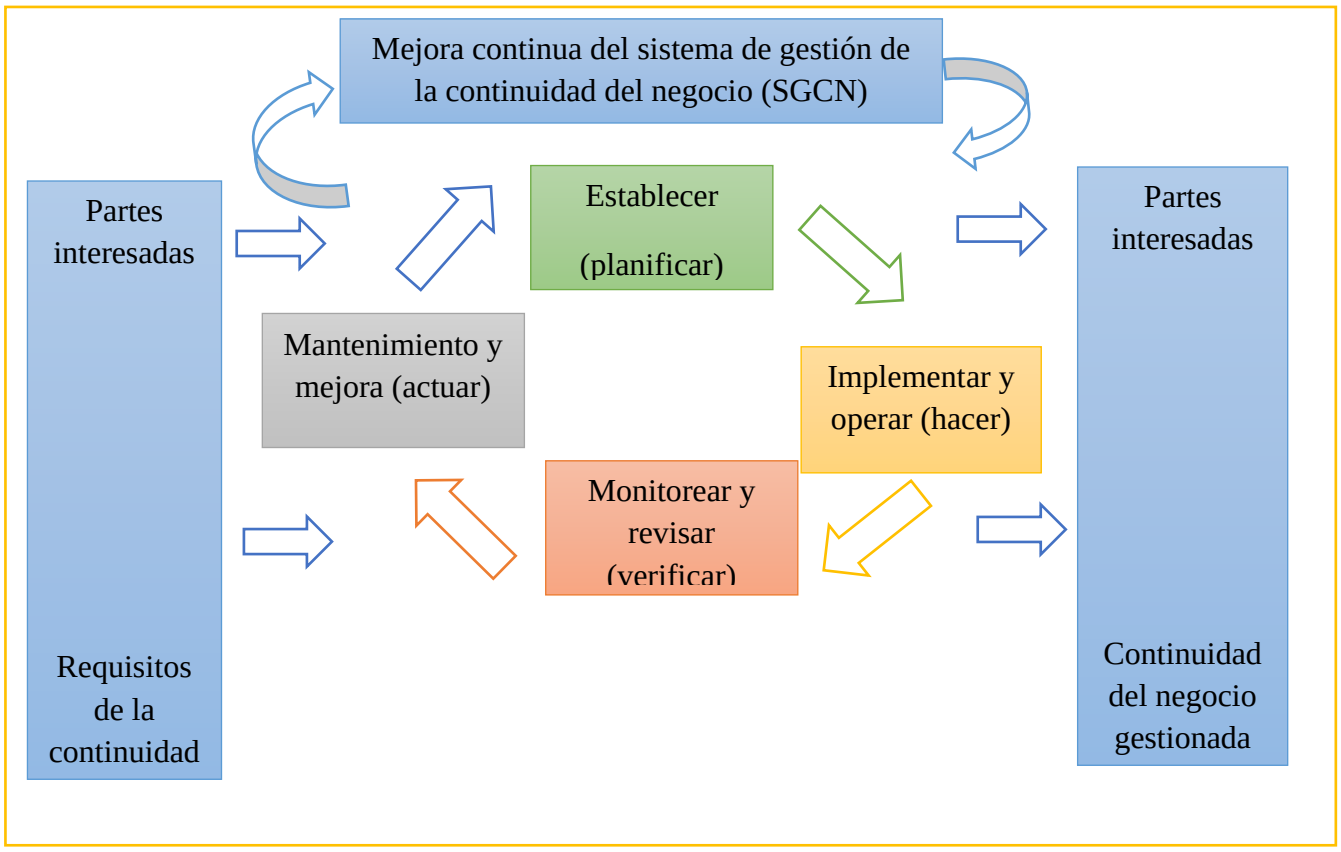


Ilustración 10: Modelo PDCA aplicado al SGCN; Fuente: (CATAÑO TURIÀN & PÉREZ MONSALVE, 2015).

(ISO, 2012) describe el modelo PDCA aplicado al sistema de gestión de continuidad de negocio.

Plan (Planificar) se establece las políticas de continuidad de negocio, de la misma manera se establece los objetivos, los controles, procesos y los procedimientos todo esto estarán acorde a las políticas y los objetivos organizacionales.

Do (Hacer) se aplica las políticas los controles, proceso y el procedimiento de continuidad

Check (Verificar) se realiza una supervisión del sistema de gestión tomando en cuenta los objetivos y las políticas establecidas. Una vez realizada estos pasos se procede a informar a los niveles correspondientes y que proporcionen las medidas a tomar para su corrección y mejora.

Act (Actuar) en la última etapa se debe mantener y mejorar la técnica de gestión de continuidad de negocio, considerando el resultado de la revisión de la dirección de la organización.

2.7.2.1 Beneficios de la ISO 22301

Según la (ISOtools, 2015) describe los beneficios más relevantes que puede presentar esta norma es que sus políticas y procedimientos son reconocidos internacionalmente.

Además de eso proporciona un marco de continuidad de negocio como un soporte fundamental que abarca globalmente el gobierno corporativo, y minimiza la responsabilidad de riesgo ya que se tiene un mayor grado de responsabilidad.

La metodología recomendada para el desarrollo de la GCN (apoyada en ISO 22301:2012), propone un proceso comprendido desde el inicio del proyecto hasta la definición de la estructura de respuesta ante incidentes

2.6.3.1 Fases de la ISO 22301

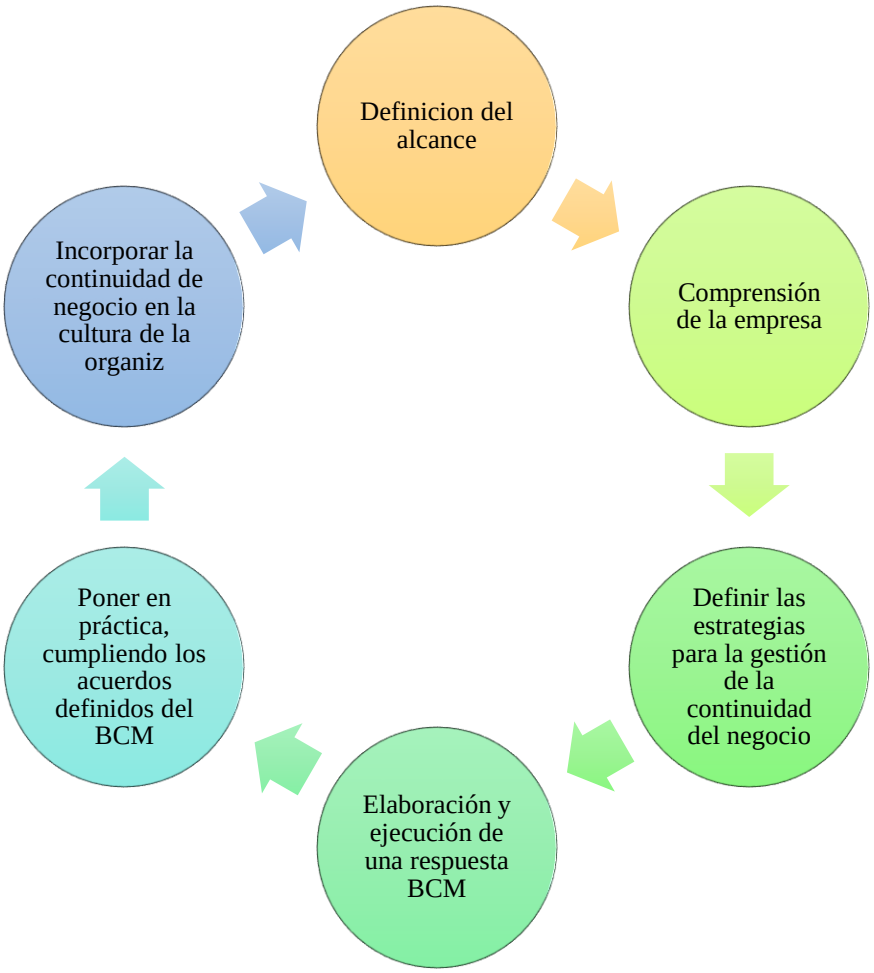


Ilustración 11: Pasos para la gestión de continuidad de negocio. Fuente: (ISO, 2018)

Paso 1: Definición del alcance

En esta fase se diseña el programa de gestión de un BCP, considerando el tamaño y la **propia complejidad de la empresa**. Se define el equipo básico encargado del BCM, incluyendo funciones y responsabilidades. (ISOTools Excellence, 2018)

Paso 2: Comprensión de la empresa

En esta etapa, se obtiene la información para priorizar las actividades, diferenciando aquellas que son clave de las que son de apoyo, así como **los recursos requeridos por las mismas.** Se analiza el impacto que genera el negocio y se evalúan los riesgos. (ISOTools Excellence, 2018)

Paso 3: Definir las estrategias para la gestión de la continuidad del negocio

Mediante esta fase se determinan todas las actividades de negocios clave por las que la empresa puede **recuperar su servicio dentro de un determinado plazo** tras una interrupción. (ISOTools Excellence, 2018)

Paso 4: Elaboración y ejecución de una respuesta BCM

Aquí se desarrollan todas las respuestas necesarias ante las situaciones de emergencia. Es decir, se detallarán todos los planes con los pasos a seguir para **poner en práctica tanto antes de la interrupción, como durante y después** de la misma, con el fin de reestructurar los procesos de negocio por orden de prioridad. (ISOTools Excellence, 2018)

Paso 5: Poner en práctica, cumpliendo los acuerdos definidos del BCM

Mediante este paso se pone de relieve el grado en que las estrategias y planes son adecuados al propósito perseguido, mediante la **planificación de ejercicios en ciertos intervalos que permitan revisar la continuidad del negocio**, además, de detectar la oportunidad de mejora. (ISOTools Excellence, 2018)

Paso 6 Incorporar la continuidad de negocio en la cultura de la organización

En esta última se debe de conseguir que la continuidad de negocio sea parte de los valores de **todos los miembros de la organización**, se crea confianza en la capacidad de la empresa de hacer frente a las interrupciones. (ISOTools Excellence, 2018)

2.8.CUADRO COMPARATIVO DE NORMAS Y ESTÁNDARES PARA LA ELABORACIÓN DE UN PLAN DE CONTINUIDAD DE NEGOCIO

Luego de haber realizado una investigación bibliográfica de las normas y estándares para la elaboración de un Plan de continuidad de negocio se procede a elaborar una tabla comparativa que ayudara a seleccionar la norma o estándar con la que se va a trabajar en la presente investigación.

Tabla 7: Tabla comparativa de normas y estándares de un BCP Fuente: (VARGAS, s.f.)

Estándares, Metodologías y Buenas Prácticas	Ventajas	Desventajas
BS 25999	Orientada a la Gestión de la Continuidad del Negocio.	Contempla parcialmente el tema de Recuperación ante desastres de TI (Tecnologías de la Información).
BS 25777	Establece un marco para crear y mejorar un sistema de gestión de continuidad de servicios en los Sistemas de TI.	Contempla parcialmente el tema de Continuidad del Negocio, se usa el estándar BS 25999 como complemento
ITIL	Guía de buenas prácticas destinadas a facilitar la entrega de servicios de TI de alta calidad abarcando la infraestructura, desarrollo y operaciones de TI.	Contempla la mayoría de los procesos relacionados con la continuidad del servicio, no tiene un enfoque integrado de todo el proceso
ISO 31000	El propósito de esta norma, es proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo	ISO 31000 no se puede utilizar con fines de certificación, pero proporciona una guía para los programas de auditoría interna o externa
ISO 22301	Orientada a la Gestión de la Continuidad del Negocio con más más énfasis en la comprensión de los requisitos, el establecimiento de los objetivos y en la medición del desempeño.	Menos prescriptiva que las normas británicas, lo que deja una puerta abierta a interpretaciones por parte de las organizaciones que aplican la norma, así como por parte de los auditores.

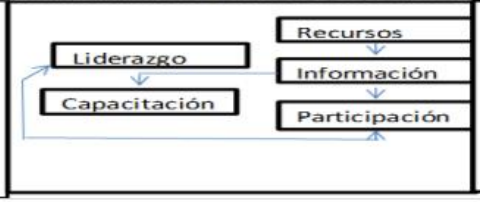
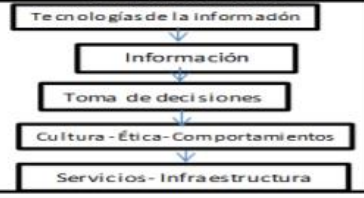
REFERENTES INTERNACIONALES PARA LA CONTINUIDAD DEL NEGOCIO				
MEJORA CONTINUA	ISO/IEC 27005: 2011 (A)	22301:2012 (B)	COBIT 5 ©	BUENAS PRÁCTICAS (D)
PLANIFICAR	**Establecimiento del contexto** Conocer la organización Determinar alcances y limitaciones **Identificación y estimación de riesgos** Identificar activos de soporte/ Procesos/ Datos Determinar amenazas * Estratégias * Materiales * Técnicas * Accidentales *Intencionales Establecer prioridades Evaluación de riesgos **Plan de Comunicación** * Aspectos generales sobre los riesgos * Comunicación sobre la marcha * Comunicación de resultados **Establecer acciones para enfretar los riesgos definidos** **(ISO, 2011) (SGSI, 2015)**	**Contexto de la organización** Actividades/ Priorizadas Vinculación de objetivos y políticas Necesidades de partes interesadas Legislaciones Estrategia organizacional * Integración de los requisitos del sistema con los proceso Determinación de riesgos Evaluación de los riesgos definidos Determinación de : **Políticas de CN** **Requisitos del BCP** **Principios del BCP** **Objetivos del BCP** **Determinar procedimientos de actuación** Protocolos de comunicación Impactos de eventos no deseados Presuposiciones y análisis de interdependencia **(Estándar Internacional ISO 22301, 2012)**	Definir objetivos organizacionales **Definir objetivos de TI** Definir principios, políticas y modelos Guías prácticas **Actividades para el logro de los objetivos** **Definir requerimiento de CN, objetivos y alcance** Definir escenarios de incidencia **Definir estrategias de CN** Socialización y capacitación Definir acciones de capacitación Procedimientos de actuacion **(Palacios, 2016)**	**Entendimiento de la organización** **Identificar necesidades** Identificar peligros y evaluación de riesgos Matriz de riesgos Probabilidad de ocurrencua Vulnerabilidades Impacto **Estrategias de mitigación** **(Blanco, 2008)**
HACER	**Implementación del tratamiento de riesgos** **(SGSI, 2015)**	Implantar Operación Análisis del impacto del SGCN Implementar estrategias de CN Aplicación de los procedimientos **(Estándar Internacional ISO 22301, 2012)**	**Operar** **Desarrollo e implementacion** **Ejecutar** **(Palacios, 2016)**	**Implementación** **Operaciones y procedimientos** **Ejecutar planes de soporte al programa** **(Blanco, 2008)**
VERIFICAR	**Monitoreo y revisión** Control de cambios Evaluar cumplimiento de los planes Análisis costo-beneficio **(ISO, 2011)**	**Revisar y Monitorear** Supervisión de la dirección Pruebas de seguimiento Evaluacion del desempeño * Revisar periodicamente Metas * Auditorías internas **(Estándar Internacional ISO 22301, 2012)**	**Monitorear** **Pruebas y revisión** **Revisiones post-reanudacion** **Evaluacion de CN** **Acuerdos de respaldo** **(Palacios, 2016)**	**Dirección, control y coordinación** **Evaluaciones** **Monitoreo** **(Blanco, 2008)**
ACTUAR	**Mantener la gestión continuamente actualizada** **(ISO, 2011)**	**Mejora continua** **Mantenimiento del plan** **Sistematización** **Informes de resultados** **(Estándar Internacional ISO 22301, 2012)**	**Construir e implementar mejoras** **Mantenimiento** **(Palacios, 2016)**	**Recuperación** Acciones correctivas y preventivas **(Blanco, 2008)**
PILARES	INFORMACIÓN			

Ilustración 12: Comparación de referentes enfoques de un plan de continuidad de negocio Fuente: (Rojas Bustamante , UDLA, 2017, pág. 51)

CAPITULO III

3 MARCO METODOLÓGICO

3.1 Enfoque de la Investigación

En la presente investigación se considera cada uno de los posibles problemas a presentarse en el correcto funcionamiento de la empresa Cañar Net.

