OFICINA DE POSTGRADOS

TEMA:

DISEÑO DE UN PLAN DE CONTINUIDAD DE SERVICIOS DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN EN CASOS EXCEPCIONALES PARA LA EP-EMAPA DE LA CIUDAD DE AMBATO

Proyecto de Investigación previo a la obtención del título de
Magister en Gerencia Informática

Línea de Investigación:

Sistemas de información y/o nuevas tecnologías de la información y comunicación y sus aplicaciones

Autor:

Ing. Jorge Alfonso Jaramillo Camacho

Director:

Ing. José Marcelo Balseca Manzano Mg.

Ambato – Ecuador

Marzo 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

DISEÑO DE UN PLAN DE CONTINUIDAD DE SERVICIOS DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN EN CASOS EXCEPCIONALES PARA LA EP-EMAPA DE LA CIUDAD DE AMBATO

Línea de Investigación:

Sistemas de información y/o nuevas tecnologías de la información y comunicación y sus aplicaciones

Autor:

Jorge Alfonso Jaramillo Camacho

José Marcelo Balseca Manzano, Ing. Mg. f._____

CALIFICADOR

Galo Mauricio López Sevilla, Mg. f._____

CALIFICADOR

Betty Viviana Avellán Herrera, Mg. f._____

CALIFICADOR

Padre Juan Carlos Acosta Teneda, MSc. f._____

DIRECTOR UNIDAD ACADÉMICA

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

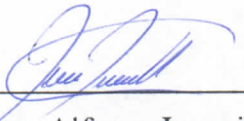
Marzo 2022

DECLARACIÓN Y AUTENTICIDAD

Yo **JORGE ALFONSO JARAMILLO CAMACHO**, con CC. **1802272508**, autor del trabajo de graduación intitulado: "DISEÑO DE UN PLAN DE CONTINUIDAD DE SERVICIOS DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN EN CASOS EXCEPCIONALES PARA LA EP-EMAPA DE LA CIUDAD DE AMBATO", previa a la obtención del título profesional de MAGISTER EN GERENCIA INFORMÁTICA, en la Oficina de Postgrados.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, marzo 2022



Ing. Jorge Alfonso Jaramillo Camacho

CC: 1802272508

AGRADECIMIENTO

Mi agradecimiento a todas las personas que siempre me apoyan y están junto a mí para brindarme sus palabras de aliento y comprensión, especialmente a mis padres Jorge y Luz Angélica, quien jamás desconfiaron de mi potencial para seguir capacitándome.

El reconocimiento y gratitud a todos los docentes y compañeros que me apoyaron en el desarrollo de conocimientos, en especial al Ing. Marcelo Balseca, quien como tutor me oriento en el desarrollo del presente proyecto de investigación.

DEDICATORIA

Todo fruto de esfuerzo personal se los dedico a mis hijos, Steven Alejandro, Isabel Cristina, Dominica Samanta, y Sara Amelia, para quienes quedará demostrado que lo que se propongan como objetivos de vida, lo pueden conseguir con el apoyo de los seres queridos y sobre todo con el valor y entereza que les ha regalado Dios desde su nacimiento.

A mis padres, que se merecen lo mejor de la vida.

RESUMEN

El presente proyecto de investigación, tiene por objeto implementar un plan de continuidad de servicios para el Departamento de Tecnologías de la Información de la EP-Empresa Municipal de Agua Potable y Alcantarillado de la ciudad de Ambato ya que no cuenta con dicho plan, por ende es necesario que se pueda determinar la forma de actuar frente a casos excepcionales con el fin de mantener la continuidad de los servicios que entrega el Departamento de TI, tanto a los clientes internos como externos. Además, los factores que intervienen en la metodología del análisis del impacto del negocio (BIA), lo cual, a futuro, en el caso de eventualidades no deseadas, puede experimentar riesgos críticos y colapsos en su sistema, incluyendo en este punto de amenaza de información temporal y definitiva. El plan pretende mantener preparada a la empresa frente a posibles desastres naturales como: erupciones volcánicas, terremotos, inundaciones u otros; además, desastres provocados intencionalmente como: sabotajes, ciberataques, negligencia, desorganización, mala administración de los recursos y otros percances accidentales como: incendios, cortes de energía eléctrica. Por ende, es importante reducir significativamente amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información, tanto física como electrónica, que procesa la institución. Así mismo, esta contribuye a establecer un proceso de mejora continua de la gestión de la seguridad de la información e incrementa la cultura de los servidores públicos en cuanto al manejo de la información que utilizan para cumplir sus funciones sea institucional o de la ciudadanía así mismo la legalización del plan de continuidad de la EP-EMAPA-A.

Palabras claves: recuperación; gestión de la información; plan de continuidad; riesgos críticos; tecnología de la información.

ABSTRACT

The purpose of this research work is to implement a service continuity plan for the Department of Information Technology of the EP-Municipal Company of Drinking Water and Sewerage of the city of Ambato since it does not have such a plan, therefore It is necessary to determine the way to act in exceptional cases in order to maintain the continuity of the services provided by the Department of Information Technology, both internal and external customers. In addition, the factors involved in the business impact analysis (BIA) methodology, which, in the future, in the case of unwanted eventualities, may experience critical risks and collapses in your system, including at this point of threat of Temporary and definitive information. The plan aims to keep the company prepared against possible natural disasters such as: volcanic eruptions, earthquakes, floods or others; In addition, intentionally caused disasters such as: sabotage, cyber-attacks, neglect, disorganization, mismanagement of resources and other accidental disasters such as: fires, power outages. Therefore, it is important to significantly reduce threats, risks and vulnerabilities related to the management of information, both physical and electronic, processed by the institution. Likewise, it contributes to establish a process of continuous improvement of information security management and increases the culture of public servants in terms of handling the information they use to fulfill their functions, whether institutional or citizenship. the legalization of the continuity plan of the EP-EMAPA-A.

Keywords: recovery; Information management; Services; External and internal customers; Business impact analysis; Critical Risks; Information technology

ÍNDICE GENERAL

Introducción

La evolución tecnológica representa una herramienta que permite integrar los procesos de información a través del control y organización especialmente en las empresas privadas como públicas en consecuencia, los departamentos de tecnología se han transformado en uno de los ejes primordiales en donde las direcciones generales de las empresas hacen cumplir con las responsabilidades desde el factor intrínseco es decir, la delegación hacia los trabajadores o clientes internos y desde la perspectiva externa la relación que se establece con los usuarios con la finalidad de entregar un servicio en base a la atención, servicio, calidad y satisfacción.

El propósito de la presente investigación se centra en la descripción de un plan de continuidad en los servicios mediante el uso informático de información para ser una guía de aplicación, en situaciones de riesgo que puedan afectar de forma crítica a una determinada empresa especialmente al departamento correspondiente a la tecnología. En este sentido se ha tomado como referencia la Empresa Pública - Empresa Municipal de Agua Potable y Alcantarillado de Ambato (EP-EMAPA-A), tiene la tarea de administrar el servicio de agua potable y alcantarillado a la ciudad de Ambato cuya, infraestructura corresponden a un edificio central y varias agencias, que permiten mantener una estrecha relación con los usuarios y brindar una atención óptima; además, las agencias cuentan con ventanillas para el cobro de las facturas y balcones de servicios que prestan atención a diferentes requerimientos que se realizan por medio de una red integrada de comunicación como las Tecnologías de la Información (TI´s)

Por tanto, la empresa realiza un proceso de gestión y operación garantizando un servicio de agua potable para beneficiar a la ciudadanía ambateña bajo este aspecto se desarrolló en el campo de la tecnología de la información la adopción eficaz de una planificación para incluir en los diferentes departamentos al integrar los sistemas de gestión de la calidad; que obedece a la norma ISO 9001 que a la presente mantiene la empresa EP-EMAPA-A; sin embargo, dentro de la empresa existe la delimitación en las tecnologías de la información de los servicios, por ende, existe la oportunidad de minimizar este tipo de problemas generados en la empresa pública.

La investigación pretende documentar de forma detallada la planificación de la continuidad del servicio del departamento de TI, estableciéndose los principios necesarios, el uso de la terminología además de la identificación y ejecución de procesos que permita a la empresa, por ende, al personal para saber sobre los procedimientos que se deberán seguir en caso de existir una eventualidad excepcional ya sea natural o humana.

El desarrollo de la documentación de un plan de continuidad del servicio del departamento de TI, para la empresa EP-EMAPA-A; se basa en el uso de diferentes principios y prácticas de las normas como la *ISO 22301*, que permite proporcionar confianza en las relaciones entre empresas y empresa – usuario. Por tanto, sirve como garantía entre las partes interesadas de que la institución se encuentra plenamente preparada y cumple a cabalidad con los requisitos para la continuidad de las operaciones durante imprevistos inesperados que afecten el normal desenvolvimiento del personal involucrado.