Para esta investigación se manejará variables tanto cualitativas como cuantitativas por lo cual el enfoque es cuali-cuantitativo mixto.

3.2 Nivel de Investigación

La investigación será de carácter descriptivo por lo que se realizará un levantamiento de información del departamento de TI de la empresa Cañar Net.

3.3 Población y muestra

El universo de la investigación estará centrado en el gerente, responsable del área de TI de la empresa Cañar Net.

3.4 Métodos de investigación

En esta investigación se utilizará la metodología deductiva, que va de lo general a lo particular.

3.5 Técnicas e instrumentos de recolección

Para el levantamiento y recolección de la información se realizará mediante entrevistas a los directivos del proyecto de TI.

3.6 Tratamiento de la información

La información obtenida de las entrevistas a los directivos y el responsable del área de TI será debidamente tratada y sistematizada en forma de matrices.

3.7 Interpretación de resultados

El análisis del nivel de madures, será realizado en base a una entrevista realizada al gerente de la empresa proveedora de internet Cañar Net y al encargado de TI, quienes conformaran el 100% de la población.

3.8 Análisis de resultados

Para determinar el estado actual y los procesos manejados dentro de la empresa proveedora de internet Cañar Net se aplicó la encuesta al director del área de TI y al gerente de la empresa.

Cañar Net Internet de alta velocidad y TV en full HD	Empresa **CAÑAR NET**	**Código:** G001 **Fecha:** 00/00/2021
	Encuesta Gerente	**Versión:** 01 **Pagina:**

Objetivo de la Encuesta: Encontrar los puntos problemáticos que serán abordados en el proyecto.

Preguntas	**Respuestas**		
	Si	**No**	**Análisis**
¿La empresa cuenta con un plan de continuidad de negocio?	X		La empresa Cañar Net, cuentan con plan de continuidad de negocio, pero no implementado
	Análisis		
¿La empresa proveedora de internet cuenta con procesos bien definidos y con sus respectivos responsables?	La empresa cuenta con procesos, pero no bien definidos y de la misma manera respecto a sus responsables.		
	Si la gestiona	**No lo gestiona**	**Análisis**
¿La empresa proveedora de internet realiza la gestión de riesgos de seguridad de la información?	X		La empresa gestiona y cuenta con un plan de tratamiento de riesgo, existe un plan que tienen en cumplimiento al ente de control.
	Análisis		
¿Cuándo se produce problemas con los equipos o suspensión de servicio, estos son atendidos con el fin de disminuir el	La empresa manifiesta que existen problemas en los equipos, y para disminuir el impacto se reemplaza el equipo, se actualiza el equipo, repara el equipo entre otras.		

impacto que puede ocasionar a la empresa?	En cuanto a la suspensión en el servicio, la empresa manifiesta que no existe tal inconveniente, que depende de los problemas en los equipos**.**		
	Analisis		
¿Cuál es el tiempo que emplea para realizar el análisis de gestión de riesgos dentro de la empresa?	No existe un tiempo defindo		
	Si	**No**	**Analisis**
¿Alguna vez ha realizado la identificación de los factores determinantes de los riesgos que enfrenta su empresa?	X		La identificación de los factores de riesgos si lo han realizado, pero no se han documentado
	Analisis		
¿Conoce usted la probabilidad de ocurrencia y el impacto de los riesgos que su empresa enfrenta?	El gerente de la empresa, responde que si conoce los riesgo, su impacto, su probabilidad y que consta en el informe remitido al ente de seguridad.		
	Analisis		
¿Dentro de su empresa que tipos de información maneja?	La Empresa Cañar Net Maneja informacion de: Clientes, Proveedores, Personal.		
	Analisis		
¿De los tipos de información manejada dentro de la empresa a cuál de ella considera importante?	Toda la informacion manejada en la Empresa Cañar Net es importamte.		

	Empresa **CAÑAR NET**	**Código:** G001
	Entrevista director	**Fecha:** 11/08/2021 **Versión:** 01 **Pagina:**

Objetivo de la Encuesta: Encontrar los puntos problemáticos que serán abordados en el proyecto.

Preguntas	Respuestas
	Análisis
¿La empresa proveedora de internet cuenta con un plan de continuidad de negocio?	La empresa Cañar Net, cuentan con plan de continuidad de negocio, pero no implementado
	Análisis
¿Cree usted que el departamento de TI tiene riesgos tecnológicos que puedan afectar los diferentes procesos de la empresa?	Si, existen riesgos que pueden afectar tanto al área como a la empresa, provocando una pausa en los servicios.
	Análisis
¿Dentro del departamento de TI cuales son los procesos más críticos que afecten el normal desempeño de los servicios?	En la empresa existen dos procesos críticos el proceso de Gestión y la de administración de red de datos las cuales pueden afectar el normal desempeño de la empresa.
	Análisis
¿Ante la identificación de amenazas informáticas ¿El departamento de TI tiene estandarizado los tiempos de	El departamento de TI y la empresa en general no tienen tiempo definido, sin embargo, el director del área de TI

recuperación en caso de que se llegaran a ejecutar estas amenazas?	manifiesta que se trata de minimizar la afectación en el servicio.		
	Analisis		
¿Dentro del área de TI Tiene definido un manual de procesos o procedimientos en la proveedora de internet?	El departamento de TI no cuenta con un manual de procesos, pero sin embargo se encuentra por aprobar el manual de funciones de la empresa como tal.		
	Si	**No**	**Analisis**
¿El departamento de TI cuenta con procesos bien definidos y con sus respectivos responsables?		**X**	
	Si	**No**	**Analisis**
¿Conoce usted la probabilidad de ocurrencia y el impacto de los riesgos que el departamento de TI enfrenta?		X	Dentro de la empresa no se tiene conocimiento de la probabilidad de ocurrencia, pero si se tiene conocimiento de los riesgos que se presentan, la cuales buscan ser analizados de inmediato.
	Analisis		
¿La empresa proveedora de internet cuenta con un plan de control operacional de seguridad de información ante la presencia de amenazas o riesgos?	La empresa no cuenta con un plan de control de seguridad de la informacion ante la presencia de incidentes.		
	Analisis		
¿Cumple usted con la seguridad física en el departamento de TI?	No.		

3.9 Análisis general de la encuesta

De acuerdo al análisis realizado de cada pregunta aplicada al gerente y al director de TI de la empresa Cañar Net, se ha podido constatar que no existe una ligera gestión en lo que respecta la continuidad de negocio, la empresa y el departamento de TI no cuentan con procesos definidos por lo que la empresa Cañar Net no es eficaz en su totalidad, no cuentan

con una coordinación y un control de sus funciones, de la misma manera no tienen tiempo de recuperación definidos, sin embargo se trata de minimizar la afectación en el servicio.

La Empresa proveedora de servicio de internet Cañar net, debe brindar mayor importancia a las amenazas y las consecuencias que puede ocurrir cuando se presenta un riesgo, es importante establecer el tiempo de recuperación y así conocer el tiempo máximo permitido para restablecer el servicio antes de que se materialice las amenazas y ponga en riesgo la organización.

3.10 Selección de la metodología para el plan de continuidad de negocio.

Se realizó una matriz comparativa de los estándares que permiten la elaboración del plan de continuidad de negocio Tabla 7, en la cual se analizó las características, ventajas y desventajas de las mismas, por otra parte, también se basó en una comparativa tabla 8, realizada por Jairo Rojas B., con la cual se llega a determinar la ISO 323001como el estándar seleccionado, debido a que se enfoca principalmente en que la organización tome la determinación de que aspectos serán cubiertos por la continuidad de negocio y del mismo modo decida que será excluido y comunicado a todas las partes tanto externas como internas.

3.11 Selección de la metodología para Análisis y gestión de riesgo en la seguridad de la información.

En base a una matriz comparativa realizada de todas las metodologías de análisis y gestión de riesgo, en las cuales se evaluaron los siguientes criterios como: Tipo de análisis, caracterización y valoración de activos, caracterización y valoración de amenazas, caracterización y valoración de vulnerabilidades, caracterización y valoración de salvaguardas, estimación de riesgo, tratamiento de riesgo, de la mimas manera se realizó un análisis del ámbito de aplicación, las etapas y las faces que lleva cada metodología de gestión de riesgo, una vez realizada la comparación de cada una de ella, se determinó que para el desarrollo del presente trabajo de investigación se hará uso de la metodología MAGERIT.

Todo lo antes descrito es una parte de las actividades de planificación, en donde se toman decisiones de tratamiento. Estas decisiones se pueden llegar a materializar en la etapa de implementación en donde es conveniente desplegar elementos que permitan la monitorización de las medidas desplegadas para poder evaluar la efectividad de las mismas y actuar en consecuencia, dentro de un circulo de mejora continua.

CAPÍTULO IV

A continuación, se presenta la propuesta para la elaboración del plan de continuidad de negocio para la empresa Cañar Net con el objetivo de mantener la funcionalidad de sus actividades ante la presencia de incidentes dentro y fuera de la organización.

Para la elaboración de esta propuesta se va a tomar como referencia las fases de la norma ISO 22301 y la metodología Magerit para el análisis y gestión de riesgos con la información recolectada de la empresa mediante la encuesta antes descrita.

4 DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIOS TOMANDO COMO REFERENCIA A LA NORMA ISO 23001

4.1 DEFINICIÓN DEL ALCANCE

Para el alcance de los procedimientos documentados en este Plan de Continuidad de Negocios está restringido a los servicios críticos proporcionados por la empresa Cañar Net. El alcance de los procedimientos cubre los siguientes servicios:

Departamento de TI.

4.2 COMPRENSIÓN DE LA EMPRESA

4.2.1 MISIÓN

Ser una empresa que trabaja profesional y capaz para poder brindar soluciones de conectividad que satisfaga las necesidades de todos los usuarios.

4.2.2 VISIÓN

Brindar excelencia en el servicio de Internet y las telecomunicaciones en general con valores y principios propios de una organización moderna, dinámica y creativa. Satisfacer los requerimientos de comunicación con soporte personalizado y especializado para lograr que cada vez más usuarios nos consideren parte de su organización.

4.2.3 VALORES

- Trabajo en equipo.
- Responsabilidad.
- Respeto.
- Honestidad

4.2.4 Identificación y análisis de procesos organizacionales y sus interrelaciones

Para la identificación de procesos de la empresa Cañar Net se utilizaron datos proporcionados por el gerente de la empresa los mismos que se detallan a continuación:

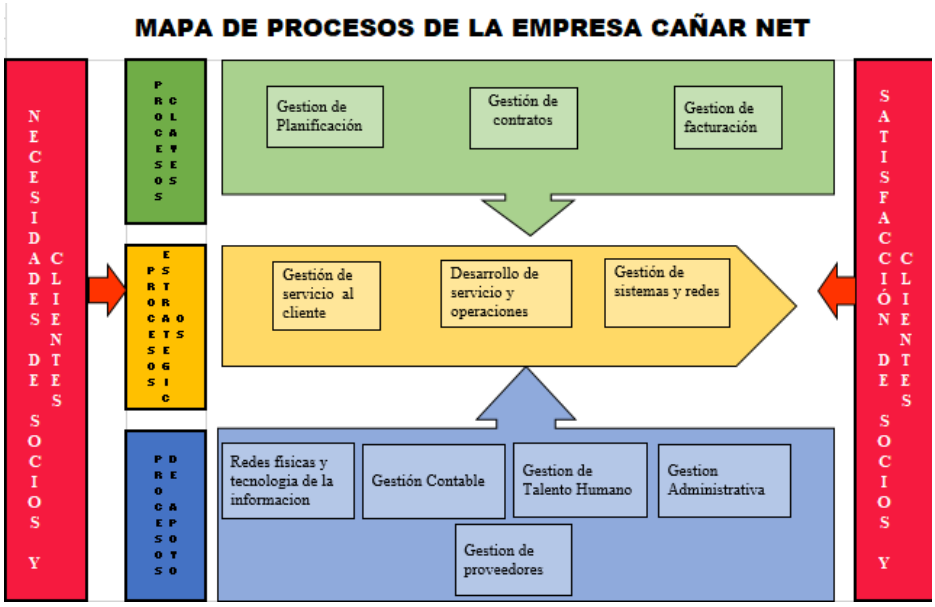


Ilustración 13: Mapa de Procesos de la empresa Cañar Net. Fuente: Empresa Cañar Net.

Como se observa en la gráfica anterior Cañar Net se encuentra formada por macro procesos de los cuales 3 pertenecen a los Procesos Claves, seguidamente se tiene 3 Procesos Estratégicos y finalmente 5 Procesos de Apoyo.

4.3 EVALUACIÓN DEL IMPACTO DEL NEGOCIO Y DE LOS RIESGOS EN BASE A LA METODOLOGÍA MAGERIT.

Luego de haber realizado el entendimiento y análisis de los procesos con los que cuenta Cañar Net se procede a la determinación de los procesos críticos. Para la calificación de la

criticidad de los procesos y subprocesos se determina aspectos fundamentales que pueden influir al mismo, cabe recalcar que estos elementos fueron seleccionados del libro II de Magerit 3.0

Tipos de procesos	MacroProceso	Proceso	SubProceso	Criterios de valoración												
				[pi]información de carácter personal	[lpo]Obligaciones legales	[si]Seguridad	[cei]intereses comerciales o económicos	[da]Interrupción de servicio	[po]Orden público	[olm]Operaciones	[adm]Administración y gestión	[lg]Pérdida de confianza(reputacion)	[crm] Persecución de delitos	[rto]Tiempo de recuperacion del servicio	[lbl.nat] Información clasificada(nacional)	Total
PROCESOS CLAVES	Gestion de Planificación	Plan estratégico institucional		4	5	1	7	1	1	1	7	3	1	0	8	39
		Plan Operativo Anual		3	5	1	7	1	1	1	7	3	1	0	8	38
	Gestión de Contratos	Etapa Precontractual	Planeacion	2	1	1	1	0	0	1	1	1	0	0	8	16
			Documentos Presupuestales	2	1	1	1	0	0	1	1	1	0	0	8	16
			Proceso de selección	1	1	1	1	0	0	1	1	1	0	0	8	15
		Etapa Contractual	Suscripción y legalizacion del contrato	2	3	1	1	0	0	1	1	1	0	0	8	18
			Ejecución Contractual	1	1	1	1	0	0	1	1	1	0	0	8	15
			Supervición	1	1	1	1	0	0	1	1	1	0	0	8	15
			Pagos	2	7	1	1	0	0	1	1	1	0	0	8	22
		Etapa Poscontractual	Liquidación	2	7	1	1	0	0	1	1	1	0	0	8	22
			Obligaciones post-contractuales	1	1	1	1	0	0	1	1	1	0	0	8	15
			Indemnidad	1	1	1	1	0	0	1	1	1	0	0	8	15
	Gestión de Facturación	Obligaciones Formales	Preparar la factura	2	1	1	1	1	0	1	1	1	0	0	5	14
			Envío en tiempo y forma al cliente	1	1	1	1	0	0	1	1	1	0	0	5	12
		Gestion de Cobro	Planificación, seguimiento, avisos y tramitar el cobro	2	1	1	1	0	0	1	1	1	0	0	5	13
			Anticipar Facturas y cobrar de inmediato	1	1	1	1	0	0	1	1	1	0	0	5	12
PROCESOS ESTRATEGICOS	Gestión de servicio al cliente	Ventas		5	5	1	7	1	0	5	1	7	0	0	8	40
		Gestión de pedidos		2	1	1	2	1	1	5	1	7	0	1	8	30
		Gestión de incidentes		6	9	10	9	9	9	10	9	9	0	7	8	95
		Facturación y pagos		2	7	3	2	0	1	0	1	7	0	0	8	31
	Desarrollo de servicio y operaciones	Planificación y desarrollo del servicio		2	1	3	2	1	1	5	9	9	0	7	8	48
		Configuración del servicio		2	1	3	3	9	9	10	1	9	4	7	8	66
		Gestión de incidentes en el servicio		4	1	10	7	9	9	9	9	9	4	7	8	86
		Gestión de la calidad del servicio		6	9	10	7	9	9	10	9	9	4	7	8	97
		Tarifas y Descuentos		1	1	1	2	0	0	1	1	1	0	0	8	16
	Gestión de sistemas y redes	Planificación y desarrollo de redes		1	5	3	2	9	9	5	9	9	4	7	8	71
		Aprovisión de redes		4	9	1	2	5	9	5	1	9	4	7	8	64
		Gestión de inventario de redes		1	3	1	2	1	1	1	1	9	4	1	8	33
		Mantenimiento y restauración de redes		6	9	10	7	9	9	10	9	9	4	7	8	97
		Gestión de datos de redes		4	5	1	2	5	9	5	9	3	4	7	8	62
PROCESOS DE APOYO	Redes físicas y tecnología de la información	Gestión de tecnologías de la información y seguridad informatica	Respaldo y restauración de información de los servidores	6	9	10	9	9	1	1	7	7	4	7	8	78
			Procedimiento para mantenimiento software y hardware.	3	1	1	3	3	1	3	1	3	4	7	8	38
	Gestión Contable	Gestión Económica	Registrar y contabilizar ingresos economicos	1	5	3	2	1	0	1	1	2	4	1	8	29
		Gestión Financiera	Generar Información Financiera	1	5	3	2	1	0	1	1	2	4	1	8	29
		Gestión de seguridad Contable	Asegurar la calidad de la información contable	1	5	3	2	1	0	1	1	2	4	1	8	29
	Gestión de Talento Humano	Incorporación del Talento Humano		2	7	1	1	1	0	1	7	5	0	1	8	34
		Permanencia de Talento Humano		2	3	1	1	1	0	1	7	5	0	1	8	30
		Desvinculación de Talento Humano		2	5	1	1	1	0	1	7	5	0	1	8	32
		Administración de nomina		1	1	1	1	1	0	1	1	1	0	1	8	17
	Gestión Administrativa	Administración de adquisición de bienes y servicios		3	9	7	7	1	0	1	3	7	4	1	8	51
		Gestion de Activos Fijos e inventarios		1	3	7	3	1	0	1	3	5	4	1	8	37
		Gestión de servicios administrativos varios	Gestión de archivo general/bodega	1	1	3	3	1	0	1	3	1	0	1	8	23
			Gestion de mensajeria	1	1	3	2	1	0	1	3	1	0	1	8	22
	Gestión de proveedores	Administración de las relaciones de los Proveedores		3	3	3	2	1	1	1	1	7	4	1	8	35
		Gestion de Información de Proveedores		3	5	3	7	1	1	1	1	7	4	1	8	42
		Gestión de Riesgo, Diversidad y Cumplimiento de Proveedores		3	5	3	7	1	1	1	1	7	4	1	8	42

Ilustración 14: Matriz de calificación de procesos y subprocesos de Cañar Net.

En la ilustración Nº12 está constituida por el tipo de proceso, Macro proceso, Proceso, Subproceso con el cual dispone la empresa Cañar Net, de la misma manera se encuentra formada por los criterios de valoración del Libro II Catalogo de Elementos MAGERIT versión 3.0. Luego de tener definido todo lo antes mencionado se procede a la calificación de cada una de ella, eligiendo una escala detallada de diez valores, dejando en valor 0 como determinante de la que sería un valor despreciable (a efectos de riesgo).

Tabla 8: Escala de valores. Fuente: (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., 2012)

	Valor	Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante

Luego de la calificación se realizó la sumatoria de todas las denominaciones del criterio de valoración para que finalmente se obtenga la lista de los procesos más críticos dentro de la institución.

4.3.1. Identificación de activos

Para la identificación de los activos se obtuvo en base a los datos e información brindada por el gerente general de la empresa Cañar Net, posteriormente se lo categorizo por el tipo y en relación con los procesos y subprocesos antes ya calificados.

Para el levantamiento de los activos se dividió en dos grupos, activos esenciales para la institución y activos secundarios en los cuales se encuentran hardware, software, redes informáticas, personal y estructura de la organización.

A continuación, se presenta un inventario de activos de información pertenecientes a la empresa Cañar Net.

Tabla 9: Inventario de activos de información Cañar Net; Autor: Desarrollador de Tesis.

Caracterización	Código activo	Denominación
[D] Datos / Información	Ac-Sis-001	Red de Datos
[essential] Activos esenciales	Ac-Sis-002	Documentación de información
[SW] Software - Aplicaciones informáticas	Ac-Sis-003	Sistema RP
[SW] Software - Aplicaciones informáticas	Ac-Sis-004	Sistemas informáticos
[P] Personal	Ac-Sis-005	Equipo Técnico y Soporte
[COM] Redes de comunicaciones	Ac-Sis-006	Servidor Proxy
	Ac-Sis-007	Transmisor Óptico ODF
	Ac-Sis-008	Equipo de soporte
	Ac-Sis-009	Antena Sectorial 19 dbi 120g
	Ac-Sis-010	Antena mimosa Al B5c para punto a punto
	Ac-Sis-011	RBLHG-5nD (Para Clientes)
	Ac-Sis-012	OLT ZTE de 34 puertos
[HW]Equipamiento informático (hardware)	Ac-Sis-013	Router principal Backup (Cañar)
	Ac-Sis-014	Swich 12 puertos
	Ac-Sis-015	Router Honorato Vasquez
	Ac-Sis-016	Router Pilcopata
	Ac-Sis-017	Router Altarhurco
	Ac-Sis-018	Router Hueran
	Ac-Sis-019	Equipo de monitoreo

Luego de categorizar los activos se lo relaciono con los procesos para posteriormente calificarlos en base a las dimensiones que ofrece Magerit.

MacroProceso	Proceso	SubProceso	Activos
Gestión de servicio al cliente	Gestión de incidentes		Equipo de monitoreo
			Sistemas informaticos
			Equipo de soporte
Desarrollo de servicio y operaciones	Gestión de incidentes en el servicio		Sistema RP
			Antena Sectorial 19 dbi 120g
			Antena mimosa Al B5c para punto a punto
	Gestión de la calidad del servicio		RBLHG-5nD(Para Clientes)
			OLT ZTE de 34 puertos
Gestión de sistemas y redes	Planificación y desarrollo de redes		Ducumentacion de informacion
			Red de Datos
	Mantenimiento y restauración de redes		Transmisor Optico ODF
			Swich 12 puertos
des físicas y tecnologia de la informaci	Gestión de tecnologías de la información y seguridad informatica	Respaldo y restauración de información de los servidores	Servidor Proxy
			Router principal Backup (Cañar)
			Router Honorato Vasquez
			Router Pilcopata
			Router Altarhurco
			Router Hueran

Ilustración 15: Matriz de relación Procesos y activos. Autor: Desarrollador de Tesis.

4.3.1.1. Escalas para determinar el valor de los activos de información

Para valorar los activos se realizó una combinación de escalas tanto cualitativamente como cuantitativamente que a continuación se visualizara en tablas: En la escala cuantitativa, se utilizan valores numéricos, esto ayuda a realizar análisis económicos comparando lo que se

está arriesgando con lo que cuesta la solución por otra parte se tiene la escala cualitativa en donde se utiliza una escala de condiciones para describir la magnitud de las posibles consecuencias y la probabilidad de que estas consecuencias se produzcan. En la tabla #8 se observa una escala detallada de diez valores en donde el valor 0 se considera como un valor despreciable (a efectos de riesgo) y 10 será considerado como valor extremo.

Establecida la escala de valor se procede a la calificación de los activos en base a las distintas dimensiones posteriormente se obtendrá el valor del activo critico aplicando la siguiente ecuación: Valor de activo = autenticidad +confidencialidad +integridad +disponibilidad + trazabilidad

CARACTERIZACIÓN	CODIGO ACTIVO	DENOMINACION	AUTENTICIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	TOTAL
[D] Datos / Información	Ac-Sis-001	Red de Datos	10	10	9	10	9	48
[essential] Activos esenciales	Ac-Sis-002	Documentacion de informacion	8	10	9	10	8	45
[SW] Software - Aplicaciones informáticas	Ac-Sis-004	Sistemas informaticos	10	10	10	10	10	50
[P] Personal	Ac-Sis-005	Equipo Técnico y Soporte	8	10	8	10	5	41
[COM] Redes de comunicaciones	Ac-Sis-006	Servidor Proxy	9	10	9	10	10	48
	Ac-Sis-007	Transmisor Optico ODF	7	5	5	8	5	30
	Ac-Sis-009	Antena Sectorial 19 dbi 120g	8	9	8	10	5	40
	Ac-Sis-010	Antena mimosa Al B5c para punto a punto	7	5	8	9	5	34
[HW]Equipamiento informatico (hardware)	Ac-Sis-011	RBLHG-5nD(Para Clientes)	10	10	7	10	5	42
	Ac-Sis-012	OLT ZTE de 34 puertos	8	5	6	10	5	34
	Ac-Sis-013	Router principal Backup (Cañar)	10	9	9	10	10	48
	Ac-Sis-014	Swich 12 puertos	9	9	9	10	5	42
	Ac-Sis-015	Router Honorato Vasquez	10	10	10	10	8	48
	Ac-Sis-016	Router Pilcopata	10	10	10	10	8	48
	Ac-Sis-017	Router Altarhurco	10	10	10	10	8	48
	Ac-Sis-018	Router Hueran	10	10	10	10	8	48
	Ac-Sis-019	Equipo de monitoreo	9	10	10	10	10	49

Ilustración 16: Inventario de activos y valoración. Fuente: Desarrollador de tesis.

4.3.2. Identificación y clasificación de las amenazas según la metodología MAGERIT versión 3.0

Una vez realizado la calificación de los activos se procede a la identificación de las posibles amenazas que podrían presentarse en el activo.

De la misma manera las amenazas proceden del Libro II de Magerit v3.0 y a continuación se detallan las mismas.

Tabla 10: Matriz de Activos y Amenazas Autor: Diseñador de Tesis.

Código	Activo	Código Amenaza	Amenaza	Probabilidad de ocurrencia	Degradación (% o nivel)				
					A	C	I	D	T
Ac-Sis-001	Red de Datos	[I.5]	Avería de origen físico o lógico	MB				M	
		[I.6]	Corte del suministro eléctrico	B				M	
		[I.8]	Fallo de servicios de comunicaciones	A				A	
		[I.9]	Interrupción de otros servicios y suministros esenciales	M				A	
		[E.1]	Errores de los usuarios	M		B	B	M	
		[E.2]	Errores del administrador	B		M	B	M	
		[E.3]	Errores de monitorización (log)	MB			M		
		[E.4]	Errores de configuración	MB			M		
		[E.8]	Difusión de software dañino	M		A	M	M	
		[E.10]	Errores de secuencia	MB			M		
		[E.14]	Escapes de información	A		A			
		[E.15]	Alteración accidental de la información	M			M		
		[E.19]	Fugas de información	M		A			
		[E.20]	Vulnerabilidades de los programas (software)	M		M	M	M	
		[E.21]	Errores de mantenimiento / actualización de programas (software)	MB			B	B	

		[E.24]	Caída del sistema por agotamiento de recursos	MB			MB
		[A.4]	Manipulación de la configuración	B	B	B	B
		[A.7]	Uso no previsto	MB	B	B	
		[A.11]	Acceso no autorizado	MB	MB	B	B
		[A.18]	Destrucción de información	MB			M
		[A.24]	Denegación de servicio	M			M
Ac-Sis-004	Sistemas informaticos	[I.5]	Avería de origen físico o lógico	A			MB
		[I.6]	Corte del suministro eléctrico	A			M
		[I.7]	Condiciones inadecuadas de temperatura o humedad	MB			M
		[I.8]	Fallo de servicios de comunicaciones	A			M
		[I.9]	Interrupción de otros servicios y suministros esenciales	A			M
		[E.1]	Errores de los usuarios	A	B	B	B
		[E.2]	Errores del administrador	A	B	B	B
		[E.4]	Errores de configuración	MB		MB	
		[E.8]	Difusión de software dañino	B	M	M	B
		[E.14]	Escapes de información	MB	A		
		[E.15]	Alteración accidental de la información	MB		B	
		[E.18]	Destrucción de información	B			M
		[E.19]	Fugas de información	MB	M		

		[E.20]	Vulnerabilidades de los programas (software)	MB	A	B	M	
		[E.21]	Errores de mantenimiento / actualización de programas (software)	B		B	MB	
		[E.24]	Caída del sistema por agotamiento de recursos	M			M	
		[A.23]	Manipulación de los equipos	M	B		B	
		[A.24]	Denegación de servicio	B			M	
Ac-Sis-006	Servidor Proxy	[N.1]	Fuego	B			A	
		[N.2]	Daños por agua	B			B	
		[I.1]	Fuego	MB			B	
		[I.2]	Daños por agua	MB			B	
		[I.5]	Avería de origen físico o lógico	M			M	
		[I.6]	Corte del suministro eléctrico	B			A	
		[I.8]	Fallo de servicios de comunicaciones	MB			A	
		[E.1]	Errores de los usuarios	MB	B	B	B	
		[E.2]	Errores del administrador	M	M	M	MB	
		[E.3]	Errores de monitorización (log)	MB		B		B
		[E.4]	Errores de configuración	B			M	
		[E.8]	Difusión de software dañino	MB	M	M	B	
		[E.10]	Errores de secuencia	M			MB	
		[E.14]	Escapes de información	M	M			

		[E.15]	Alteración accidental de la información	A		B	
		[E.18]	Destrucción de información	B			M
		[E.20]	Vulnerabilidades de los programas (software)	MB	A	B	M
		[E.24]	Caída del sistema por agotamiento de recursos	MB			A
		[A.4]	Manipulación de la configuración	B	M	MB	M
		[A.8]	Difusión de software dañino	B	M	M	M
		[A.10]	Alteración de secuencia	MB		M	
		[A.12]	Análisis de tráfico	MB	A		
		[A.15]	Modificación deliberada de la información	MB		MB	
		[A.18]	Destrucción de información	B			MB
		[A.22]	Manipulación de programas	M	M	A	A
		[A.24]	Denegación de servicio	MB			A
Ac-Sis-013	Router principal Backup (Cañar)	[N.1]	Fuego	M			M
		[N.2]	Daños por agua	M			M
		[I.5]	Avería de origen físico o lógico	M			A
		[I.6]	Corte del suministro eléctrico	A			A
		[I.8]	Fallo de servicios de comunicaciones	A			A

		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	A		A	M
		[E.25]	Pérdida de equipos	M	M		A
		[A.23]	Manipulación de los equipos	M	MB		A
		[A.24]	Denegación de servicio	A			A
		[A.26]	Ataque destructivo	M			M
Ac-Sis-015	Router Honorato Vasquez	[N.1]	Fuego	M			M
		[N.2]	Daños por agua	M			M
		[I.5]	Avería de origen físico o lógico	M			A
		[I.6]	Corte del suministro eléctrico	A			A
		[I.8]	Fallo de servicios de comunicaciones	A			A
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	A		A	M
		[E.25]	Pérdida de equipos	M	M		A
		[A.23]	Manipulación de los equipos	M	MB		A
		[A.24]	Denegación de servicio	A			A
		[A.26]	Ataque destructivo	M			M
Ac-Sis-016	Router Pilcopata	[N.1]	Fuego	M			M
		[N.2]	Daños por agua	M			M
		[I.5]	Avería de origen físico o lógico	M			A
		[I.6]	Corte del suministro eléctrico	A			A

		[I.8]	Fallo de servicios de comunicaciones	A			A
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	A		A	M
		[E.25]	Pérdida de equipos	M	M		A
		[A.23]	Manipulación de los equipos	M	MB		A
		[A.24]	Denegación de servicio	A			A
		[A.26]	Ataque destructivo	M			M
Ac-Sis-017	Router Altarhurco	[N.1]	Fuego	M			M
		[N.2]	Daños por agua	M			M
		[I.5]	Avería de origen físico o lógico	M			A
		[I.6]	Corte del suministro eléctrico	A			A
		[I.8]	Fallo de servicios de comunicaciones	A			A
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	A		A	M
		[E.25]	Pérdida de equipos	M	M		A
		[A.23]	Manipulación de los equipos	M	MB		A
		[A.24]	Denegación de servicio	A			A
		[A.26]	Ataque destructivo	M			M
Ac-Sis-018	Router Hueran	[N.1]	Fuego	M			M
		[N.2]	Daños por agua	M			M

		[I.5]	Avería de origen físico o lógico	M			A
		[I.6]	Corte del suministro eléctrico	A			A
		[I.8]	Fallo de servicios de comunicaciones	A			A
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	A		A	M
		[E.25]	Pérdida de equipos	M	M		A
		[A.23]	Manipulación de los equipos	M	MB		A
		[A.24]	Denegación de servicio	A			A
		[A.26]	Ataque destructivo	M			M
Ac-Sis-019	Equipo de monitoreo	[N.1]	Fuego	M			M
		[N.2]	Daños por agua	B			M
		[I.5]	Avería de origen físico o lógico	M			A
		[I.6]	Corte del suministro eléctrico	A			A
		[I.8]	Fallo de servicios de comunicaciones	A			A
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	A		A	M
		[E.25]	Pérdida de equipos	A	M		A
		[A.23]	Manipulación de los equipos	A	M		M
		[A.24]	Denegación de servicio	A			A
		[A.26]	Ataque destructivo	A			A

4.3.3. Análisis de riesgo y amenazas

Luego de identificar y calificar las amenazas con sus respectivos activos se procedió a la valoración de los mismos en base a la probabilidad de que ocurra esa amenaza el nivel de impacto que surge y el nivel del riesgo que llegara a tener si esa amenaza se materializa. Para la calificación se basó en los valores de las tablas que a continuación se detalla:

Probabilidad: hace referencia a cuan probable o improbable es que se plasme la amenaza, estos pueden ser medidos con criterios de frecuencia y factibilidad.