Sin embargo, la empresa tuvo la necesidad de aumentar la capacidad en base al servicio destinado a los clientes, por ende, se recurrió a ampliar la infraestructura y construcción de un nuevo edificio departamental en que incluía el estudio de ubicación en redes para agua potable y alcantarillado, ubicación de servidores, puntos de conexión para ser adecuadas dentro del departamento que a partir del año 2007, paso a denominarse como departamento de las tecnologías de información con el propósito de fomentar nuevas actividades entre ellas actualización de línea de base de datos, mantenimiento, redes.

Es así que esta entidad gubernamental fomenta la participación activa de las instituciones con el objetivo de trabajar anticipadamente en el fortalecimiento de las capacidades y potencialidades de la tecnología, enfocándose en consolidar el sistema económico social y solidario de forma sostenible, al desarrollo del entorno en el que se encuentre para colaborar con el eje número dos del Plan Nacional de Desarrollo 2017 – 2021 “Toda una Vida”, que determina la economía al servicio de la sociedad.

A partir del desarrollo del presente documento se proyecta generar un adecuado manejo claro, de mantener y actualizar las estrategias de recuperación y los programas de concienciación, ejercicios y capacitación a empleados y usuarios para la adecuada ejecución de los respectivos generales de los planes de recuperación de los servicios.

A nivel mundial, el avance de la tecnología ha requerido de un gran desafío para adoptar nuevos procesos en base de la planificación, sistematización de la información de una empresa, en vista que se deben documentar y mantener planes de continuidad, que garantice el fortalecimiento operativo en aquellos puntos críticos para proveer una guía e información a los equipos de recuperación de las tecnologías de la información para responder a la disrupción y asistir a la organización con la respuesta y la recuperación. Ortega (2017) enfatiza: "Los planes de continuidad de servicio de la información deben considerarse como un procesamiento alternativo y capacidad de recuperación en todos los puntos críticos sobre las TI para cubrir lineamientos en el uso, roles y responsabilidades de la información para un servicio".

Además, los planes de continuidad de servicios son los instrumentos más adecuados para ayudar a las empresas a superar situaciones extremas y continuar con la actividad minimizando las consecuencias más negativas. En el mercado de las Tecnologías de la Información es difícil encontrar un tema sobre el que exista tanta unanimidad como en torno a la necesidad de que todas las empresas y organizaciones cuenten con un plan de continuidad de servicios. El plan de continuidad de servicios es el conjunto de procedimientos que se realizan para reactivar las tareas de una empresa después de un suceso inesperado. Según Arteaga (2017) menciona: "La continuidad de los servicios de un negocio representa una prioridad que una empresa debe cuidar a otra mediante la aplicación de estrategias que identifiquen los riesgos latentes e impactos que generen peligro las organizaciones"

Al hablar sobre las tecnologías de la información, que se aplican en las empresas cuya necesidad sea llevar una adecuada planificación, organización y control asociados a un sistema en donde, Cruz et al. (2018) identifican que: "Cualquier producto que almacene, recupere, manipule, transmita o reciba información electrónicamente en forma digital puede permitir el acceso, producción, interacción, tratamiento y comunicación de información. Una de las formas más peligrosas de poner en riesgo la rentabilidad de una empresa es ignorar los peligros que amenazan a las organizaciones y que pueden tener un impacto directo sobre las finanzas y los intereses de clientes internos o externos. De acuerdo con, Córdoba (2008) opina que las razones para poner en marcha un *Bussiness Continuity Plan* (BCP) tienen que ver no sólo con ataques terroristas, desastres naturales, actos vandálicos, intrusiones no controladas, virus informáticos, interrupciones del suministro eléctrico o los inevitables errores humanos, sino también con la gran

interdependencia que existe entre los datos, los sistemas informáticos y de comunicación y el funcionamiento y el negocio de las empresas.

Los imprevistos son parte de la vida personal o de grupo, por lo que, es necesario estar preparados para poder prevenirlos, distinguirlos y planificarlos antes, durante y después del evento, para tener el menor impacto posible tanto en humanos como en bienes físicos; tomando acciones para enfrentar posibles riesgos, ya sea de origen natural o humano, con la finalidad de recuperar y restaurar todas sus principales funciones de forma parcial o total en el caso de existir interrupciones no esperadas. El presente trabajo busca demostrar que cualquier administración debe contar con una planificación, constante actualización y capacitación del personal adecuada y probada para brindar confianza a los clientes internos y externos, en el caso de los departamentos de Tecnología de la Información que son los que cuentan con las herramientas y servicios tecnológicos sobre el que giran grandes volúmenes de información y servicios.

Bajo este aspecto, es importante identificar los problemas que generen disrupción en relación a un sistema de información, es decir, fallos en la operatividad informática y de servicios que pueden suscitarse por el inadecuado manejo de un plan de continuidad. Es así que el departamento de las tecnologías de la información de la empresa EP-EMAPA-A, desde el año 2014 detectó los problemas vinculados a los resultados en base a una auditoria informática, destacando que la principal deficiencia se centró en la falta de organización, desarrollo en información y administración técnica dentro del departamento se promovía una baja calidad en los servicios prestados hacia los clientes internos, limitando la rapidez de atención al cliente externo. La EP-EMAPA-A., necesita manejar y respaldar los procesos para incrementar las posibilidades de recuperación de tal forma que su vida institucional se prolongue en el tiempo.

La ausencia de planificaciones para solventar cualquier tipo de inconvenientes que surjan dentro de la empresa pone en riesgo la satisfacción del cliente, que en la era tecnológica actual requieren de una atención oportuna y adecuada y siendo el departamento de TI el eje de la administración de los sistemas informáticos y comunicaciones es requisito indispensable garantizar la continuidad del servicio al usuario interno y externo.

El no contar con un modelo planificado para la continuidad de servicios del departamento de TI no garantiza la atención permanente que los usuarios requieren en la época tecnológica que vivimos, por lo que se necesita de estrategias de continuidad en los sistemas informáticos y de comunicaciones. La falta de capacitación del personal que debe intervenir en los procesos de recuperación ante cualquier crisis natural o humana, impide que los sistemas puedan reponerse de una forma ágil y oportuna, dando como consecuencia un caos en el manejo de responsabilidades para dirigir cada proceso que permita volver a la normalidad en atención de los usuarios interno o externos. Se origina en la administración por la falta de experiencia en la recuperación de crisis, ya que no se puede saber cuándo se presentarán eventos excepcionales, por lo que se debe planificar un modelo que permita diseñar un plan de continuidad de los servicios del departamento de tecnologías de la información, además la capacitación permanente para que las personas involucradas directa o indirectamente tengan clara la forma de actuar en el caso de presentarse algún tipo de incidente.

En la administración de la empresa, en las agencias de atención al usuario y en el departamento de Tecnologías de la Información de la EP-Empresa Municipal de Agua Potable y Alcantarillado de la ciudad de Ambato que atiende a los usuarios internos y externos.

Objetivo general

Diseñar un plan de continuidad de servicios para el departamento de tecnologías de información de la EP-Empresa Municipal de Agua Potable y Alcantarillado de la ciudad de Ambato.

Objetivos específicos

1. Fundamentar teóricamente aspectos relacionados a las TI, en base a un plan de continuidad de servicios, mediante la recopilación de la información para ser sustentados.
2. Diagnosticar la situación actual de la EP-EMAPA para afrontar situaciones de riesgo en los servicios que se ofrece a los clientes externos.
3. Determinar la metodología empleada en el desarrollo de las tecnologías de la información para la gestión de un plan de continuidad de servicios.
4. Proponer la legalización del plan de continuidad de servicios del departamento de TI de la EP-EMAPA en casos excepcionales.

Justificación

El presente trabajo implica el diseño del plan de continuidad que permita brindar los servicios, en caso de una crisis, de forma normal a los usuarios internos y externos del departamento de tecnologías de la información de la empresa EP-EMAPA-A, llegando inclusive a la implementación de los procedimientos necesarios para prevenir el mayor número de posibles eventos excepcionales.

¿Qué será capaz de hacer el producto final del trabajo de titulación?

El plan de continuidad de servicios del departamento de tecnologías de la información logrará:

- Conformar un comité de crisis.
- Diseñar un modelo de gestión para la continuidad del servicio que presta el departamento de Tecnologías de la Información de la EP-EMAPA-A.
- Desarrollar un plan de capacitación para todo el personal de la EP-EMAPA-A.
- Reducir los tiempos de respuesta a los desastres mediante simulacros continuos
- Contribuir en la identificación de los puntos críticos dentro de la oficina matriz como en las agencias.
- Aplicación de herramientas informáticas para prevención de fraudes internos como externos.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.2. Definiciones y conceptos

Las tecnologías de la información, corresponde al uso de equipos de contenido de un sistema informático que permite clasificar, ordenar, controlar y planificar las actividades que realiza una empresa, en relación al servicio que ofrece a un determinado grupo de clientes con el propósito de flexibilizar y optimizar el tiempo mediante las diferentes actividades que son establecidas a través de un departamento específico, que busca minimizar la probabilidad y problemas técnicos para ser integrados en los planes de recuperación de desastres para proteger contra la principal pérdida de los servicios de tecnologías de la información y continuar con el funcionamiento.

Además, la información es considerada como uno de los recursos más valiosos para cualquier tipo de empresa, sin importar el sector económico al cual pertenezcan las decisiones más importantes y acertadas se toman con base a la información que contenga cada una de las mismas; adoptando medidas y planes que mitiguen el impacto ante cualquier incidente o riesgo.

De acuerdo con la Organización de las Naciones Unidas para la Educación, la Ciencia y Cultura "UNESCO" (2013) considera que los especialistas han optado en denominar a la humanidad como la sociedad del conocimiento porque no está enfocada únicamente en las innovaciones y avances tecnológicos, sino en el derecho de todas las personas, comunidades y pueblos de poder crear, consultar, utilizar y compartir la información y el conocimiento para fortalecer e incrementar las posibilidades de desarrollo y la calidad de vida de forma sostenible. Como ejemplo de la dependencia tecnológica, podríamos imaginar una empresa a nivel nacional que presta servicios a múltiples empresas en todo el territorio; y, que ante una descarga eléctrica ocasionada a un transformador de la zona pierde toda la información del sistema de ese día en particular, siendo temporada alta de grandes transacciones. Seguramente comenzaría a recibir, cientos de llamadas de clientes consultando por las fallas al sistema de seguimiento de guías en tiempo real o retrasos en los tiempos acordados de entregas, etc.

Bajo este aspecto, se menciona el trabajo investigativo de Torres (2014) en donde desarrolla un "Diseño y propuesta de implementación de un plan de continuidad del servicio aplicable a los hospitales en la ciudad de Bogotá"; en el cual concluyen que;

La infraestructura tecnológica, información en medios digitales y el software especializado son parte fundamental para su normal y correcto funcionamiento, sin embargo, no implementan planes ni estrategias que respalden los activos, permitiéndose proteger las actividades claves de la cadena de valor, debe ser tratada de manera prioritaria y en lo posible a corto plazo; esto teniendo en cuenta que existen riesgos o desastres naturales en la localidad. (p. 143)

Para Ferrer (2014), indica que En el caso de ITIL, dentro del ciclo del diseño de los servicios de TI, la gestión de continuidad de los servicios de TI, se menciona la política y alcance, análisis de impacto, evaluación de riesgos, estrategias, organización y planificación. Se recalca la importancia de contar con un sitio alterno, en vista a la supervisión de la continuidad del negocio. (p. 34)

Un estudio proporcionado por el Consejo de Preparación para la Recuperación de Desastres el 04 de marzo de 2014, realizado por Council (2014) describe que el 73% de las empresas no están preparadas para la recuperación de desastres; y, las malas prácticas de recuperación de desastres han provocado pérdidas de hasta $5 millones. “Se aplicó una encuesta en algunas organizaciones cuyos, resultados fueron que no se tomaron las medidas adecuadas a favor de la protección de su información y sistemas TI, ya que existe una deficiente planificación, nulidad en pruebas y deficiencias tecnológicas”. (p. 49)

En el trabajo investigativo de Carrizo (2016) menciona la implementación de una variante del modelo de continuidad de negocio, el objetivo es presentar una variante del modelo *Business Continuity Institute* (BCI), a través de un caso de estudio misma que concluye;

Un plan de continuidad de negocio es clave para asegurar que una empresa puede protegerse contra los riesgos que son inherentes a su entorno y poder continuar con sus funciones, las empresas son cada vez más dependientes de la disponibilidad y resguardo de información con el fin de prestar servicios a los clientes. (p. 102)

A partir de los años setenta se inicia el proceso de desarrollo de las nuevas tecnologías de la información y comunicación, mejor conocidas como TIC´s. El desarrollo de estas tecnologías ha producido cambios sustanciales en la forma de vida de la gente, en cómo aprenden, su manera particular de trabajar y de facilitar su comunicación, al punto de que en la actualidad los servicios de generación, almacenamiento, procesamiento y

distribución de todo tipo de información se han convertido en el mayor generador de riqueza y puestos de trabajo a nivel mundial.

En el estudio de Correa (2018) destaca que con el paso del tiempo las empresas centran las ideas por aplicar un plan de continuidad que garantice la recuperación de la información en base a un siniestro o actividades de contingencia para las operaciones en los sistemas. “Algunas empresas estadounidenses aplicaron un sistema denominado *Sungard 7 Availability Systems*, fue uno de los primeros proveedores de recuperación de desastres de centros de datos y actualmente es uno de los más importantes proveedores de servicios de producción de TI”. (p. 118)

En los años ochenta y noventa las empresas se recuperaron ante desastres tecnológicos, en vista de la implementación de un plan de continuidad de forma sistémica dentro de la organización. Méndez (2019) opina “Las empresas se dieron cuenta que tener alguna interrupción de TI traería un impacto negativo en la continuidad de las operaciones que afectan al negocio y sobre todo en los procesos críticos. (p. 72)

Con el avance de la tecnología y la adopción estratégica del internet en las empresas de servicio se tornaron más dependientes a la aplicación de un sistema informático, (Portillo y Martínez (2019) mencionan que:

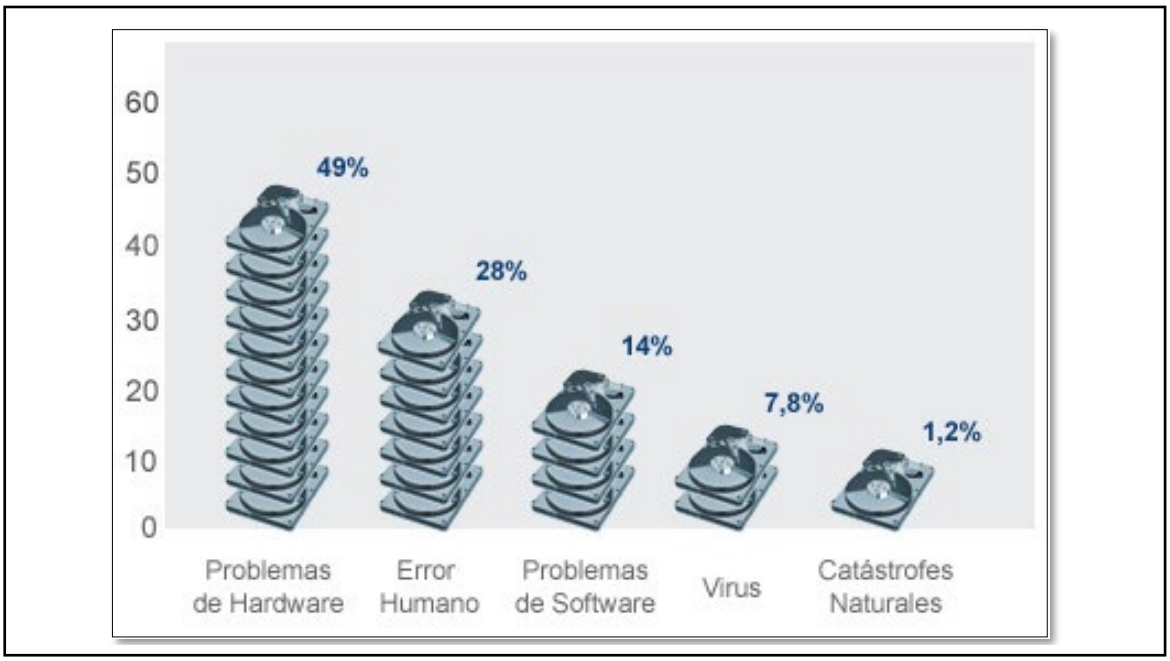
Un plan de continuidad de servicios críticos de TI engloba todas las funciones y recursos que busca identificar, analizar y evaluar riesgos de posibles amenazas para luego elaborar estrategias que permitan minimizar las caídas y paralización de operaciones de los sistemas informáticos en las organizaciones. Es un elemento clave dentro del gran escenario de la continuidad del negocio. (p. 54)

Sin embargo, contar con un plan de continuidad en las empresas requiere de la preparación organizacional para enfrentar alguna eventualidad, incertidumbre, disrupción, con el propósito de garantizar la provisión de servicios, salvaguardando los intereses de los colaboradores o clientes internos, en base a las actividades que generan valor al tiempo y trabajo empleado. Para garantizar las tecnologías de la información se puede adoptar en el plan de continuidad la norma ISO 22301 al igual que las otros modelos que se encontrán más adelante en el diseño del plan, también está basada en el modelo PDCA (Plan – Do – Check – Act) referente a la planeación.