Tabla 11: Matriz de probabilidad. Autor: Desarrollador de tesis

Probabilidad	Frecuencia	Valor
Casi seguro	Más de una vez al año	5
Probable	Al menos una vez el último año.	4
Posible	Al menos una vez en los últimos dos años	3
Improbable	Al menos una vez en los últimos cinco años.	2
Raro	No se ha presentado en los últimos cinco años.	1

Impacto: son las consecuencias que podría ocasionar a la empresa al materializarse el riesgo.

Tabla 12: Matriz de impacto. Autor: Desarrollador de tesis

Impacto	Descripción	Valor
Catastrófico	Si se llegara a presentar tendría, desastrosas consecuencias que podrían terminar con la organización: • Pérdida de recursos secundarios. • Perdida de información interna no publicada. • Suspensión de los sistemas críticos • Perdida de información confidencial estratégica • Deterioro de la imagen institucional.	5
Mayor	Si se presenta tendría altas consecuencias o efectos sobre la empresa. Investigaciones • Sanciones • Demandas	4
Moderado	Si se presentara tendría medianas consecuencias sobre la empresa.	3
Menor	Al presentarse tendría consecuencias mínimas sobre la empresa.	2
Insignificante	Al presentarse tendría consecuencias mínimas sobre la empresa. • Perdida de elementos críticos pero que cuentan con respaldos. • Caída notable del rendimiento del proceso del negocio. • Perdida de información confidencial pero no considerada estratégica. Suspensión temporal del servicio.	1

Tabla 13: Análisis de riesgo Autor: Desarrollador de la tesis. Fuente análisis realizada a la empresa proveedora de internet Cañar Net.

ACTIVO	CÓDIGO AMENAZA	AMENAZA	PROBABILIDAD DE OCURRENCIA	IMPACTO	RIESGO
Red de Datos	[I.5]	Avería de origen físico o lógico	1	3	Bajo
	[I.6]	Corte del suministro eléctrico	2	3	Medio
	[I.8]	Fallo de servicios de comunicaciones	4	3	Alto
	[I.9]	Interrupción de otros servicios y suministros esenciales	3	2	Medio
	[E.1]	Errores de los usuarios	3	1	Bajo
	[E.2]	Errores del administrador	2	1	Bajo
	[E.3]	Errores de monitorización (log)	1	1	Bajo
	[E.4]	Errores de configuración	1	3	Bajo
	[E.8]	Difusión de software dañino	3	3	Medio
	[E.10]	Errores de secuencia	1	1	Bajo
	[E.14]	Escapes de información	4	3	Alto
	[E.15]	Alteración accidental de la información	3	3	Medio
	[E.19]	Fugas de información	3	2	Medio
	[E.20]	Vulnerabilidades de los programas (software)	3	3	Medio
	[E.21]	Errores de mantenimiento / actualización de programas (software)	1	3	Bajo
	[E.24]	Caída del sistema por agotamiento de recursos	1	3	Bajo
	[A.4]	Manipulación de la configuración	2	1	Bajo
	[A.7]	Uso no previsto	1	1	Bajo
	[A.11]	Acceso no autorizado	1	1	Bajo
	[A.18]	Destrucción de información	1	3	Bajo
	[A.24]	Denegación de servicio	3	2	Bajo
	[I.5]	Avería de origen físico o lógico	4	1	Bajo

Sistemas informaticos	[I.6]	Corte del suministro eléctrico	4	2	Medio
	[I.7]	Condiciones inadecuadas de temperatura o humedad	1	1	Bajo
	[I.8]	Fallo de servicios de comunicaciones	4	3	Alto
	[I.9]	Interrupción de otros servicios y suministros esenciales	4	3	Alto
	[E.1]	Errores de los usuarios	4	1	Bajo
	[E.2]	Errores del administrador	4	1	Bajo
	[E.4]	Errores de configuración	1	1	Bajo
	[E.8]	Difusión de software dañino	2	3	Medio
	[E.14]	Escapes de información	1	3	Bajo
	[E.15]	Alteración accidental de la información	1	3	Bajo
	[E.18]	Destrucción de información	2	4	Medio
	[E.19]	Fugas de información	1	4	Bajo
	[E.20]	Vulnerabilidades de los programas (software)	1	4	Bajo
	[E.21]	Errores de mantenimiento / actualización de programas (software)	2	4	Medio
	[E.24]	Caída del sistema por agotamiento de recursos	3	3	Medio
	[A.23]	Manipulación de los equipos	3	3	Medio
	[A.24]	Denegación de servicio	2	3	Medio
Servidor Proxy	[N.1]	Fuego	2	3	Medio
	[N.2]	Daños por agua	2	3	Medio
	[I.1]	Fuego	1	3	Bajo
	[I.2]	Daños por agua	1	3	Bajo
	[I.5]	Avería de origen físico o lógico	3	1	Bajo
	[I.6]	Corte del suministro eléctrico	2	3	Medio
	[I.8]	Fallo de servicios de comunicaciones	1	3	Bajo
	[E.1]	Errores de los usuarios	1	3	Bajo
	[E.2]	Errores del administrador	3	1	Bajo
	[E.3]	Errores de monitorización (log)	1	1	Bajo

	[E.4]	Errores de configuración	2	1	Bajo
	[E.8]	Difusión de software dañino	1	3	Bajo
	[E.10]	Errores de secuencia	3	1	Bajo
	[E.14]	Escapes de información	3	3	Medio
	[E.15]	Alteración accidental de la información	4	2	Medio
	[E.18]	Destrucción de información	2	4	Medio
	[E.20]	Vulnerabilidades de los programas (software)	1	3	Bajo
	[E.24]	Caída del sistema por agotamiento de recursos	1	2	Bajo
	[A.4]	Manipulación de la configuración	2	1	Bajo
	[A.8]	Difusión de software dañino	2	3	Medio
	[A.10]	Alteración de secuencia	1	1	Bajo
	[A.12]	Análisis de tráfico	1	1	Bajo
	[A.15]	Modificación deliberada de la información	1	2	Bajo
	[A.18]	Destrucción de información	2	3	Medio
	[A.22]	Manipulación de programas	3	4	Alto
	[A.24]	Denegación de servicio	1	3	Bajo
Router principal Backup (Cañar)	[N.1]	Fuego	3	3	Medio
	[N.2]	Daños por agua	3	3	Medio
	[I.5]	Avería de origen físico o lógico	3	2	Medio
	[I.6]	Corte del suministro eléctrico	4	3	Alto
	[I.8]	Fallo de servicios de comunicaciones	4	3	Alto
	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	3	Alto
	[E.25]	Pérdida de equipos	3	3	Medio
	[A.23]	Manipulación de los equipos	3	2	Medio
	[A.24]	Denegación de servicio	4	1	Bajo
	[A.26]	Ataque destructivo	3	1	Bajo
	[N.1]	Fuego	3	3	Medio

Router Honorato Vasquez	[N.2]	Daños por agua	3	3	Medio
	[I.5]	Avería de origen físico o lógico	3	3	Medio
	[I.6]	Corte del suministro eléctrico	4	3	Alto
	[I.8]	Fallo de servicios de comunicaciones	4	3	Alto
	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	3	Alto
	[E.25]	Pérdida de equipos	3	1	Bajo
	[A.23]	Manipulación de los equipos	3	1	Bajo
	[A.24]	Denegación de servicio	4	4	Alto
	[A.26]	Ataque destructivo	3	3	Medio
Router Pilcopata	[N.1]	Fuego	3	3	Medio
	[N.2]	Daños por agua	3	3	Medio
	[I.5]	Avería de origen físico o lógico	3	3	Medio
	[I.6]	Corte del suministro eléctrico	4	3	Alto
	[I.8]	Fallo de servicios de comunicaciones	4	3	Alto
	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	2	Medio
	[E.25]	Pérdida de equipos	3	2	Medio
	[A.23]	Manipulación de los equipos	3	1	Bajo
	[A.24]	Denegación de servicio	4	3	Alto
	[A.26]	Ataque destructivo	3	3	Medio
Router Altarhurco	[N.1]	Fuego	3	3	Medio
	[N.2]	Daños por agua	3	3	Medio
	[I.5]	Avería de origen físico o lógico	3	3	Medio
	[I.6]	Corte del suministro eléctrico	4	3	Alto
	[I.8]	Fallo de servicios de comunicaciones	4	3	Alto
	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	2	Medio
	[E.25]	Pérdida de equipos	3	2	Medio
	[A.23]	Manipulación de los equipos	3	1	Bajo

	[A.24]	Denegación de servicio	4	3	Alto
	[A.26]	Ataque destructivo	3	3	Medio
Router Hueran	[N.1]	Fuego	3	3	Medio
	[N.2]	Daños por agua	3	3	Medio
	[I.5]	Avería de origen físico o lógico	3	3	Medio
	[I.6]	Corte del suministro eléctrico	4	3	Alto
	[I.8]	Fallo de servicios de comunicaciones	4	3	Alto
	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	2	Medio
	[E.25]	Pérdida de equipos	3	2	Medio
	[A.23]	Manipulación de los equipos	3	1	Bajo
	[A.24]	Denegación de servicio	4	3	Alto
	[A.26]	Ataque destructivo	3	3	Medio
Equipo de monitoreo	[N.1]	Fuego	3	3	Medio
	[N.2]	Daños por agua	2	3	Medio
	[I.5]	Avería de origen físico o lógico	3	3	Medio
	[I.6]	Corte del suministro eléctrico	4	3	Alto
	[I.8]	Fallo de servicios de comunicaciones	4	3	Alto
	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	2	Medio
	[E.25]	Pérdida de equipos	4	2	Medio
	[A.23]	Manipulación de los equipos	4	1	Bajo
	[A.24]	Denegación de servicio	4	3	Alto
	[A.26]	Ataque destructivo	4	3	Alto

4.3.4. Salvaguardas y Contramedidas

En la siguiente tabla se determina las salvaguardas que brinda MAGERIT para cada uno de los activos y las diferentes amenazas que podrían surgir en algún momento dentro o fuera de la organización, esto se lo hace con el objetivo de brindar controles en caso de presentarse daños y se pueda actuar de la forma más inmediata de esta manera evitaremos que la empresa Cañar Net detenga sus actividades.

Tabla 14: Matriz de amenazas y salvaguardas.

Código	Activo	Código Amenaza	Amenaza	Nivel de Amenaza	Salvaguarda
Ac-Sis-001	Red de Datos	[I.6]	Corte del suministro eléctrico	Medio	HW. A Aseguramiento de la disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Alto	COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
		[I.9]	Interrupción de otros servicios y suministros esenciales	Medio	AUX.A Aseguramiento de la disponibilidad
		[E.8]	Difusión de software dañino	Medio	SW Protección de las Aplicaciones Informáticas SW.CM Cambios (actualizaciones y mantenimiento)
		[E.14]	Escapes de información	Alto	SW Protección de las Aplicaciones Informáticas SW Protección de las Aplicaciones Informáticas
		[E.15]	Alteración accidental de la información	Medio	D Protección de la Información H.tools Herramientas de seguridad
		[E.19]	Fugas de información	Medio	D Protección de la Información D.C Cifrado de la información

		[E.20]	Vulnerabilidades de los programas (software)	Medio	SW Protección de las Aplicaciones Informáticas
Ac-Sis-004	Sistemas informáticos	[I.6]	Corte del suministro eléctrico	Medio	HW.A Aseguramiento de la disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Alto	COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
		[I.9]	Interrupción de otros servicios y suministros esenciales	Alto	AUX.A Aseguramiento de la disponibilidad
		[E.8]	Difusión de software dañino	Medio	SW Protección de las Aplicaciones Informáticas SW.CM Cambios (actualizaciones y mantenimiento)
		[E.18]	Destrucción de información	Medio	MP. A Aseguramiento de la disponibilidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Medio	SW Protección de las Aplicaciones Informáticas SW.CM Cambios (actualizaciones y mantenimiento)
		[E.24]	Caída del sistema por agotamiento de recursos	Medio	HW Protección de los Equipos Informáticos HW. A Aseguramiento de la disponibilidad HW.CM Cambios

					(actualizaciones y mantenimiento) S Protección de los Servicios
		[A.23]	Manipulación de los equipos	Medio	HW Protección de los Equipos Informáticos HW.CM Cambios (actualizaciones y mantenimiento)
		[A.24]	Denegación de servicio		S. A Aseguramiento de la disponibilidad
				Medio	S.CM Gestión de cambios (mejoras y sustituciones)
					S.www Protección de servicios y aplicaciones web
Ac-Sis-006	Servidor Proxy	[N.1]	Fuego		disponer de extintores de fuego HW Protección de los Equipos Informáticos
				Medio	AUX.wires Protección del cableado
		[N.2]	Daños por agua	Medio	HW Protección de los Equipos Informáticos

[I.6]	Corte del suministro eléctrico	Medio	HW Protección de los Equipos Informáticos disponer de un generador de energía eléctrica
[E.14]	Escapes de información	Medio	SW Protección de las Aplicaciones Informáticas SW.SC Se aplican perfiles de seguridad
[E.15]	Alteración accidental de la información	Medio	SW Protección de las Aplicaciones Informáticas SW.SC Se aplican perfiles de seguridad SW. A Copias de seguridad (backup)
[E.18]	Destrucción de información	Medio	MP Protección de los Soportes de Información MP.A Aseguramiento de la disponibilidad MP.IC Protección criptográfica del contenido
[A.8]	Difusión de software dañino	Medio	MP.IC Protección criptográfica del contenido COM.A Aseguramiento de la disponibilidad
[A.18]	Destrucción de información	Medio	MP Protección de los Soportes de Información

					MP. A Aseguramiento de la disponibilidad MP.IC Protección criptográfica del contenido
		[A.22]	Manipulación de programas	Alto	COM.SC Se aplican perfiles de seguridad SW Protección de las Aplicaciones Informáticas SW.SC Se aplican perfiles de seguridad
Ac-Sis-013	Router principal Backup (Cañar)	[N.1]	Fuego	Medio	disponer de extintores de fuego HW Protección de los Equipos Informáticos AUX.wires Protección del cableado
		[N.2]	Daños por agua	Medio	HW Protección de los Equipos Informáticos
		[I.5]	Avería de origen físico o lógico	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio
		[I.6]	Corte del suministro eléctrico	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico

		[I.8]	Fallo de servicios de comunicaciones	Alto	AUX.A Aseguramiento de la disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Alto	AUX.wires Protección del cableado COM.CM Cambios (actualizaciones y mantenimiento)
		[E.25]	Pérdida de equipos	Medio	HW.SC Se aplican perfiles de seguridad HW. A Aseguramiento de la disponibilidad
		[A.23]	Manipulación de los equipos	Medio	D.I Aseguramiento de la integridad
Ac-Sis-015	Router Honorato Vasquez	[N.1]	Fuego	Medio	Disponer de un extintor
		[N.2]	Daños por agua	Medio	S.A Aseguramiento de la disponibilidad
		[I.5]	Avería de origen físico o lógico	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio
		[I.6]	Corte del suministro eléctrico	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad

			AUX.power Suministro eléctrico
[I.8]	Fallo de servicios de comunicaciones	Alto	COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Alto	HW Protección de los Equipos Informáticos HW. A Aseguramiento de la disponibilidad
[A.24]	Denegación de servicio	Alto	S. A Aseguramiento de la disponibilidad S.SC Se aplican perfiles de seguridad
[A.26]	Ataque destructivo	Medio	H Protecciones Generales H. IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de incidencias H.tools Herramientas de seguridad

					H.tools.AV Herramienta contra código dañino H.tools.SFV Verificación de las funciones de seguridad
Ac-Sis-016	Router Pilcopata	[N.1]	Fuego	Medio	Disponer de un extintor
		[N.2]	Daños por agua	Medio	S.A Aseguramiento de la disponibilidad
		[I.5]	Avería de origen físico o lógico	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio
		[I.6]	Corte del suministro eléctrico	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico
		[I.8]	Fallo de servicios de comunicaciones	Alto	COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones

	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Medio	HW Protección de los Equipos Informáticos HW. A Aseguramiento de la disponibilidad
	[E.25]	Pérdida de equipos	Medio	HW.SC Se aplican perfiles de seguridad HW. A Aseguramiento de la disponibilidad
	[A.24]	Denegación de servicio	Alto	S.A Aseguramiento de la disponibilidad S.SC Se aplican perfiles de seguridad
	[A.26]	Ataque destructivo	Medio	H Protecciones Generales H. IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.SFV Verificación de las funciones de seguridad

Ac-Sis-017	Router Altarhurco	[N.1]	Fuego	Medio	Disponer de un extintor
		[N.2]	Daños por agua	Medio	S.A Aseguramiento de la disponibilidad
		[I.5]	Avería de origen físico o lógico	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio
		[I.6]	Corte del suministro eléctrico	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico
		[I.8]	Fallo de servicios de comunicaciones	Alto	COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Medio	HW Protección de los Equipos Informáticos HW. A Aseguramiento de la disponibilidad
		[E.25]	Pérdida de equipos	Medio	HW.SC Se aplican perfiles de seguridad

					HW. A Aseguramiento de la disponibilidad
		[A.24]	Denegación de servicio	Alto	S.A Aseguramiento de la disponibilidad S.SC Se aplican perfiles de seguridad
		[A.26]	Ataque destructivo		H Protecciones Generales H. IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.SFV Verificación de las funciones de seguridad
Ac-Sis-018	Router Hueran	[N.1]	Fuego	Medio	Disponer de un extintor
		[N.2]	Daños por agua	Medio	S.A Aseguramiento de la disponibilidad

	[I.5]	Avería de origen físico o lógico	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio
	[I.6]	Corte del suministro eléctrico	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico
	[I.8]	Fallo de servicios de comunicaciones	Alto	COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Medio	HW Protección de los Equipos Informáticos HW. A Aseguramiento de la disponibilidad
	[E.25]	Pérdida de equipos	Medio	HW.SC Se aplican perfiles de seguridad

					HW. A Aseguramiento de la disponibilidad
		[A.24]	Denegación de servicio	Alto	S. A Aseguramiento de la disponibilidad S.SC Se aplican perfiles de seguridad
		[A.26]	Ataque destructivo		H Protecciones Generales H.IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.SFV Verificación de las funciones de seguridad
Ac-Sis-019	Equipo de monitoreo	[N.1]	Fuego	Medio	Disponer de un extintor
		[N.2]	Daños por agua	Medio	S.A Aseguramiento de la disponibilidad

	[I.5]	Avería de origen físico o lógico	L.AC Control de los accesos físicos
		Medio	L.A Aseguramiento de la disponibilidad
			BC Continuidad del negocio
	[I.6]	Corte del suministro eléctrico	BC Continuidad del negocio
		Alto	AUX.A Aseguramiento de la disponibilidad
			AUX.power Suministro eléctrico
	[I.8]	Fallo de servicios de comunicaciones	COM.SC Se aplican perfiles de seguridad
		Alto	COM.A Aseguramiento de la disponibilidad
			COM Protección de las Comunicaciones
	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	HW Protección de los Equipos Informáticos
		Medio	HW. A Aseguramiento de la disponibilidad
	[E.25]	Pérdida de equipos	HW.SC Se aplican perfiles de seguridad
		Medio	

			HW. A Aseguramiento de la disponibilidad
[A.24]	Denegación de servicio	Alto	S.A Aseguramiento de la disponibilidad S.SC Se aplican perfiles de seguridad
[A.26]	Ataque destructivo	Alto	H Protecciones Generales H. IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.SFV Verificación de las funciones de seguridad

Luego de haber realizado la calificación de los procesos y subprocesos, activos, la calificación e identificación de las amenazas y finalmente la identificación de las posibles salvaguardas, se obtuvo una matriz con los procesos críticos el mismo que sirvió como base fundamental para el diseño de estrategias para la empresa Cañar Net y se procede con la continuación de las fases de un Plan de Continuidad de Negocios. Se diseñaron estrategias de recuperación tecnológica que pueda satisfacer las necesidades de mitigación del riesgo. También se incluye el tiempo de recuperación Objetivo (RTO) y punto de Recuperación Objetivo (RPO) para los procesos.

Tabla 15: Matriz de RTO y RPO para el proceso critico de Gestión de servicio al cliente. ***Autor:*** *Desarrollador de la tesis.*

Proceso	Subproceso	Responsable	Tiempo máximo de recuperación (RTO)	Tiempo máximo de obtención de respaldos (RPO)
Gestión de servicio al cliente	Gestión de incidentes	Responsable de atención y servicio al cliente.	1 hora	30 minutos

Tabla 16: Matriz de RTO y RPO para el proceso critico de Desarrollo de servicios y operaciones. Autor: Desarrollador de la tesis.

Proceso	Subproceso	Responsable	Tiempo máximo de recuperación (RTO)	Tiempo máximo de obtención de respaldos (RPO)
Desarrollo de servicio y operaciones	Gestión de incidentes en el servicio	Gerente general. Técnicos de soporte y mantenimiento de equipos.	24 horas	2 horas
	Gestión de la calidad del servicio	Gerente general.	24 horas	2 horas

		Técnicos de soporte y mantenimiento de equipos.		

Tabla 17: Matriz de RTO y RPO para el proceso critico de Gestión de sistemas y redes. Autor: Desarrollador de la tesis.

Proceso	**Subproceso**	**Responsable**	**Tiempo máximo de recuperación (RTO)**	**Tiempo máximo de obtención de respaldos (RPO)**
Gestión de sistemas y redes	Mantenimiento y restauración de redes	Técnicos de soporte y mantenimiento de equipos.	1 hora	30 minutos

Tabla 18: Matriz de RTO y RPO para el proceso critico de Redes físicas y tecnología de la información. Autor: Desarrollador de la tesis.

Proceso	**Subproceso**	**Responsable**	**Tiempo máximo de recuperación (RTO)**	**Tiempo máximo de obtención de respaldos (RPO)**
Redes físicas y tecnología de la información	Gestión de tecnologías de la información y seguridad informática	Gerente general Encargado del área de TI.	1 hora	30 minutos

4.3.5. DEFINIR LAS ESTRATEGIAS PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

A continuación, se definen las estrategias de mitigación de riesgos para los procesos y subprocesos en base a la matriz realizada del análisis de riesgo de esta manera determinaremos como se logrará la continuidad y recuperación de incidentes. Para el diseño de las estrategias se consideró los tiempos objetivos de recuperación antes definido.

Tabla 19: Estrategias para procesos críticos de Gestión de servicio al cliente Autor: Desarrollador de la tesis.

Proceso	Subproceso	Estrategia Requerida	Tiempo máximo de recuperación (RTO)
Gestión de servicio al cliente	Gestión de incidentes	- Creación de una mesa de servicios de gestión de incidentes nivel 1. Esta estrategia servirá para dar solución a los problemas más comunes que puede ocurrir en el entorno de la empresa Cañar Net.	1 hora

Tabla 20: Estrategias para procesos críticos de Desarrollo de servicio y operaciones. Autor: Desarrollador de la tesis.

Proceso	Subproceso	Estrategia Requerida	Tiempo máximo de recuperación (RTO)
Desarrollo de servicio y operaciones	Gestión de incidentes en el servicio	Seguir los procesos establecidos entro del departamento de TI. Para mejorar y garantizar los servicios prestados a sus clientes.	24 horas
	Gestión de la calidad del servicio	Establecer una mejora continua del servicio en la que se revisen y mejoren los procedimientos, políticas, roles, tecnología y otros aspectos del proceso de gestión de incidentes.	24 horas

Tabla 21: Estrategias para procesos críticos de Gestión de sistemas y redes. Autor: Desarrollador de la tesis.

Proceso	Subproceso	Estrategia Requerida	Tiempo máximo de recuperación (RTO)
Gestión de sistemas y redes	Mantenimiento y restauración de redes	Plan de aseguramiento, capacidad y disponibilidad de la infraestructura tecnológica (instalación, configuración y administración de hardware, bases de datos, repositorios, entre otros recursos tecnológicos) con la que cuenta la institución.	1 hora

Tabla 22: Estrategias para procesos críticos de Redes físicas y tecnología de la información. Autor: Desarrollador de la tesis.

Proceso	Subproceso	Estrategia Requerida	Tiempo máximo de recuperación (RTO)
Redes físicas y tecnología de la información	Gestión de tecnologías de la información y seguridad informática	-Plan de aseguramiento, capacidad y disponibilidad de la infraestructura tecnológica (instalación, configuración y administración de hardware, bases de datos, repositorios, entre otros recursos tecnológicos) con la que cuenta la institución. -Disponer con un generador de energía para la matriz de la cooperativa. -Contar con un Manual de permisos de usuario. -Disponer con más personal en el departamento de sistemas. -Disponer de extintores y cámaras de niebla.	1 hora

	-Plan de mantenimiento preventivo y correctivo de hardware y software de la Infraestructura Tecnológica. -Políticas de procedimiento de seguridad

4.4 CONCLUSIONES Y RECOMENDACIONES

4.4.1 CONCLUSIONES

- Como resultado del presente trabajo de plan de continuidad de negocio desarrollado en la empresa proveedora de internet Cañar Net, se realizó un análisis para la determinación de los procesos más críticos entre los cuales destacan: la gestión de incidentes, gestión de incidentes en el servicio, mantenimiento y restauración de redes entre otras y todos estos están solventados sobre los procesos del departamento de TI, también se realizó un análisis y gestión de riesgos de los procesos determinando las amenazas y riesgos que presenta la misma, y en base a eso se obtuvo el documento de estrategias a seguir ante la presencia de un incidente.
- Para la determinación de las normas y metodologías de un plan de continuidad de negocio y el análisis y gestión de riesgos se realizó una tabla comparativa de las normas existentes para el diseño del BCP de la misma manera se lo realizo para la metodología del análisis y gestión de riesgos, el cual dio como resultado la Norma ISO 22301 para el diseño de un BCP y de la misma manera se seleccionó la metodología Magerit para el análisis y gestión de riesgo.
- Las políticas de continuidad de negocio establecidas para la empresa Cañar Net se plantearon en base a un análisis de riesgo de los diferentes proceso, activos y calificación de las mismas, obteniendo un nivel de riesgo tolerable, con el fin de proteger la continuidad de sus actividades, sus intereses y la de los usuarios.

4.4.2 RECOMENDACIONES

- Que tomen como referencia el trabajo realizado por mi persona ya que está basado en la Norma Internacional ISO 22301 esta norma brinda los requisitos necesarios con los que debe contar la organización para asegurar la continuidad de sus procesos ante la presencia de incidentes que afecten el normal funcionamiento de la empresa proveedora de internet, permitiendo de esta manera ser más eficientes y eficaces a la hora de brindar un servicio, mejora su imagen y credibilidad ante sus clientes.
- Comunicar y capacitar a todos los empleados de la empresa Cañar Net con el objetivo de que cuenten con un conocimiento básico de un Plan de Continuidad de Negocio y que participe activamente brindando ideas de cómo actuar ante situaciones o incidentes que se presenten dentro de la misma.

Se recomienda a la Universidad Católica de Cuenca extensión Cañar:

- Emprender capacitaciones en el área de Administración de TI, Auditoria Informática que permita a los estudiantes generar conocimiento en áreas Administrativas para que de esta manera puedan involucrarse en un mundo laboral.

4.5 REFERENCIA

Heredero, C. (2006). *Dirección y gestión de los sistemas de información en la empresa.* ESIC Editorial, 2006.

Caballero Gonzáles , C., & Clavero García, J. A. (2016). *Sistemas de almacenamiento.* Ediciones Paraninfo, S.A., 2016.

CERDA, W. O. (2013). *repositorio.puce.edu.ec.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/12656/Tesis_JacomeWilsonMGTI.pdf?sequence=1

Corrales, J. D. (2005). *Ayudantes tecnicos. Opcion informatica. Junta de andalucia. Temario volumen ii.* MAD-Eduforma, 2005.

Cruz, D., López de León, F., Pascual, L., & Battaglia, M. (2010). *Guía Técnica de producción de hongos comestibles de la especie de Hongos Ostra.*

GABRIELA, M. B. (01 de 01 de 2017). *docplayer.es.* Obtenido de docplayer.es: https://docplayer.es/85952413-Universidad-de-guayaquil-facultad-de-ingenieria-industrial.html

GARCÍA., F. Y. (MARZO de 2018). *UEES (UNIVERSIDAD ESPIRITU SANTO).* Obtenido de Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a Empresas Navieras.: http://201.159.223.2/bitstream/123456789/2763/1/HOLGUIN%20GARCIA%20FRESIA%20YANINA.pdf

Garreta, J. S. (2003). *Ingeniería de proyectos informáticos: actividades y procedimientos.* Publicacions de la Universitat Jaume I, 2003. Obtenido de https://books.google.com.ec/books?id=MXTI43ThoS4C&pg=PA81&dq=fases+del+riesgo+informatico&hl=es-419&sa=X&ved=0ahUKEwiy7tiUmI7lAhUi01kKHTfOBjEQ6AEIJzAA#v=onepage&q=fases%20del%20riesgo%20informatico&f=true

Gaspar Martínez, J. (2004). *Planes de contingencia: la continuidad del negocio en las organizaciones.* Ediciones Díaz de Santos, 2004.

Heredero , C. (2006). *Dirección y gestión de los sistemas de información en la empresa.* ESIC Editorial, 2006.

ISO. (2012). *www.iso.org.* Obtenido de www.iso.org: https://www.iso.org/obp/ui/es/#iso:std:iso:22301:ed-1:v2:en

ISO. (15 de marzo de 2018). *https:www.pmg-ssi.com*. Obtenido de https://www.pmg-ssi.com/2018/03/iso-22301-gestionar-continuidad-negocio/#:~:text=Un%20Sistema%20de%20Gesti%C3%B3n%20de%20Continuidad%20de%20Negocio%20certificado%20bajo,su%20impacto%20en%20la%20continuidad.