En la investigación de Ochoa (2019) considera que: “Un plan integra establecimiento, implementación, operación, monitoreo, revisión, ejercicios, mantenimiento y mejoramiento de la efectividad para la continuidad de servicios en una organización y la gestión de continuidad preparare a la empresa a responder y recuperarse oportunamente de interrupciones”. (p.28)

Por tanto, es necesario que un plan de continuidad de servicios sea el mecanismo de acción para las TI que sirve para actuar frente a desastres y permita valorar las causas y el impacto que pueden tener y poner en marcha un Plan de Recuperación de Desastres (DRP). Se puede identificar varias causas que podrían afectar el normal desenvolvimiento de las actividades en el Departamento de Tecnologías.

Figura N° 1. Principales factores que causan pérdida de información



Fuente: (Recovery Labs, 2016)

En la gráfica anterior se representan los principales factores que causan las pérdidas de la información, donde se determina que el 49% son los problemas de hardware como los principales en los departamentos de la tecnología de las empresas, considerando fallos en discos, en memorias, en las tarjetas madre, etc. Así mismo el 28% menciona que los errores humanos son los causantes de la pérdida de la información, como por ejemplo accesos no autorizados, fallas fortuitas, negligencia o ataques intencionales. Otro de los puntos a considerar es el problema de software con un grado porcentual del 14%, en el

caso de programas desarrollados, contratados o comprados para el funcionamiento dentro de la empresa, mientras que el 7.8% indica que los virus son un factor causante del deterioro de datos y por último el 1.2% señala que las catástrofes naturales como otro de los factores que ocasionan la pérdida de la información.

Fallos en el suministro eléctrico. - *Benchmark*, (2013) menciona que una de las principales causas señaladas por una gran cantidad de organizaciones como desencadenante de eventualidades no programadas en los sistemas de información, es algo tan cotidiano como un fallo en el suministro o la red eléctrica. Al menos, esto es lo que afirmaron el 43% de las empresas encuestadas para la elaboración del informe *Global Disaster Recovery Preparedness*, publicado por la consultora Forrester en el año 2013.

Fallos en el *hardware* y los sistemas de almacenamiento. – Rodriguez (2016) considera que se dispone de varios niveles de redundancia en componentes críticos, tales como controladores de red o múltiples fuentes de alimentación, es posible que exista una sensación de mayor protección. Aun así, los fallos en la SAN (*Storage-Area Network*) o Red de Almacenamiento figuran entre las principales causas de desastres entre las organizaciones. Con frecuencia, las empresas cuentan con una amplia red de almacenamiento y todos los servidores virtuales dentro de ésta.

Fallos humanos. – Gilart (2016) opina que el error humano también es una causa señalada en el 13% de los casos de desastres de TI. La casuística entre los errores humanos es muy variada. No obstante, el borrado accidental de un sistema de archivos de un servidor es una de las causas más comunes, tanto entre novatos, como expertos de TI de consumada experiencia. Las salvaguardas utilizadas para advertir a los usuarios del borrado o sobre-escritura de archivos son frecuentemente ignoradas por éstos. Cuando se trata de información crítica, la ausencia de un sistema de backup y recuperación de datos se convierte en una dolorosa situación.

Fallos de software. - Gilart (2016) identifica la principal razón que subyace detrás de los fallos de software es la falta de supervisión y comprobación de los parches y actualizaciones que éstos reciben. Esto puede dar lugar a la corrupción de determinadas aplicaciones y la consiguiente caída de los sistemas. Por otro lado, el uso de sistemas operativos anticuados y con un deficiente mantenimiento también está detrás de muchos de los fallos de software que desencadenan un desastre de TI.

Ataques maliciosos y virus informáticos. – Gilart (2016) enfatiza que los fenómenos son mucho menos confirmados que los señalados anteriormente. El problema radica en las consecuencias de los mismos. Si el hecho de sufrir un desastre de los sistemas de información supone una gran pérdida de credibilidad y confianza por parte de los clientes, hacerlo como consecuencia de un ciber-ataque suele ser mediáticamente terrible. Por otra parte, conviene tener en cuenta que estos ataques pueden tener su origen tanto en el exterior de una organización, como en el interior, con independencia de la voluntad maliciosa de los empleados. Finalmente, no podemos olvidar que la presencia de virus, *malwares* y *ransomware's* también es un constante y creciente problema que amenaza la operatividad diaria de muchas organizaciones. El mayor problema de este tipo de infecciones digitales es que los archivos pueden parecer intactos hasta el momento en que se intenta acceder a ellos.

De acuerdo con Marroquín (2015) describe el estudio denominado *Forrester Research* y *Disaster Recovery Journal*, en base al entorno de la continuidad del servicio, que se centra en la madurez y preparación de la continuidad de negocios con el fin de recopilar datos para la comparación y evaluación comparativa de empresas con lo que se orienta la investigación y se publique las mejores prácticas y recomendaciones:

La misma que se realizó por primera vez en 2009, posteriormente en 2012 y en 2015. IBM ha realizado un estudio a nivel internacional sobre los sectores que sufren más interrupciones en las actividades de negocio debido a desastres. Banca y Finanzas, con un 26 por ciento; Gobierno, Administraciones Públicas e Instituciones (19 por ciento) y Educación (11,3 por ciento) se sitúan en las primeras posiciones, seguidos por Industria (10,9 por ciento), Servicios (9,5 por ciento) y Comunicaciones (8,2 por ciento). Un estudio del *Disaster Recovery Institute* aporta que, el 90 por ciento de las empresas que tienen pérdidas significativas de datos quiebran en el plazo de tres años. El 40 por ciento de las empresas que sufren un desastre no vuelve a abrir nunca y el 60 por ciento cierra en los siguientes tres años. (p. 83)

Morales (2017) enfatiza un informe de la firma de analistas *Enterprise Strategy Group* indica que el mercado contaba con un promedio del 30 por ciento de fallos en copias de seguridad y de un 50 por ciento en restauración de archivos. Al realizar el estudio, muchos departamentos de TI reconocían no estar seguros de ser capaces de recuperar todos los datos críticos de negocio y si se podía realizar en un tiempo aceptable. Una encuesta

realizada por *Freedom Dynamics* entre más de 700 directivos de TI europeos, establecía que la pérdida de datos críticos para el negocio y el tiempo de actividad de los sistemas clave de TI son dos de los mayores riesgos a los que se enfrentan los responsables de Tecnologías de la Información a la hora de planificar. (p. 76)

Durante un discurso destacado en la Conferencia *VivaTech* en París; Partinez (2014) presidenta y CEO de IBM, *Ginni Rometty*, convocó a la industria de tecnología para ayudar a construir un futuro mejor. Para ello, comprometió la aplicación de tecnología de IBM y una inversión de USD $30 millones en un plazo de 5 años en la Iniciativa anual *Global Call for Call* con el objetivo de unir a los desarrolladores del mundo y aprovechar las tecnologías de datos e inteligencia artificial, *blockchain, cloud* e internet de las cosas (IoT), para abordar desafíos sociales. “En IBM aprovechamos el poder de las tecnologías como IA, blockchain, IoT y cloud para abordar algunas de las mayores oportunidades y desafíos en los negocios", dijo Bob Lord, Chief Digital Officer de IBM. "Ahora, con Call for Code, estamos llamando a todos los desarrolladores para unirse a nosotros y utilizar estas mismas tecnologías de vanguardia para ayudar a las personas, a sus comunidades y la sociedad". (p.35)

A través de *Call for Code*, IBM y *David Clark Cause* están uniendo fuerzas con la Oficina de Derechos Humanos de la ONU y con su enfoque de la acción humanitaria, basado en los derechos humanos, que se enfoca en garantizar la participación de los grupos afectados en los esfuerzos de preparación, respuesta y recuperación. Dirige la atención a las poblaciones más excluidas y marginalizadas y a los que están en riesgo de sufrir violaciones a sus derechos humanos.

“La tecnología puede ser una fuerza potente para promover los derechos humanos y construir sociedades más equitativas. Call for Code es una oportunidad excelente de explorar cómo la tecnología puede tener un papel en abordar las necesidades de las poblaciones más vulnerables y de los que están en riesgo de sufrir violaciones a sus derechos humanos, en el contexto de una crisis humanitaria”, señaló Laurent Sauveur, Director de Relaciones Exteriores de la Oficina del Alto Comisionado para los Derechos Humanos de la ONU Sauveur (2016) sobre la investigación en el desarrollo e implementación de un plan de recuperación del desastre cualquiera que sea la fuente a través de la aplicación de los procesos que se encuentran en el plan de continuidad del servicio del departamento de tecnologías de la información, además de contar con un plan

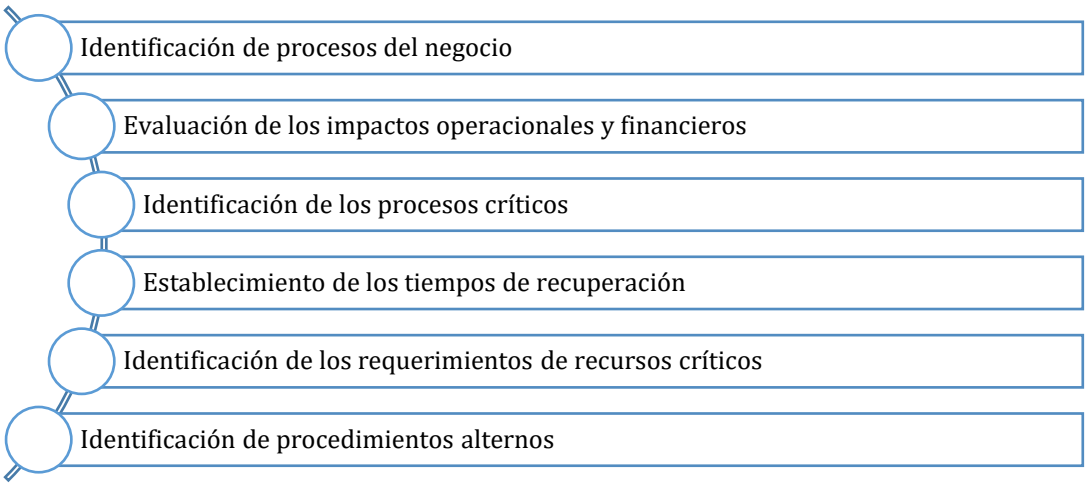
de actualizaciones, simulacros con la participación del personal a cargo de los procesos y la dirección que conforma un comité dentro de sus funciones. (p. 46)

Una vez que se ha determinado los procesos que intervienen dentro de una amenaza o un posible desastre, se reconoce los siguientes aspectos que deben ser tomados en cuenta dentro de cualquier institución para disminuir al máximo posible el impacto.

1.2.1. Análisis de impacto en el negocio (BIA)

Previamente es necesario evaluar el impacto que generará en el negocio los riesgos identificados, dentro de los procesos que lleva el departamento de TI dentro y fuera de la empresa. Para dar cumplimiento al análisis debemos considerar las siguientes etapas mostradas en la figura 2:

Figura N° 2. Metodología del análisis del impacto del negocio (BIA)



Fuente: (MINTIC, 2015)

Al final de socializarse esta fase se recomienda realizar un informe con el detalle de las funciones y procesos críticos del servicio. Este documento debe contener la información básica de los recursos requeridos y los tiempos de recuperación para que las entidades puedan poner en funcionamiento los servicios y por ende la continuidad del servicio del negocio. El análisis de impacto del negocio, consiste en definir una serie de pasos interactivos con el objetivo de identificar claramente los impactos de las interrupciones y tomar decisiones respecto a aquellos procesos que se consideran críticos para la organización y que afectan directamente el negocio ante la ocurrencia de un desastre, estos pasos se muestran en la figura 2.

a) Identificación de procesos del negocio

En este paso se identifican las funciones de la dependencia del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de la Entidad. Así mismo, su resultado generar un listado de roles y procesos, que sirven de análisis para el cumplimiento de los siguientes pasos del BIA.

b) Evaluación de los impactos operacionales y financieros

Teniendo en cuenta los elementos operacionales de la organización, se requiere evaluar el nivel de impacto de una interrupción dentro de la Entidad. El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C representados en el Cuadro N° 1.

En la tabla No. 1 se muestra un ejemplo con los niveles de criticidad en una empresa, que contempla un sistema de tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema; por lo tanto, la tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo.

Tabla N° 1. Niveles de criticidad en una Entidad

Categoría	Proceso (Servicios)	Nivel	Tolerancia	Descripción
Aplicaciones	Sistema de Control de flujo de documentos	B	3	Contenedor de aplicaciones
Web	Sitio web Entidad	A	1	Capa de presentación
Base de Datos	SQL nómina	A	1	Contenedor de aplicaciones en SQL
Seguridad de Información	Firewall	A	1	Servicio de *firewall* de la Entidad
Sistemas de Almacenamiento	SAN (Storage Área Network)	A	3	Capacidad de almacenamiento en SAN
Comunicaciones	Acceso Local a Internet	C	4	Comunicación de Internet del usuario local
Cuartos de Máquinas	Centro de datos	A	1	Servicio de Centro de datos de la Entidad
Proveedores de Aplicaciones y/o comunicaciones	Interno/externo	B	2	Desarrollo Interno o contratado por externos. Canales de comunicaciones
Recursos humanos	Interno/externo	C	3	Profesionales encargados de administrar las infraestructuras de la Entidad

Fuente: (MINTIC, 2015)

c) Identificación de los procesos críticos

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según esta tabla No. 1.

Cuadro N° 1. Identificación del proceso critico

Valor	Interpretación del proceso crítico
A	Crítico para el Negocio, la función del negocio no puede realizarse
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

Fuente: (MINTIC, 2015)

d) Establecimiento de los tiempos de recuperación

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA. Los tiempos de recuperación se describen a continuación en el cuadro N° 2:

Cuadro N° 2. Descripción de tiempos de recuperación

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Fuente: (MINTIC, 2015)

Una vez identificados los procesos críticos del negocio, función que hace parte del análisis de los impactos operacionales, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio). Esto quiere decir que si por ejemplo un proceso tiene un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a otros que tienen mayor tolerancia.

e) Identificación de los requerimientos de recursos críticos

Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto, es clave en este punto, la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto del negocio de las Entidades. Se representa un ejemplo de identificación de recursos críticos de Sistemas de Tecnologías de Información en el Cuadro N°3.

Cuadro N° 3. Identificación de recursos críticos de sistemas TI

Categoría (Función Crítica del Negocio)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistemas TI
Aplicaciones	Sistema de nómina	• Sistema de entrada de novedades administrativas. • Interfaces con el Sistema Financiero.
Seguridad de Información	*Firewall*	• Reglas de entrada y salida de puertos. • Reglas NAT/PAT. • Direccionamiento IP público.
Comunicaciones	Servicio WiFi	• Control de identificación usuarios con Portal Cautivo. • Control de usuarios locales Vs Invitados.
Cuartos de Máquinas	Centro de Datos	• Control de operaciones de Servidores, Equipos de Comunicaciones, Sistemas de Almacenamiento, Sistemas de *Backups*, Aire Acondicionado, Acometida Eléctrica.

Fuente: (MINTIC, 2015)

f) Identificación de procedimientos alternos

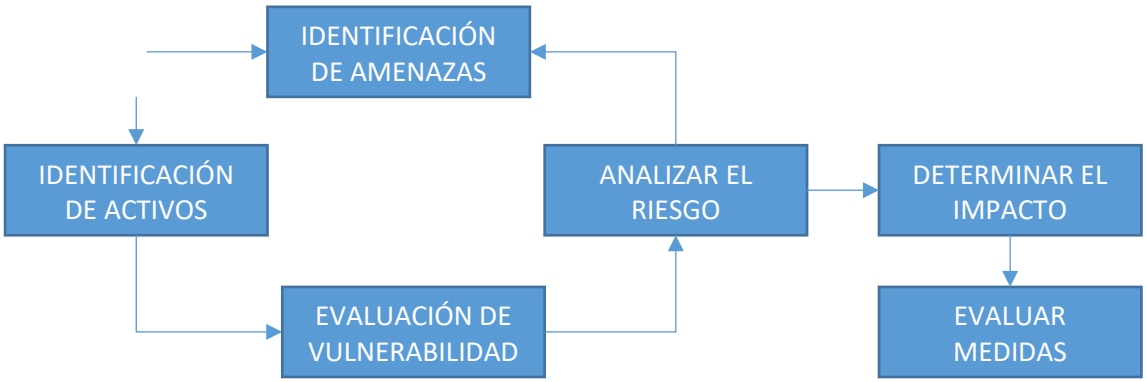
La identificación de procesos alternos hace posible que los procesos del negocio puedan continuar operando en caso de presentarse una interrupción; para ello es oportuno que las entidades tengan métodos alternativos de manera temporal que ayuden a superar la crisis que ha generado una interrupción; por lo tanto, para cada proceso crítico que se establezca (en los servicios), se debe poseer un procedimiento manual de continuidad del servicio.

g) Análisis de riesgos

Dentro del análisis del riesgo que se desarrolla, en el plan de continuidad se permite conocer los riesgos y gestionarlos de forma adecuada. Existen diferentes metodologías de riesgo (*NIST, MAGERIT, OCTAVE*, etc.) que pueden aplicarse para realizar el análisis de riesgos.