ISO. (s.f.). *www.isotools.org*. Obtenido de www.isotools.org: https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301

ISOtools. (4 de noviembre de 2015). *www.isotools.org*. Obtenido de www.isotools.org: https://www.isotools.org/2015/11/04/norma-iso-22301-requisitos-y-principales-beneficios/

isotools. (15 de octubre de 2018). *www.isotools.org*. Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000/

ISOTools Excellence. (15 de marzo de 2018). *www.pmg-ssi.com*. Obtenido de www.pmg-ssi.com: https://www.pmg-ssi.com/2018/03/iso-22301-gestionar-continuidad-negocio/

LossAd Parthners S.A.S. (01 de 01 de 2021). *http://lossad.com.co/*. Obtenido de http://lossad.com.co/: http://lossad.com.co/servicios-complementarios

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (2012). Madrid: © Ministerio de Hacienda y Administraciones Públicas .

Maldonado Mariño, D. C. (diciembre de 2013). *dspace.uniandes.edu.ec*. Obtenido de dspace.uniandes.edu.ec: http://dspace.uniandes.edu.ec/bitstream/123456789/4522/1/TUAMIE001-2013.pdf

Navarro, E. d. (2003). *Manual de outsourcing informático: (análisis y contratación)*. Ediciones Díaz de Santos, 2003.

Navarro, E. d., Ramos Gonzáles , M. A., Del Peso Ruiz , M., & Del Peso Ruiz , M. (2012). *Nuevo reglamento de protección de datos de carácter personal: Medidas de seguridad.* Díaz de Santos.

Nieto Muñoz, B. V. (abril de 2015). *dspace.ups.edu.ec*. Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/10303/1/UPS-GT001200.pdf

Numpaque Pineda, E. O. (s.f.). *repository.unipiloto.edu.co*. Obtenido de ANÁLISIS DE RIESGOS: PROCESO, REGULACIONES Y METODOLOGÍAS: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8653/An%c3%a1lisis%20de%20riesgos%20proceso%2c%20regulaciones%20ymetodologias.pdf?sequence=1&isAllowed=y

Quevedo, J. (2012). Revisión de modelos de gestión de continuidad del negocio. *REVISTA DE INVESTIGACIÓN DE SISTEMAS E INFORMÁTICA*, 91-111.

Rojas Bustamante , J. D. (2017). *UDLA.* Obtenido de http://dspace.udla.edu.ec/bitstream/33000/7531/1/UDLA-EC-TMGSTI-2017-08.pdf

SÁEZ VARGAS, V. A. (2013). *cybertesis.uach.c.* Obtenido de www.uach.cl: http://cybertesis.uach.cl/tesis/uach/2013/bpmfcis127m/doc/bpmfcis127m.pdf

School, E. B. (s.f.). *www.ealde.es/iso-31000.* Obtenido de https://www.ealde.es/iso-31000-para-que-sirve/

sigweb. (s.f). *www.sigweb.cl.* Obtenido de http://www.sigweb.cl/wp-content/uploads/biblioteca/MatrizdeRiesgo.pdf

Solarte Solarte , F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. C. (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*.

Tarazona T., C. H. (04 de 08 de 2007). *revistas.uexternado.edu.co.* Obtenido de https://revistas.uexternado.edu.co/index.php/derpen/article/view/965

Tejada, E. C. (2015). *Auditoría de seguridad informática. IFCT0109.* IC Editorial, 2015.

VARGAS, V. A. (s.f.). *cybertesis.uach.cl*. Obtenido de cybertesis.uach.cl: http://cybertesis.uach.cl/tesis/uach/2013/bpmfcis127m/doc/bpmfcis127m.pdf

Veiga, J. M. (2020). *Perito Judicial en Auditoria Informática.* José Manuel Ferro Veiga, 2020.

Vieites, Á. G. (2011). *Enciclopedia de la Seguridad Informática. 2ª edición.* Grupo Editorial RA-MA, 2011. Obtenido de https://books.google.es/books?id=Bq8-DwAAQBAJ&dq=gesti%C3%B3n+de+riesgos+en+seguridad+inform%C3%A1tica&lr=&hl=es&source=gbs_navlinks_s

Vieites, Á. G. (2011). *Enciclopedia de la Seguridad Informática. 2ª edición.* Grupo Editorial RA-MA, 2011.

Welivesecurity.com. (06 de 01 de 2014). *www.welivesecurity.com*. Obtenido de www.welivesecurity.com: https://www.welivesecurity.com/la-es/2014/01/06/iso-22301-2012-estandar-continuidad-negocio/

ANEXOS

4.6.1. ANEXO A: PROTOCOLO DE TESIS

<table>
<tr><td colspan="4">A. TÍTULO</td></tr>
<tr><td colspan="4">Diseño de un Plan De Continuidad de Negocio en la Empresa Cañar Net</td></tr>
<tr><td colspan="4">B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN</td></tr>
<tr><td rowspan="7">Tecnologías de Información y Comunicación</td><td rowspan="7">Ciencias exactas, naturales y tecnológicas</td><td>Analítica de Datos</td><td></td></tr>
<tr><td>Ingeniería de Software</td><td></td></tr>
<tr><td>Algoritmos computacionales</td><td></td></tr>
<tr><td>Inteligencia de negocios</td><td></td></tr>
<tr><td>Gobierno de TI</td><td></td></tr>
<tr><td>Auditoria y Seguridad Informática</td><td>X</td></tr>
<tr><td>Simulación</td><td></td></tr>
<tr><td colspan="4">C. PLANTEAMIENTO DEL PROBLEMA</td></tr>
<tr><td colspan="4">En la actualidad las organizaciones sufren diferentes cambios en el mercado ya sean estos organizacionales, tecnológicos, competitivos, sociedades, y culturales por tal motivo se considera poco pertinente seguir realizando las actividades bajo el mismo rumbo tradicional.

Las organizaciones proveedoras de internet que existen en el cantón Cañar de alguna manera u otra han sufrido algún incidente ya sea esto provocado por el hombre o por la naturaleza teniendo como resultado la perdida de servicio, perdida de equipos informáticos, pérdidas económicas etc., esto debido a que no cuentan con un plan de continuidad de negocios bien estructurado.

El plan de continuidad de negocio es una disciplina que prepara a la organización a mantener la continuidad en sus negocios durante un desastre, a través de la implementación de la misma.</td></tr>
</table>

El BCP **(Business Continuity Plan)** es adaptable en cualquier tipo de organización, es importante debido a la prioridad que proporciona al servicio de los clientes

No importa el tamaño de la empresa o las medidas de seguridad implantadas, toda empresa necesita de un plan de continuidad de servicio, ya que tarde o temprano se encontrará con una incidencia de seguridad que pongan en riesgos a los servidores, o algún evento que detenga totalmente la operación de la empresa.

La empresa Cañar Net, en la actualidad es una importante entidad que proporciona internet a la provincia del Cañar y sus parroquias, y gracias a los beneficios que ofrece, maneja una gran cantidad de clientes. El Problema surge cuando sus redes de distribución y la gran cantidad de información que manejan sus servidores aumenta, ocasionando fallos en su correcto funcionamiento debido a la sobrecarga de información, evitando así su normal funcionamiento y sostenibilidad de la empresa.

Por este motivo la elaboración de un plan de continuidad, es creado con el objetivo de dar solución a algunos problemas que puedan afectar a la empresa, el cual tiene como finalidad promocionar una guía, para que la empresa pueda superar cierto problema que afecte en su desarrollo.

D. OBJETIVO GENERAL

Diseñar un Plan de Continuidad de negocio en la empresa Cañar Net. Mediante la utilización de estándares reconocidos para garantizar la provisión de los servicios que brinda a sus clientes.

E. OBJETIVOS ESPECÍFICOS
Realizar un estudio teórico de las normativas del plan de continuidad de negocio.
Identificar los riesgos internos que presenta la empresa Cañar Net. Y que generen interrupciones en el servicio mediante el análisis del entorno.
Elaborar el plan de continuidad de negocio para la empresa Cañar Net. Como herramienta preventiva que garantice la continuidad del proceso ante un incidente existente.

F. JUSTIFICACIÓN

En la actualidad las tecnologías de información han evolucionado considerablemente obligando a que las necesidades de los consumidores cambien a otro ritmo y busquen una atención adecuada, soluciones efectivas y servicios apropiados.

Las organizaciones hoy en día dependen mucho de la tecnología ya que en base a un conjunto de técnicas realizan sus actividades, de la misma manera que la tecnología ayuda a cumplir con los objetivos de la empresa también trae consigo un sin número de riesgos, amenazas que puede afectar el normal funcionamiento de la organización. [1]

Las organizaciones buscan un estándar o metodología que brinde seguridad y tranquilidad al momento de enfrentar problemas y situaciones adversas a las cuales se encuentran expuestas. Lamentablemente han ocurrido incidentes en empresas proveedoras de internet que por no disponer de una estructura definida de un plan de continuidad de negocios han perdido la credibilidad de sus clientes, equipos informáticos y pérdidas económicas.

El propósito de esta investigación es dar a conocer las pautas necesarias de lo que se debe realizar ante desastres provocados por el hombre, problemas técnicos, la naturaleza etc. Para ello la utilización de un Plan de continuidad de negocio ayudara a estar preparados frente a la contingencia con el único propósito de minimizar las pérdidas de la organización.

Al implementar un Plan de Continuidad de Negocio en la empresa Cañar Net. Proporcionaría una ventaja competitiva frente a otras empresas ya que el hecho de mostrar que se toman medidas para garantizar la continuidad del negocio mejora la imagen pública, consigue mayor confianza de los clientes. Por otra parte, ayuda también a la gestión preventiva de los riesgos que puede impactar en sus operaciones así podrá prevenir y minimizar las pérdidas de la organización en caso de que se presente un desastre.

El Plan de Continuidad se realizará con el objetivo de las necesidades que surge en la empresa, que permita reducir la perdida de información y disponibilidad de servicio.

G. ALCANCE

El alcance de la presente investigación tiene como finalidad la evaluación y diagnostico de la empresa Cañar Net.

H. CONCEPTOS RELACIONADOS

Concepto de BCP (Plan de Continuidad de Negocios)

Es una disciplina que prepara a una organización a mantener continuidad en sus negocios durante un desastre, a través de la implementación de un Plan Continuidad de Negocio. [2]

Continuidad de Negocio

El termino BCP[3], según la definición antes descrita es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona estrategias que debe seguir al momento de presentar interrupción en las funciones o actividades que viene realizando la empresa tomando en cuenta las medidas de prevención ante la criticidad de los procesos y el tiempo de recuperación. [3]

[3] Bussiness Continuity Plan o plan de continuidad de negocio

El plan de continuidad de negocio tiene como objetivo identificar todo lo necesario para que el negocio continúe con sus actividades antes, durante y después de un incidente severo, grave, desastroso. Puede estar compuesto por otros planes, como el parecido Plan de Contingencia, que se ciñe a las tecnologías de la información y las comunicaciones o el Plan de Recuperación ante desastres, más centrado en la gestión de crisis-incidentes. [4]

Un plan de continuidad de negocio consta básicamente del diseño de medidas y la adaptación de recursos para hacer frente a la situación creada como consecuencia de la materialización de un riego, antes de adoptar esas medidas, se deben analizar cuáles son las amenazas más probables para la organización y la probabilidad de que estas amenazas se materialicen causando la interrupción de las operaciones de la organización. [5]

Estructura de un plan de continuidad de negocios

El plan de continuidad de negocio cuenta con la siguiente estructura:

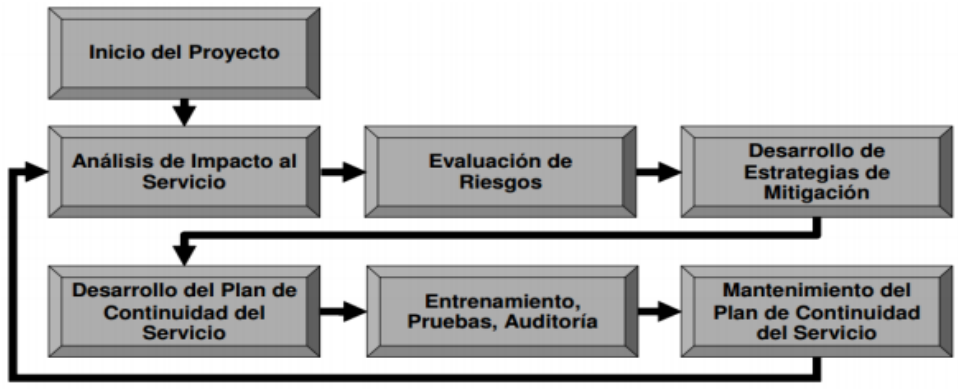


Ilustración 17: Estructura Plan de Continuidad del Negocio

Análisis del impacto del negocio (BIA)

"El propósito del BIA es poner en correlación los componentes específicos del sistema con los servicios críticos que ellos proporcionan, y basado en esa información, analizar las

consecuencias de una ruptura de los componentes del sistema. El objetivo fundamental es identificar las áreas que sufrirían las pérdidas financieras y operacionales más grandes en el caso de un desastre. Además, identifica los sistemas críticos y estima el tiempo que la compañía puede tolerar en caso de un desastre"

Metodologías y estándares para la elaboración de un plan de continuidad de negocio

Metodologías

Cuando se habla sobre administración de continuidad de negocio, el núcleo del concepto se enfoca en todos los procesos que se deben ejecutar para asegurar la supervivencia de una empresa o institución en caso de que esta se sometiera a una interrupción no deseada de su negocio y por ende de su funcionamiento.

Citando las cifras descritas por el Emergency Management Forum (Estados Unidos), de cada 100 empresas que afrontan un desastre sin contar con una Administración de Continuidad, 43% nunca reabren el negocio, 51% sobrevive, pero están fuera del mercado en 2 años y solo el 6% logra sobrevivir a largo plazo. Es por este motivo que el mundo ha tomado conciencia sobre la importancia de tener normas, estándares y un consenso de buenas prácticas en lo referente a la Administración de continuidad del Negocio, entre las cuales se puede citar las siguientes:

British Standards Institute (BSI): BS 25999-1 BS 25999-2

Es un estándar británico desarrollado en un inicio como un Plan de Continuidad de Negocio (BCP) y luego expandido a una Administración de Continuidad de Negocio (BCM) creado y mejorado por un grupo de expertos de relevancia mundial en los sectores de la industria. Se trata de una norma certificable; es decir, que entrega una certificación a quienes

comprueben conocimiento y práctica de la misma; en el cual se tienen en cuenta tanto los recursos humanos, como las infraestructuras, la información vital, las tecnologías de información y los equipos que la soportan. [6]

La norma consiste en una serie de recomendaciones o buenas prácticas para facilitar la recuperación de los recursos antes mencionados en caso de que se presente una crisis, y fue dividida en dos partes:

- BS 25999-1: (2005) Documento orientativo que proporciona las recomendaciones prácticas para el BCM

- BS 25999-2: (2006) Establece los requisitos para un sistema de Administración de Continuidad de Negocio (BCM): es la parte certificable a través de la implementación, auditoría y certificación. [6]

ISO 22301 BCM Standard

Este estándar se constituye en la publicación más actual en lo referente a especificaciones de la Administración de Continuidad del Negocio; apenas el 16 de mayo del 2012 fue su publicación oficial cuyo nombre completo es: "ISO 22301:2012 Societal Security – Business Continuity Management Systems - Requeriments". Este constituye uno más de los 100 estándares de BCM disponibles en el mercado, su particularidad nace de que al ser un estándar ISO tiene más credibilidad porque ha sido desarrollador por un grupo de expertos en dicho dominio. [6]

I. TRABAJOS RELACIONADOS

Seguridad de la Información
"El Análisis De Riesgos Informáticos Y Su Incidencia En La Seguridad E Integridad De La Información
"Análisis de Riesgos Informáticos y Desarrollo de un Plan de Seguridad de la Información para el Gobierno Autónomo Descentralizado Municipal de Catamayo"

J. METODOLOGÍA

Cuando se habla sobre administración de continuidad de negocio, el núcleo del concepto se enfoca en todos los procesos que se deben ejecutar para asegurar la supervivencia de una empresa o institución en caso de que esta se sometiera a una interrupción no deseada de su negocio y por ende de su funcionamiento.