Ochoa (2013) menciona que la evaluación de riesgos puede plantear si se verá afectado en base al coste estimado, por tanto, se tendrá en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. “De esta forma, se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado”. (p. 56)

Figura N° 3. Esquema del análisis del riesgo



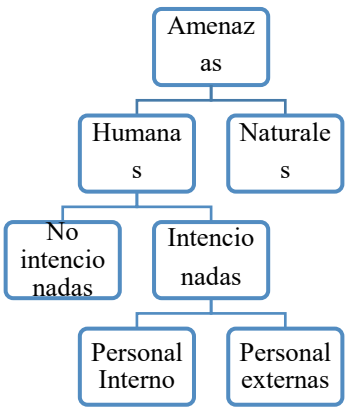
Fuente: (Ochoa M. J., 2013)

h) Identificación de amenazas

Las amenazas se definen como un suceso imprevisto que desencadenan incidentes en las empresas entre ellos daños materiales y pérdidas en los servicios. Ochoa (2013) opina que. “Al analizar los riesgos hay que evaluar las distintas amenazas que pueden provenir de diversas fuentes. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y catástrofes”. (p. 34)

La siguiente ilustración clasifica las distintas amenazas a los sistemas:

Figura N° 4. Principales amenazas a los sistemas



Fuente: (Ochoa M. J., 2013)

De acuerdo con la organización y el proceso analizado, serán aplicables distintos tipos de amenazas. Estas mismas tendrán una probabilidad de ocurrencia que dependerá de la existencia de una vulnerabilidad que pueda ser explotada, para materializarse en un incidente. Por ejemplo, una amenaza de tipo de desastre natural que tiene la empresa como; temblores, terremoto; erupciones volcánicas; Incendios; estos mismos deben estar valoradas en la probabilidad de ocurrencia de una amenaza, resulta más complicado valorar las amenazas humanas (ataques maliciosos, robos de información, etc.), que las amenazas naturales.

En el componente humano existen dos factores a tener en cuenta:

AMENAZA= CAPACIDAD X MOTIVACIÓN

La motivación es una característica humana que es difícil de valorar, pero que, sin embargo, es un factor a considerar: empleados descontentos, exempleados. Mientras que las amenazas corresponden a los factores externos que pueden afectar a la infraestructura entre ellos desastres naturales, daños accidentales y ataques intencionados.

i) Vulnerabilidades

Las vulnerabilidades se consideran como impotencias en la explotación de convertir las amenazas en un posible riesgo real que pueden causar daños graves a la empresa. Las vulnerabilidades son incertidumbres de ser causantes o no de algún daño más bien, se considera como una condición a un conjunto de acondicionamientos que pueden causar afectaciones a los activos de la empresa.

Tomando como base los objetivos de seguridad de la Norma ISO 27002 “Código de Práctica para la Gestión de la Seguridad de la Información” y en función de las Amenazas que hemos marcado como posibles, establecemos los escenarios en que una amenaza puede convertirse en un incidente de seguridad.

Cuadro N° 4. Vulnerabilidades

ESCENARIOS	NIVEL DE PROTECCIÓN	RESPUESTA
1. Inundación del centro de proceso de datos	¿El centro está situado en un terreno alto?	SI
2. Fallos del suministro Eléctrico.	¿Existen Unidades de suministro eléctrico alternativo (UPS)?	NO
3. Pérdida de información clave de la compañía.	¿Se realizan copias de seguridad de los datos periódicamente?	No periódicamente
4. Accesos no autorizados al edificio	¿Existe un control de acceso físico a los edificios de la compañía?	SI
5. Robo de datos	¿Existe una clasificación de la información adecuada al nivel de confidencialidad de los datos?	NO
6. Pérdida de servicios por infección de virus	¿Están los equipos protegidos por un antivirus?	NO

Fuente: Elaboración Propia

j) Evaluación del riesgo

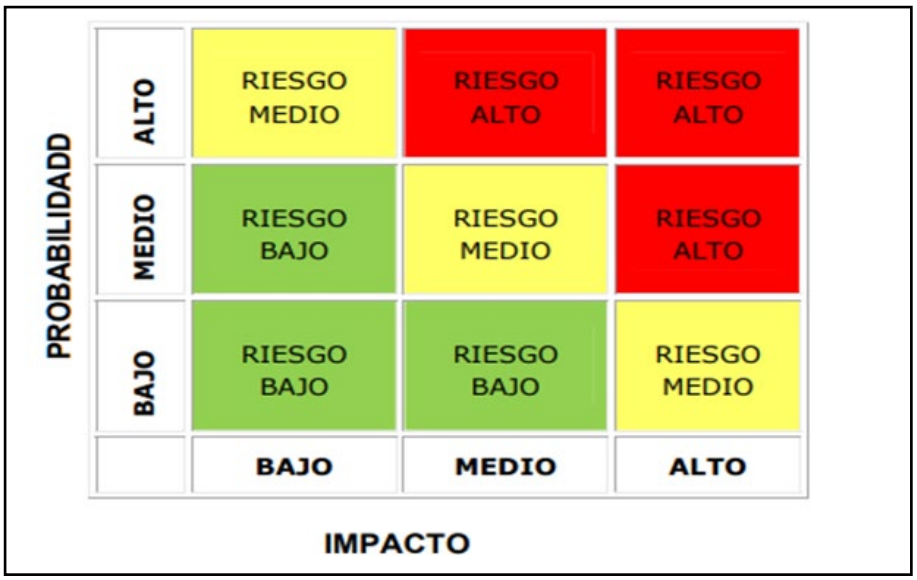
El riesgo es la posibilidad de que se produzca un impacto determinado en la organización. El riesgo calculado es simplemente un indicador ligado al par de valores calculados de vulnerabilidad y el impacto, ambos ligados a su vez de la relación entre el activo y la amenaza a la que el riesgo calculado se refiere.

PROBABILIDAD DE INCIDENTES= AMENAZA X VULNERABILIDAD

RIESGO= PROBABILIDAD DE INCIDENTES X IMPACTO

El riesgo suele expresarse en términos cualitativos (Alto, Medio, Bajo). A continuación, se muestra un ejemplo de una matriz de probabilidad/impacto basado en la Norma INEN ISO/IEC 27005.n

Figura N° 5. Matriz de riesgos



Fuente: (Ochoa M. J., 2013)

La probabilidad de ocurrencia (no existan vulnerabilidades) y el impacto sobre la compañía sea también bajo, estaremos en un nivel de riesgo bajo. Sin embargo, si existen vulnerabilidades que aumentan la probabilidad de ocurrencia o el impacto del incidente sea alto para la empresa estará en unos niveles de riesgo medio-alto.

1.2.2. Plan de contingencias (CP)

Nippon (2017) opina sobre el plan de contingencias permitirá contrarrestar y/o evitar los efectos generados por la ocurrencia de emergencias, ya sean eventos asociados a fenómenos naturales o causados por el hombre, los mismos que podrían ocurrir durante la construcción y operación del proyecto.

El Plan de contingencias deberá estar disponible en un lugar visible para que todo el personal pueda acceder a él, así mismo al finalizar cada jornada se deberá evaluar los tipos de riesgos que se hubiesen generado durante las actividades, con la finalidad de adaptar y/o complementar las acciones correspondientes. (p. 38)

Las contingencias se refieren a la ocurrencia de efectos adversos sobre el ambiente por situaciones no previsibles, de origen natural o antrópico, que están en directa relación con el potencial de riesgo y vulnerabilidad del entorno. Estas contingencias, de ocurrir, pueden afectar el proceso, la seguridad de las tareas, la integridad o salud del personal y la calidad ambiental del área de influencia. Este plan prepara las actividades que comprende la elaboración de los procesos de facturación y recaudación, el cual deberá ser

actualizado en la medida que se definan nuevos procesos o tareas no especificadas hasta el momento.

1.2.3. Plan de Continuidad del Servicio (BCP)

Hernández y Galeano (2016) consideran que un *Bussines Impact Analisys* (BIA) determina las funciones o procesos de negocios críticos y necesarios, sus dependencias o recursos, e identifica aplicaciones informáticas claves para el negocio, estima el impacto financiero y operacional de una interrupción y el marco de tiempo de recuperación necesario para las funciones críticas del negocio. El BIA proporciona a la organización las bases para desarrollar un plan de continuidad de negocio. (p. 56)

Balladares (2018), define al "Plan de continuidad del negocio (PCN) como una herramienta que mitiga los recursos del sistema de gestión de riesgo operacional. Así como elementos de control la prevención y atención a emergencias, gestión de crisis, planes de contingencia y capacidad de retomar operaciones" (pág. 65).

El PCN es el documento que permite que la Clasificadora asegure que los objetivos de la continuidad del negocio se cumplan, sean medibles y consistentes con las políticas, de igual forma como con las normativas regulatorias y legales que le sean aplicables. En este documento se definen y determinan las responsabilidades y quienes estarán a cargo, planes de acción, recursos para su adecuada gestión, control, supervisión y mejoramiento.

Un plan de continuidad del servicio, implica que una buena realización e informe del análisis de impacto sobre el negocio proporcione a la organización o alta dirección un entendimiento común de las funciones que son críticas para su supervivencia, así como la información necesaria para la toma de decisiones en el desarrollo de estrategias que se fundamenta en el desarrollo de un plan de continuidad del negocio, lo que implica que una buena realización e informe de BIA conlleva a entregar a la dirección la información necesaria para la toma de decisiones asertivas.

- **Estrategias de continuidad**

Una estrategia de continuidad puede ser considerada como un mecanismo que permite la recuperación y continuidad de las funciones críticas de una organización frente a un desastre o una interrupción mayor. Siendo estrategias no sólo los recursos y actividades

requeridas frente a la interrupción del servicio, sino los que se necesitan para mitigar la probabilidad de ocurrencia y el impacto en caso de suceder.

Las estrategias de continuidad posible o viable, de manera efectiva y eficiente, son las que cuentan con un entendimiento sobre los siguientes aspectos que se señalan en la figura 3:

Figura N° 6. Estrategias de continuidad

1. Resultados del Análisis de Impacto al Negocio (BIA).
2. Tiempos y puntos objetivo de recuperación (RTO y RPO) requeridos para los procesos críticos.
3. Procesos críticos a soportar
4. Porcentaje aceptable de degradación de la operación del proceso.
5. Aspectos de carácter jurídico que se deben cumplir según la naturaleza del proceso al momento de implementar una estrategia de recuperación.
6. Resultados del análisis de riesgos y las alternativas de tratamiento de riesgo a implementar sobre los activos asociados a los procesos.
7. Amenazas posibles a los activos de los procesos.
8. Vulnerabilidades existentes en los activosde los procesos.

Fuente: (Oficina de Sistemas e Informática , 2018)

El propósito de esta fase consiste en seleccionar las estrategias de recuperación o continuidad, orientadas a brindarle confiabilidad a los servicios, considerando los resultados del BIA, la evaluación de riesgos y complementado lo anterior, con la realización de un análisis cuantitativo de los elementos requeridos para la recuperación.

1.2.4. Plan de Recuperación de Desastres (DRP)

De acuerdo con Arévalo (2016) menciona que un plan de recuperación de desastres (DRP) está diseñado como lista de comprobación o instructivo de trabajo en caso de la materialización de un escenario de desastre a nivel de infraestructura. En él, se describen las estrategias, los recursos, los procesos y los procedimientos que los equipos de recuperación de desastres que la dirección de informática y tecnología, utilizará para cualquier incidente o acontecimiento imprevisto.

Este DRP busca dar los lineamientos para conseguir las metas que se observan en la figura 4:

Figura N° 7. Metas para plan de recuperación de desastres

A. Disponer de un plan de acción organizado, para atender una interrupción inesperada en los servicios críticos ofrecidos por la Dirección de Tecnologías de la Información.

B. Prestar una oportuna continuidad en los servicios tecnológicos de la Dirección de Tecnologías de la Información, en caso de presentarse una situación de contingencia mayor o catastrófica.

C. Establecer la coordinación de actividades y comunicación interna y externa, adecuada, entre los líderes de la Dirección de Tecnologías y los usuarios de servicios de tecnología finales.

D. Recuperar las aplicaciones críticas del servicio de una manera oportuna, incrementando la habilidad de la empresa para recuperarse de una pérdida o daños a las instalaciones y servicios.

E. Administrar exitosamente los eventos de desastre, minimizando el impacto al servicio.

Fuente: (Arévalo, 2016).

La protección de datos se enmarca bajo la entrega del *Desaster Recovery Plan* (DRP), a terceras partes que no pertenecen a la dirección de tecnologías, se entregará una copia del mismo en la que no se incluyan datos de carácter personal de los miembros de los equipos de recuperación ni de ningún otro participante en el DRP. Si se requiere comprobar que los miembros están definidos se puede invitar a una tercera empresa a visualizar una copia del DRP desde un computador del sistema de información del departamento, sin permitir ningún tratamiento sobre los datos personales ni el contenido del mismo. De igual manera se tratarán los datos confidenciales de sistemas, configuraciones, contraseñas y dirección IP de las redes, etc.

DRP se enfoca en la recuperación del servicio de TI y los recursos, dado un evento que ocasionara una interrupción mayor en su funcionamiento y tiene las siguientes etapas:

- Desarrollo de un reglamento de políticas de planificación de contingencias.
- Análisis del impacto en la empresa (BIA) sobre el negocio, es determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto. Este proceso es parte fundamental dentro de la elaboración de un plan de continuidad de servicios

- Identificación de los controles preventivos, para reducir los efectos de las interrupciones del sistema pueden ayudar a incrementar la disponibilidad del sistema y reducir los costos de los ciclos de vida de las contingencias
- Especificación de las Estrategias de desarrollo de la recuperación a través de las estrategias de recuperación se asegura que el sistema pueda ser recompuesto de manera rápida y efectiva luego de una interrupción.
- Desarrollo de un plan de contingencias debe contener de manera detallada guías y procedimientos para restaurar el sistema dañado.
- Evaluación del plan, entrenamiento y ejercicios, se identifican las fallas en la planificación, mientras que el entrenamiento prepara al personal que se ocupa de la recuperación para la activación del plan; ambas actividades mejoran la efectividad del mismo y la preparación de toda la agencia.
- Mantenimiento del plan puede ser un documento vivo que se actualizará regularmente para mantener el sistema acorde con los desafíos.

Un plan de recuperación puede ser de dos tipos: desastres naturales y desastres provocados por el hombre, y cualquiera de ellos puede tomar por sorpresa a las organizaciones, con poca o ninguna advertencia. Cuando algún desastre se presenta, aquellas empresas que se han preparado y efectuado sus planes de recuperación ante desastres (DRP) sobreviven con una interrupción de su productividad o pérdida mínima de datos.

1.2.5. Esquema gubernamental de seguridad informática (EGSI)

Mediante Acuerdo Ministerial No. 166, publicado en el Registro Oficial No. 88 del 25 de septiembre de 2013, se dispone la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), en todas las entidades de la Administración Pública Central (APC); donde se establece 126 hitos o controles, basados en la norma técnica ecuatoriana INEN ISO/IEC 27002 “Código de Práctica para la Gestión de la Seguridad de la Información”, cuya implementación debe ser prioritaria para las entidades públicas (fase I) y la implementación de la fase II del EGSI se realizará en cada institución de acuerdo al ámbito de acción. Estructura orgánica, recursos y nivel de madurez en gestión de seguridad de la información. Se recomienda que previo a la implementación del EGSI se proceda a dar cumplimiento al Art. 7: Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en

base a la norma INEN ISO/IEC 27005 “Gestión del Riesgo en la Seguridad de la Información”; considerando que los activos críticos institucionales identificados en el estudio de gestión de Riesgos, permitirán determinar los controles necesarios a ser implementados por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (2019).

Para cumplir con los propósitos de la tecnología de la información; se crea la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, mismo que desarrolló el EGSI, elaborado en base a la norma NTE INEN-ISO/IEC 27002, expedidas por el Servicio Ecuatoriano de Normalización INEN. El EGSI establece un conjunto de directrices prioritarias para la gestión de la seguridad de la información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

La implementación del EGSI reducirá significativamente amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información, tanto física como electrónica, que procesa la institución. Así mismo, contribuirá a establecer un proceso de mejora continua de la gestión de la seguridad de la información e incrementar la cultura de los servidores públicos en cuanto al manejo de la información que utilizan para cumplir sus funciones sea institucional o de la ciudadanía.

CAPITULO II. DISEÑO METODOLÓGICO

2.2. Diagnóstico

En el desarrollo de la metodología se ha recurrido a un diagnóstico situacional en función de los objetivos que guían la investigación, se utiliza la metodología del análisis del impacto del negocio (BIA); que trabaja en seis ejes fundamentales, los cuales son:

- Identificación de procesos del negocio
- Evaluación de los impactos operacionales y financieros
- Identificación de los procesos críticos
- Establecimiento de los tiempos de recuperación
- Identificación de los requerimientos de recursos críticos
- Identificación de procedimientos alternos

El autor Alce (2018); deduce que, la necesidad de mantener y evaluar los impactos en casos de riesgos para prevenir y salvaguardar datos y la infraestructura tecnológica de la información, es de vital importancia para las empresas públicas, donde el ciudadano es lo más preciado, puesto que, los datos y hechos históricos no son recuperados una vez que se pierden, sino se almacena la información con los respectivos respaldos ante posibles riesgos o catástrofes. Además, Bautista (2018) textualmente menciona:

Para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, se debe emplear herramientas de gestión, para evitar afectaciones en las operaciones regulares de las organizaciones, por lo consiguiente debe formar parte de un sistema de gestión de riesgos, que sea utilizado como mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencia. (p. 62)

2.3. Método de la investigación

Para establecer el problema de estudio con claridad y exactitud, fue necesario desarrollar una metodología descriptiva que permite al investigador determinar la solución más apropiada en relación a un plan de continuidad de servicios, al presentarse algún problema o incertidumbre en el departamento de tecnologías de información, encajando dentro de la realidad de la empresa EP-EMAPA-A, seleccionado los siguientes métodos asociados al proceso del estudio.