Citando las cifras descritas por el Emergency Management Forum (Estados Unidos), de cada 100 empresas que afrontan un desastre sin contar con una Administración de Continuidad, 43% nunca reabren el negocio, 51% sobrevive, pero están fuera del mercado en 2 años y solo el 6% logra sobrevivir a largo plazo. Es por este motivo que el mundo ha tomado conciencia sobre la importancia de tener normas, estándares y un consenso de buenas prácticas en lo referente a la Administración de continuidad del Negocio, entre las cuales se puede citar las siguientes:

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES						
		I	II	III	IV	V	VI	MEDIOS DE VERIFICACIÓN
1	Fundamentación Teórica	x						Primer capítulo de la Tesis (Conceptos Relacionados y Trabajos Relacionados).
2	Diagnóstico Situacional		x					Segundo capítulo de la Tesis (Problema, objetivos, justificación, alcance y

								aplicación de la metodología propuesta).
3	Desarrollo de la propuesta		x	x	x			Tercer capítulo de la Tesis.
4	Validación de la propuesta				x	x		Cuarto capítulo de la Tesis.
5	Conclusiones y recomendaciones						x	Sección de conclusiones y recomendaciones de la Tesis.

L. DECLARACIÓN FINAL

Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES

DIRECTOR:	ING. CRISTIAN FLORES U.
ESTUDIANTE 1	MIRIAM MARIBEL ALLAICO CHIMBORAZO
ESTUDIANTE 2	

N. FIRMAS DE RESPONSABILIDAD

Lugar:	
Fecha:	

Firmas:

Nombre:	Nombre:
CC:	C.C.:
Director del Proyecto	**Estudiante / Egresado**

O. APROBACIÓN

Firmas:

Nombre:	Nombre:
CC:	C.C.:
Primer Par Revisor	**Segundo Par Revisor**

P. REFERENCIAS

CERDA, W. O. (2013). *repositorio.puce.edu.ec.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/12656/Tesis_JacomeWilsonMGTI.pdf?sequence=1

Conza Gonsález , A. E., & Medrano Chimborazo, L. X. (2015). *dspace.udla.edu.e.* Obtenido de http://dspace.udla.edu.ec/bitstream/33000/4473/1/UDLA-EC-TIS-2015-02.pdf

J. Gaspar, J. G. (2004). *Planes de Contingencia la Continuidad Del Negocio en Las Organizaciones.* Ediciones Díaz de Santos, 2004.

J., G., & Martínez, J. G. (s.f.). *Planes de Contingencia la Continuidad Del Negocio en Las Organizaciones.* Madrid: Ediciones Díaz de Santos, 2004.

Moreno, J. Z. (2015). *Ciberdiccionario: Conceptos de ciberseguridad en lenguaje entendible.* Javier Zubieta, 2015.

SABINO, C. (25 de MAYO de 2016). *INVESTIGACION DESCRIPTIVA* . Obtenido de https://tesisplus.com/investigacion-descriptiva/investigacion-descriptiva-segun-autores/

Santos, E. D. (2004). *Planes de Contingencia la Continuidad Del Negocio en Las Organizaciones.* Ediciones Díaz de Santos.

ANEXO B: PROPUESTA DE PLAN DE CONTINUIDAD DE NEGOCIOS

UNIVERSIDAD CATÓLICA DE CUENCA

Cañar Net
Internet de alta velocidad y TV en full HD

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

PLAN DE CONTINUIDAD DE NEGOCIOS

MIRIAM MARIBEL ALLAICO CHIMBORAZO

MANUAL DESARROLLADO BAJO LA NORMA ISO 22301

ISO 22301

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Cañar Net es una empresa proveedora de internet dedicada a brindar servicio en los cantones: Cañar, El Tambo, Suscal con sus respetivas parroquias de acuerdo a la disponibilidad de cobertura. Esta empresa ofrece servicio de internet banda ancha ilimitada, para tener acceso a internet no necesita de una línea telefónica, el servicio es ilimitado 24/7, sin restricciones de navegación, descargas ilimitadas, la velocidad y correcto funcionamiento del servicio contratado puede variar de acuerdo a: capacidad y configuración del computador, las características del rendimiento de cada uno de los componentes de la red, y la cantidad de usuarios conectados simultáneamente al internet.

En la actualidad la demanda del servicio de internet cada vez es mayor y es una oportunidad para dar a conocer otro mecanismo que ofrezca este importante y necesario servicio en este mundo globalizado y moderno. Toda empresa proveedora de internet necesita ser eficiente y estar regulado por las mejores prácticas, normas, políticas, procedimientos y metodologías agiles que permitan restaurar el servicio de sus actividades y equipos a la hora de presentar alguna interrupción o falla.

En base a lo antes expuesto el presente trabajo investigativo ha sido fundamentado en la necesidad de la empresa Cañar Net de resguardar la información proveniente de las diferentes aplicaciones informáticas del área de TI considerando a esta información como los activos esenciales de la empresa, por otro lado, se pretende también realizar un BCP que permita mitigar los riesgos de la empresa.

El plan de continuidad facilitara la solución para un problema que afecte a la empresa, mejorando así la eficiencia y desarrollo de la misma. Las empresas experimentan situaciones de emergencia, directa o indirectamente, las cuales necesitan respuestas inmediatas. El Plan de Continuidad del Negocio (BCP) permite establecer los

procedimientos para asegurar la continuidad de una empresa en caso de que esta se viera sometida a una interrupción no deseada de su negocio. El presente trabajo está orientado al desarrollo del Plan de Continuidad del Negocio en la empresa Cañar Net, dentro de una empresa de servicios de Seguros de Vida por la factibilidad de conocer sus procesos y tener la apertura para este plan. El desarrollo está basado en la norma ISO 22301 "Sistema de Gestión de la Continuidad del Negocio", siguiendo sus fases el trabajo incluye una breve descripción de la empresa Cañar Net, se evalúa los posibles riesgos y amenazas a las que está expuesta, se realiza un Análisis de Impacto del Negocio(BIA) que es el punto de partida para crear las estrategias de continuidad, se define un conjunto de equipos para el restablecimiento de operaciones y los procedimientos a utilizarse, y se definió objetivamente los procesos críticos de la compañía que apoya a la toma de decisiones empresariales

2. OBJETIVOS

1.1. 2.1 Objetivo general

Asegurar que la empresa Cañar Net este preparado para responder a emergencias, recuperarse de la misma y mitigar los impactos ocasionados, permitiendo la continuidad de servicios críticos para la atención de clientes y la operación.

1.2. 2.2 Objetivo especifico

- Lograr el nivel de preparación frente a la presencia de incidentes que permita asegurar y proteger la integridad de las personas y equipos de la empresa en forma adecuada, realizando una buena administración de la crisis.
- Minimizar la frecuencia de interrupciones de la operación de los procesos del negocio.
- Asegurar una pronta restauración de las operaciones afectadas por el incidente.

- Minimizar las decisiones a tomar en caso de contingencia para evitar cometer errores.

3. ALCANCE

El plan de continuidad de negocio es una disciplina que prepara a la organización para que la misma pueda seguir operando durante la presencia de un incidente o desastre a través de la implementación de un BCP el cual contempla los lineamientos de administración de la continuidad de la empresa, las metodologías definidas por la empresa Cañar Net.

El alcance de la propuesta de plan de continuidad de negocios para la empresa Cañar net está orientada en la realización de un documento ya antes mencionado en donde se priorizan los procedimientos a seguir ante un incidente.

En esta documentación se plasma una descripción de los procedimientos a seguir, las responsabilidades individuales de cada departamento o personal que integra la empresa, con el fin de restaurar el servicio en el menor tiempo posible. Cada procedimiento o fase que se desarrollara en este documento están bajo los criterios de información que define un BCP y están alineados a las mejores prácticas de la norma ISO 22301

4. POLÍTICA

Dentro de las políticas de un BCP esta evitar interrupciones de los procesos críticos del negocio como consecuencia de fallas o desastres que paralicen el servicio de la empresa.

Debido a que cualquier interrupción o desastre en los procesos de negocio afecte el normal funcionamiento de las operaciones, es responsabilidad de la directiva de la organización aprobar un plan de continuidad de negocios que cubra las actividades esenciales y críticas de Cañar Net.

Dentro de las políticas de un BCP se deben considerar lo siguiente:

- Respaldos de la información.
- Seguridad física.
- Mantenimiento del plan.
- Roles y responsabilidades.

Para el último elemento de la política general es responsabilidad del gerente general de la empresa Cañar Net. Aprobar las directrices de la misma para que luego se haga un estudio previo y detallado de sus posibles consecuencias todo esto con el fin de garantizar la continuidad de negocio en el caso de que afecte el normal funcionamiento de los procesos. política de la gestión del servicio

proveer un servicio de internet de calidad y apropiado a las necesidades de sus clientes cumpliendo con los requerimientos del servicio, manteniendo un personal calificado y capacitado, gestionando la infraestructura, tecnología y recursos óptimos para la gestión del servicio y finalmente comunicando, revisando y actualizando los objetivos y directrices del sistema de gestión de servicios.

5. **REQUISITOS**

Que todo el personal administrativo y de servicio tengan conocimiento de un Plan de Continuidad de Negocio y su existencia dentro de la empresa Cañar Net.
Concienciación de todo el personal administrativo y de servicio sobre los procesos con los que cuenta la institución y las posibles amenazas que podrían presentarse y afectar a la empresa proveedora de internet. Disponibilidad de los recursos necesarios para llevar a cabo el plan de respuesta rápida ante la suspensión de servicios o incidentes.

6. PRINCIPIOS

Proteger los activos con mayor criticidad de ISP Cañar Net. Contra los diferentes incidentes o desastres de origen natural o industrial que se lleguen a presentar y cause consecuencias ya sean estas pérdidas financieras, credibilidad, pérdidas materiales entre otras, dentro de la empresa por la falta de servicios. Minimizar el riesgo o incidente que se llegara a presentar dentro de la organización, mediante un plan que permita volver a recuperar el servicio en el menor tiempo posible.

7. ESTRATEGIAS Y POLÍTICAS GENERALES PARA LA RECUPERACIÓN ANTE INCIDENTES

Para dar cumplimiento a la política general antes planteada se requiere que el personal administrativo y de servicio de la empresa proveedora de internet Cañar Net tengan conocimiento del manual de Plan de Continuidad de negocios de cada uno de los riesgos que se presenta en la institución y el procedimiento a seguir ante la presencia de un incidente.

8. ESTRATEGIAS DE PLAN DE RECUPERACIÓN ANTE INCIDENTES EN LA EMPRESA CAÑAR NET

8.1. Resumen del análisis de gestión de riesgos

De acuerdo con el trabajo investigativo que lleva como nombre DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA LA EMPRESA CAÑAR NET en donde se realizó un análisis y gestión de riesgos a los procesos, activos, etc. Se pudo evidenciar diferentes falencias con relación al área de TI tal como se plasmó en el capítulo IV dando como resultado los procesos más críticos mismos que se detallan a profundidad en el documento antes mencionado.

8.2. Resultado del análisis y gestión de riesgos

Luego de haber realizado el análisis se obtuvo como resultado los siguientes procesos críticos que podrían tener un impacto crítico sobre la continuidad de las operaciones, impacto financiero, humano y de reputación sobre la empresa, estos son:

- Gestión de servicio al cliente
    - Gestión de incidentes
- Desarrollo de servicio y operaciones

- Gestión de incidentes en el servicio
- Gestión de la calidad del servicio

- Gestión de sistemas y redes
    - Mantenimiento y restauración de redes
- Redes físicas y tecnología de la información
    - Gestión de tecnologías de la información y seguridad informática

MACROPROCESO	PROCESO	SUBPROCESO	CALIFICACIÓN DE ACTIVOS		ANALISIS DE RIESGO					SALVAGUARDAS
			CODIGO ACTIVO	DENOMINACIÓN	Código Amenaza	Amenaza	Probabilidad de ocurrencia	Impacto	Riesgo	
Gestión de servicio al cliente	Gestión de incidentes		Ac-Sis-004	Sistemas informáticos	[I.6]	Corte del suministro eléctrico	4	2	Medio	HW. A Aseguramiento de la disponibilidad
					[I.8]	Fallo de servicios de comunicaciones	4	3	Alto	COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
					[I.9]	Interrupción de otros servicios y suministros esenciales	4	3	Alto	AUX.A Aseguramiento de la disponibilidad
					[E.8]	Difusión de software dañino	2	3	Medio	SW Protección de las Aplicaciones Informáticas SW.CM Cambios (actualizaciones y

										mantenimiento)
					[E.18]	Destrucción de información	2	4	Medio	MP.A Aseguramiento de la disponibilidad
					[E.21]	Errores de mantenimiento / actualización de programas (software)	2	4	Medio	SW Protección de las Aplicaciones Informáticas SW.CM Cambios (actualizaciones y mantenimiento)
					[E.24]	Caída del sistema por agotamiento de recursos	3	3	Medio	HW Protección de los Equipos Informáticos HW.A Aseguramiento de la disponibilidad HW.CM Cambios (actualizaciones y mantenimiento) S Protección de los Servicios
					[A.23]	Manipulación de los equipos	3	3	Medio	HW Protección de los Equipos

										Informáticos HW.CM Cambios (actualizaciones y mantenimiento)
					[A.24]	Denegación de servicio	2	3	Medio	S.A Aseguramiento de la disponibilidad S.CM Gestión de cambios (mejoras y sustituciones) S.www Protección de servicios y aplicaciones web
			Ac-Sis-019	Equipo de monitoreo	[N.1]	Fuego	3	3	Medio	Disponer de un extintor
					[N.2]	Daños por agua	2	3	Medio	S.A Aseguramiento de la disponibilidad
					[I.5]	Avería de origen físico o lógico	3	3	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio

					[I.6]	Corte del suministro eléctrico	4	3	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico
					[I.8]	Fallo de servicios de comunicaciones	4	3	Alto	COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
					[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	2	Medio	HW Protección de los Equipos Informáticos HW.A Aseguramiento de la disponibilidad
					[E.25]	Pérdida de equipos	4	2	Medio	HW.SC Se aplican perfiles de seguridad HW.A Aseguramiento

										de la disponibilidad
					[A.24]	Denegación de servicio	4	3	Alto	S.A Aseguramiento de la disponibilidad S.SC Se aplican perfiles de seguridad
					[A.26]	Ataque destructivo	4	3	Alto	H Protecciones Generales H.IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.SFV Verificación de las funciones de seguridad
Desarrollo de servicio y operaciones	Gestión de incidentes en el servicio		Ac-Sis-001	Red de Datos	[I.6]	Corte del suministro eléctrico	2	3	Medio	HW.A Aseguramiento de la disponibilidad

					[I.8]	Fallo de servicios de comunicaciones	4	3	Alto	COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
					[I.9]	Interrupción de otros servicios y suministros esenciales	3	2	Medio	AUX.A Aseguramiento de la disponibilidad
					[E.8]	Difusión de software dañino	3	3	Medio	SW Protección de las Aplicaciones Informáticas SW.CM Cambios (actualizaciones y mantenimiento)
					[E.14]	Escapes de información	4	3	Alto	SW Protección de las Aplicaciones Informáticas SW Protección de las Aplicaciones Informáticas

	Gestión de la calidad del servicio				[E.15]	Alteración accidental de la información	3	3	Medio	D Protección de la Información H.tools Herramientas de seguridad
					[E.19]	Fugas de información	3	2	Medio	D Protección de la Información D.C Cifrado de la información
					[E.20]	Vulnerabilidades de los programas (software)	3	3	Medio	SW Protección de las Aplicaciones Informáticas
Redes físicas y tecnologia de la información	Gestión de tecnologías de la información y seguridad informatica	Respaldo y restauración de información de los servidores	Ac-Sis-006	Servidor Proxy	[N.1]	Fuego	2	3	Medio	disponer de extintores de fuego HW Protección de los Equipos Informáticos AUX.wires Protección del cableado
					[N.2]	Daños por agua	2	3	Medio	HW Protección de los Equipos Informáticos
					[I.6]	Corte del suministro eléctrico	2	3	Medio	HW Protección de los Equipos Informáticos disponer de un generador de energia electrica

					[E.14]	Escapes de información	3	3	Medio	SW Protección de las Aplicaciones Informáticas SW.SC Se aplican perfiles de seguridad
					[E.15]	Alteración accidental de la información	4	2	Medio	SW Protección de las Aplicaciones Informáticas SW.SC Se aplican perfiles de seguridad SW.A Copias de seguridad (backup)
					[E.18]	Destrucción de información	2	4	Medio	MP Protección de los Soportes de Información MP.A Aseguramiento de la disponibilidad MP.IC Protección criptográfica del contenido
					[A.8]	Difusión de software dañino	2	3	Medio	MP.IC Protección criptográfica del contenido COM.A Aseguramiento

										de la disponibilidad
					[A.18]	Destrucción de información	2	3	Medio	MP Protección de los Soportes de Información MP.A Aseguramiento de la disponibilidad MP.IC Protección criptográfica del contenido
					[A.22]	Manipulación de programas	3	4	Alto	COM.SC Se aplican perfiles de seguridad SW Protección de las Aplicaciones Informáticas SW.SC Se aplican perfiles de seguridad
			Ac-Sis-013	Router principal Backup (Cañar)	[N.1]	Fuego	3	3	Medio	disponer de extintores de fuego HW Protección de los Equipos Informáticos AUX.wires Protección del cableado

					[N.2]	Daños por agua	3	3	Medio	HW Protección de los Equipos Informáticos
					[I.5]	Avería de origen físico o lógico	3	2	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio
					[I.6]	Corte del suministro eléctrico	4	3	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico
					[I.8]	Fallo de servicios de comunicaciones	4	3	Alto	AUX.A Aseguramiento de la disponibilidad
					[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	3	Alto	AUX.wires Protección del cableado COM.CM Cambios (actualizaciones y mantenimiento)

					[E.25]	Pérdida de equipos	3	3	Medio	HW.SC Se aplican perfiles de seguridad HW.A Aseguramiento de la disponibilidad
					[A.23]	Manipulación de los equipos	3	2	Medio	D.I Aseguramiento de la integridad
			Ac-Sis-015	Router Honorato Vasquez	[N.1]	Fuego	3	3	Medio	Disponer de un extintor
					[N.2]	Daños por agua	3	3	Medio	S.A Aseguramiento de la disponibilidad
					[I.5]	Avería de origen físico o lógico	3	3	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio
					[I.6]	Corte del suministro eléctrico	4	3	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico

					[I.8]	Fallo de servicios de comunicaciones	4	3	Alto	COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
					[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	3	Alto	HW Protección de los Equipos Informáticos HW. A Aseguramiento de la disponibilidad
					[A.24]	Denegación de servicio	4	4	Alto	S. A Aseguramiento de la disponibilidad S.SC Se aplican perfiles de seguridad
					[A.26]	Ataque destructivo	3	3	Medio	H Protecciones Generales H. IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de

										incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.SFV Verificación de las funciones de seguridad
			Ac-Sis-016	Router Pilco pata	[N.1]	Fuego	3	3	Medio	Disponer de un extintor
					[N.2]	Daños por agua	3	3	Medio	S.A Aseguramiento de la disponibilidad
					[I.5]	Avería de origen físico o lógico	3	3	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio
					[I.6]	Corte del suministro eléctrico	4	3	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power

										Suministro eléctrico
					[I.8]	Fallo de servicios de comunicaciones	4	3	Alto	COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
					[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	2	Medio	HW Protección de los Equipos Informáticos HW. A Aseguramiento de la disponibilidad
					[E.25]	Pérdida de equipos	3	2	Medio	HW.SC Se aplican perfiles de seguridad HW. A Aseguramiento de la disponibilidad
					[A.24]	Denegación de servicio	4	3	Alto	S. A Aseguramiento de la disponibilidad S.SC Se aplican

										perfiles de seguridad
					[A.26]	Ataque destructivo	3	3	Medio	H Protecciones Generales H. IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.SFV Verificación de las funciones de seguridad
			Ac-Sis-017	Router Altarhurco	[N.1]	Fuego	3	3	Medio	Disponer de un extintor
					[N.2]	Daños por agua	3	3	Medio	S.A Aseguramiento de la disponibilidad
					[I.5]	Avería de origen físico o lógico	3	3	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad

										BC Continuidad del negocio
					[I.6]	Corte del suministro eléctrico	4	3	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico
					[I.8]	Fallo de servicios de comunicaciones	4	3	Alto	COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
					[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	2	Medio	HW Protección de los Equipos Informáticos HW. A Aseguramiento de la disponibilidad
					[E.25]	Pérdida de equipos	3	2	Medio	HW.SC Se aplican perfiles de seguridad HW. A

										Aseguramiento de la disponibilidad
					[A.24]	Denegación de servicio	4	3	Alto	S. A Aseguramiento de la disponibilidad S.SC Se aplican perfiles de seguridad
					[A.26]	Ataque destructivo	3	3	Medio	H Protecciones Generales H. IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.SFV Verificación de las funciones de seguridad
			Ac-Sis-018	Router Hueran	[N.1]	Fuego	3	3	Medio	Disponer de un extintor
					[N.2]	Daños por agua	3	3	Medio	S.A Aseguramiento

										de la disponibilidad
					[I.5]	Avería de origen físico o lógico	3	3	Medio	L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad BC Continuidad del negocio
					[I.6]	Corte del suministro eléctrico	4	3	Alto	BC Continuidad del negocio AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico
					[I.8]	Fallo de servicios de comunicaciones	4	3	Alto	COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM Protección de las Comunicaciones
					[E.23]	Errores de mantenimiento / actualización	4	2	Medio	HW Protección de los Equipos Informáticos

						de equipos (hardware)				HW.A Aseguramiento de la disponibilidad
					[E.25]	Pérdida de equipos	3	2	Medio	HW.SC Se aplican perfiles de seguridad HW.A Aseguramiento de la disponibilidad
					[A.24]	Denegación de servicio	4	3	Alto	S.A Aseguramiento de la disponibilidad S.SC Se aplican perfiles de seguridad
					[A.26]	Ataque destructivo	3	3	Medio	H Protecciones Generales H.IA Identificación y autenticación H.AC Control de acceso lógico H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino

9. ESTRATEGIAS DE CONTINUIDAD DE NEGOCIOS

A continuación, se detalla las estrategias de trabajo a seguir para de esta manera garantizar la continuidad de los procesos y la estabilidad de los servicios ante la presencia de algún incidente que llegara a suceder dentro o fuera de la empresa.

9.1. Declaración de emergencia

En esta fase del plan de continuidad de negocio se diseña una matriz en donde va a estar detallo el objetivo, el alcance, el personal responsable, el equipo estar encargado de los procedimientos a seguir ante la presencia de una emergencia.

Procedimiento para la declaración de emergencia	
Objetivo	Informar al personal administrativo y de servicio de la empresa proveedora de internet Cañar Net, que se encuentran relacionados con el plan de continuidad de negocios el procedimiento ante la presencia de un incidente y el mismo puede afectar los servicios informáticos de la empresa.
Alcance	El alcance de la declaración de emergencias inicia desde el momento en que se identifica el incidente que puede paralizar las actividades que se realizan en la organización, luego de ello el comité de administración de crisis debe declarar la emergencia y dispone la activación del Plan de continuidad de negocio (BCP)
Responsable operativo	En esta fase debe existir un comité de riesgos, el mismo que será designado por el gerente de Cañar Net, Ing. Carlos León A.
Lineamiento	Involucrados: Los involucrados son todo el personal administrativo y de servicios, directivos, proveedores que laboren en la empresa Cañar Net. Evento de riesgo: Los eventos de riesgos pueden llegar a ser ocasionados por el hombre, por desastres naturales etc. Los mismos pueden ocasionar interrupciones en los servicios.
RESPONSABLES	ACTIVIDADES
Personal administrativo o técnicos de servicio de Cañar Net.	Al momento de la identificación de incidentes se debe comunicar de inmediato a cualquier miembro del equipo de evaluación de incidentes, el mismo que lleva la siguiente jerarquía: Gerente de la empresa Cañar Net. Jefe del área de tecnologías de Información TIC Jefe de riesgos integrales.
	La notificación se lo realizara primeramente de manera telefónica posteriormente debe hacer llegar un correo electrónico notificando la presencia de incidentes que puede afectar el normal funcionamiento de las actividades de la organización.
Equipo de evaluación de incidentes	La persona encargada de recibir la notificación de incidentes ya sea vía llamada o correo electrónico debe seguir los siguientes pasos: 1. Acudir al lugar del incidente o lo podrá realizar de manera virtual dependiendo de qué tan grave sea el incidente, esto lo debe realizar en el lapso de 1 hora de haber recibido la notificación. 2. Una vez identificado el incidente comunicara a los demás miembros del equipo o comité de evaluación de incidentes. 3. Analizan y evalúan el incidente cuando el impacto del mismo no sea totalmente evidente.

	4. Determinan si la presencia del incidente ocasionara la suspensión de los servicios informáticos o la operación de alguna de las áreas de la empresa o si el daño se da en el domicilio de algún cliente. En esta etapa el equipo de incidentes tendrá la obligación de calificar el nivel de alerta en el que se encuentra tal incidente estos niveles se dividen en tres los cuales son: • Nivel de alerta bajo En este nivel se encuentra controlado el riesgo, no afecta las operaciones y servicios de la organización. • Nivel de alerta medio Es un nivel en donde el riesgo impide las operaciones de un área en específico mas no impide o afecta los servicios de toda la empresa Cañar Net. • Nivel de alerta alto Es el nivel de riesgo más crítico ya que si llegara a materializarse el riesgo podría afectar los servicios de la empresa y el área tecnológica.
Jefe(a) del departamento de tecnologías de la información	El jefe(a) o encargado(a) del área de TI será el responsable de comunicar el nivel de alerta ya sea este alerta roja o amarilla dependiendo del incidente que se presente, esto tendrá un tiempo límite de 30 a 60 minutos posteriormente se procederá a la activación del Plan de Continuidad de negocio por último debe ser informado al Gerente General de Cañar Net.
Gerente General	El Gerente General junto al encargado del área de TI debe determinar si el incidente puede ser resuelto en el plazo máximo de 2 horas caso contrario se comunicará el incidente a uno de los miembros del Comité de Administración de Crisis sobre la gravedad del incidente

Luego de formar un comité de emergencias se procede al diseño de las estrategias de recuperación ante la presencia de incidentes, para los procesos y subprocesos críticos identificados anteriormente.

Procedimiento de operación de Gestión de servicio al cliente subproceso: Gestión de incidentes	
Objetivo	Estableces los lineamientos y las acciones a tomar en caso de llegar a presentarse algún incidente de riesgo, para de esta manera minimizar el impacto ocasionado.
Alcance	Personal encargado del departamento de servicio al cliente de Cañar Net.
Responsable operativo	Jefe del departamento de servicio al cliente.
ACTIVIDADES	
Los procedimientos de gestión de incidente pueden llegar a presentar los siguientes incidentes: • Corte del suministro eléctrico • Fallo de servicios de comunicaciones • Interrupción de otros servicios y suministros esenciales • Difusión de software dañino • Destrucción de información • Errores de mantenimiento / actualización de programas (software) • Caída del sistema por agotamiento de recursos • Manipulación de los equipos • Denegación de servicio • Fuego	

- Daños por agua
- Avería de origen físico o lógico
- -Corte del suministro eléctrico
- Fallo de servicios de comunicaciones
- Errores de mantenimiento / actualización de equipos (hardware)
- Pérdida de equipos
- Denegación de servicio
- Ataque destructivo

ACTIVIDADES DEL PROCESO

1. Entrada de incidente, el usuario da a conocer la existencia de un incidente.
2. El jefe del departamento de gestión de incidentes registra el mismo y procede.
3. A la Clasificación del incidente
4. diagnostico
5. monitorización y seguimiento
6. resolución
7. cierre de incidente.

RECURSOS CRÍTICOS

- Sistemas informáticos
- Equipo de monitoreo

PLAN DE CONTINUIDAD	
Plan de aseguramiento, capacidad y disponibilidad de la infraestructura tecnológica (instalación, configuración y administración de hardware, bases de datos, repositorios, entre otros recursos tecnológicos) con la que cuenta la empresa de internet Cañar Net. Disponer con un generador de energía para la matriz de la empresa, de esta manera al momento de que se produzca la perdida de energía la empresa siga brindando el servicio de internet, y cable. Disponer con más personal técnico disponible a la hora de presentarse un incidente de perdida de conexión de internet. Los mismos pueden encontrarse divididos por zonas o por la calificación de la gravedad del incidente.	**Tiempo máximo de Recuperación** 1 hora

Procedimiento de operación Desarrollo de servicio y operaciones: Gestión de incidentes en el servicio y Gestión de la calidad del servicio	
Objetivo	Resolver cualquier incidencia de la manera más eficaz y eficiente, de forma que no pueda llegar a causar una interrupción en el servicio dado a los usuarios, y que estos ni siquiera sean conscientes de que se ha producido.
Alcance	Personal técnico de la empresa proveedora de internet Cañar Net.
Responsable operativo	Jefe del departamento de personal técnico.

ACTIVIDADES

Los procedimientos de Desarrollo de servicio y operaciones, subproceso Gestión de incidentes en los servicios pueden llegar a presentar los siguientes incidentes:

- Corte del suministro eléctrico
- Fallo de servicios de comunicaciones
- Interrupción de otros servicios y suministros esenciales
- Difusión de software dañino
- Escapes de información

ACTIVIDADES DEL PROCESO

1. El usuario detecta un incidente y envía la petición.
2. Localiza al coordinador del departamento
3. Notifica al coordinador o jefe del departamento de tecnología
4. El departamento recibe el incidente
5. Registra el incidente
6. Asigna un técnico o analista del departamento de tecnología.
7. El analista o técnico del departamento de tecnología realiza un análisis del incidente
8. Visita al departamento que notifica la incidencia
9. Investiga y da un diagnostico
10. Revisa si lo puede resolver de lo contrario comunica al proveedor o soporte
11. Finalmente, lo resuelve

RECURSOS CRÍTICOS

- **Red de Datos**

PLAN DE CONTINUIDAD

Establecer una mejora continua del servicio en la que se revisen y mejoren los procedimientos, políticas, roles, tecnología y otros aspectos del proceso de gestión de incidentes.	**Tiempo máximo de Recuperación**

Ante incidentes como indisponibilidad del personal es recomendable la Definición del personal encargado en la preparación y capacitaciones constante del personal. Contar con personal idóneo para el cargo y personal secundario en caso de que se necesite realizar rotación.	

Procedimiento de operación de Gestión de sistemas y redes subproceso: Mantenimiento y restauración de redes.	
Objetivos	Corregir fallos en el hardware o software. Realizar actualizaciones cuando sean necesarias. Volver a instalar sistemas operativos. Realizar operaciones de limpieza de virus y otro tipo de software malicioso. Reparación o sustitución de hardware. Detectar y solucionar problemas y fallos en equipos y redes.
Alcance	Personal técnico de Cañar Net.
Responsable operativo	Jefe del departamento técnico

ACTIVIDADES

El procedimiento de operación de Gestión de sistemas y redes subproceso: Mantenimiento y restauración de redes puede llegar a tener los siguientes incidentes:

- Fallos en el administrador del sistema
- Centro de servicios de redes

ACTIVIDADES DEL PROCESO

1. Localiza al coordinador del departamento
2. Notifica al coordinador o jefe del departamento de tecnología
3. El usuario detecta un incidente y envía la petición.

PLAN DE CONTINUIDAD

La empresa proveedora de internet Cañar Net deberá dar seguimiento de las redes con la finalidad de garantizar un servicio de excelencia a los usuarios que hacen uso de sus servicios.	**Tiempo máximo de Recuperación**

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Miriam Maribel Allaico Chimborazo portador(a) de la cédula de ciudadanía Nº **0302747886**. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIO EN LA EMPRESA CAÑAR NET"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, **15 de octubre de 2021**

F: ……

Miriam Maribel Allaico Chimborazo

C.I. **0302747886**