2.3.1. Método general

Con la finalidad de conocer los diferentes hechos, sucesos actividades relacionadas a la gestión y control de un plan de continuidad de servicios se aplicó este método apoyado en las siguientes técnicas:

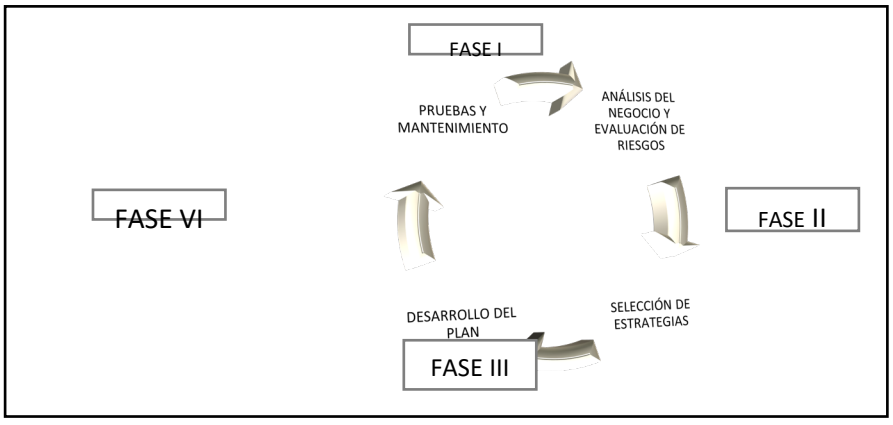
- Observación

El proceso de información fue a través de la observación directa, para verificar si la información ha sido recurrente al respecto de una adecuada planificación que integra los servicios y correcto funcionamiento del departamento de TI, en caso de que exista una irrupción, factores de riesgo o amenaza en el sistema informático. Para la aplicación de esta técnica se utilizó un *checklist*, que consta en el anexo 1.

2.3.2. Método de análisis

Se identificó los posibles riesgos e incertidumbres que se ocasionar en el sistema del departamento de TI, destacando fallos en el servicio, de facturación o daños en los equipos cuya necesidad es integrar una evaluación sistémica con el propósito de tomar una decisión acertada al ocurrir un riesgo, además, cada uno de los componentes fueron analizados desde la perspectiva tecnológica. Por tanto, el análisis se aplicó en la primera fase de la metodología BIA, desarrollada en el siguiente segmento, a través de este método se identificó ampliamente el problema. La metodología se basa en la guía para realizar el BIA propuesto por Bautista (2018) detalla para la creación de un plan de continuidad del negocio, es necesario contar con cada fase propuesta en esta guía; lo cual tomando en referencia y en resumen se plantea lo siguiente:

Figura N° 8. Método aplicado para la propuesta tecnológica



Fuente: Elaboración propia

Análisis del negocio y evaluación de riesgos

Pacheco, Apostólico y Asociados (2017) identifican a las probabilidades de ocurrencia que algún evento negativo pudiese afectar de forma adversa el logro de los objetivos de una organización. Es decir, las decisiones equivocadas pueden provocar resultados negativos o pérdidas para la empresa. Los riesgos se analizan considerando su impacto y probabilidad de ocurrencia como base para determinar cómo deben ser gestionarse y evaluar desde una doble perspectiva, inherente y residual.

Los negocios y evaluación de riesgos se establecen mediante en un proceso formal con documentación legal y protegida, para determinar el impacto del marco de evaluación, este proceso está incluido en un análisis sistemático priorizando los costos para después definir el impacto del negocio, el análisis de impacto está conformado por todas las actividades que refuerzan la provisión de los productos y servicios, evaluar los impactos que se genera al transcurso del tiempo y estableciendo plazos en un nivel acertado (ISO Tools Excellence, 2019).

En esta etapa se examina el impacto del negocio con los procesos que maneja el departamento de tecnología de la información de la EP-EMAPA-A., es así que los posibles riesgos de negocio sean incomparables a los procesos críticos, mismos que son inevitables para realizar un inventario de los activos involucrados en el sistema, estos son incluidos de manera estratégica. Los riesgos son necesarios para tener una posición estratégica en el entorno en el cual se desarrolla su actividad económica.

Selección de estrategias

Para Soto (2004) la selección de estrategias involucra a la Gerencia como grupo estratégico, deben buscar cumplir los objetivos de corto y largo plazo para llegar a la visión y se enfoca en 4 principales fases como: el análisis del negocio y evaluación de riesgos, selección de estrategias, desarrollo del plan pruebas y mantenimiento, por ende, se debe tener claro el concepto de estrategia, desarrolla el pensamiento estratégico.

Hay diferentes tipos de estrategias para aplicar en las organizaciones como liderazgo en costos; tomar una decisión conlleva a definir varias estrategias y aceptar la más adecuada para conseguir resultados positivos, se debe tener en cuenta el pensamiento estratégico

dentro del grupo en el cual se desarrolla y aplica con la finalidad de poder valorar las estrategias adaptadas para la empresa.

En esta fase se involucra las estrategias de respaldo mediante la gestión de los riesgos detectados en los procesos de la empresa pública EP-EMAPA-A., además se considera seleccionar estrategias que recuperen la continuidad de los procesos con el análisis del impacto considerándose el equipamiento de la infraestructura del centro de trabajo.

Desarrollo del plan

Pérez (2013) opina que el desarrollo del plan es un instrumento de gestión pública empleado para propulsar el desarrollo social de un determinado territorio, que puede ser el Estado en su conjunto o bien una subdivisión del mismo.

Los planes se enfocan en el desarrollo de los procesos para el capital humano y el entorno de la sociedad en conjunto, esto provoca un cambio totalmente positivo para la empresa a través de evolución al cambio de las personas e instituciones públicas y privadas, las relaciones de individuos, grupos e instituciones en una sociedad, implica principalmente desarrollo económico y humano; su proyecto a futuro es el bienestar social.

En esta etapa se desarrolla el plan de continuidad definiendo la estructura y composición de los equipos en las acciones que se ejecutan en la empresa pública de la EP-EMAPA-A., considerándose la experiencia que tenga cada uno de los trabajadores en el área que desempeñe; es importante señalar que el comité de crisis está conformado por varios equipos como el de recuperación vinculado a la unidad de negocios; el equipo de coordinación de logística, de relaciones públicas, cada uno ejecuta procedimientos desarrollados en esta fase.

Pruebas y mantenimiento

García (2005) integra las pruebas se enfocan en la revisión de los procesos en el plan de continuidad, para definir cada uno de los ítems a evaluar en los servicios en las TI de la empresa, es indispensable que se haya aplicado de forma adecuada dentro de la organización, normalmente, que las soluciones implementadas cumplan con los requisitos identificados. Se pueden llevar a cabo autoevaluaciones, si existen las personas experimentadas necesarias al interior de la empresa o se pueden llevar a cabo por un

experto o un grupo de profesionales de la continuidad del negocio externos, sin duda, lo más recomendable.

Las empresas van cambiando constantemente en medida que va evolucionando la tecnología, los procesos y productos del plan de continuidad y la instalación de la empresa. García (2005) menciona que: "Cualquier cambio dentro de la organización debe evaluarse para identificar si afecta la capacidad de las organizaciones para continuar o recuperar". Continuamente las empresas van cambiando de prioridades comerciales para ir implementando estrategias diferentes con servicios y proyectos para mejorar el desempeño optimizar materia prima y recursos, el método más óptimo es asegurar la planificación de continuidad.

Las modificaciones necesitan ser evaluadas constantemente mediante procesos de gestión, es sumamente importante registrar y evaluar las alternativas en los procesos con total exactitud, el mantenimiento forma parte de la transformación mediante planificación. En esta última fase se evalúa la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la empresa pública EP-EMAPA-A., probando su efectividad y los tiempos de respuesta del plan de continuidad para comprobar que este se encuentre alineado al desarrollo de los procedimientos realizados.

2.3.3. Método sintético tecnológico

Un sistema informático, es considerado como una herramienta de control dentro de las áreas de una empresa sin embrago, dentro del departamento de tecnologías de la información es recurrente y necesario para el control, proceso, evaluación y seguimiento para el correcto funcionamiento de un plan de continuidad. Además, se sintetizó ciertas características que apoyaban al objetivo del presente trabajo de investigación, las mismas que han sido expuestas en la fase de diseño de la metodología BIA.

Técnicas e instrumentos para recopilación de información

Basado en lo anterior y en lo manifestado por los autores sobre la utilización de la metodología del análisis del impacto del negocio (BIA); es necesario la construcción de una lista de verificación basado en cada elemento de la metodología propuesta. La validación del instrumento es en base a antecedentes y fuentes bibliográficas ya probadas; las cuales fueron aplicadas en empresas municipales.

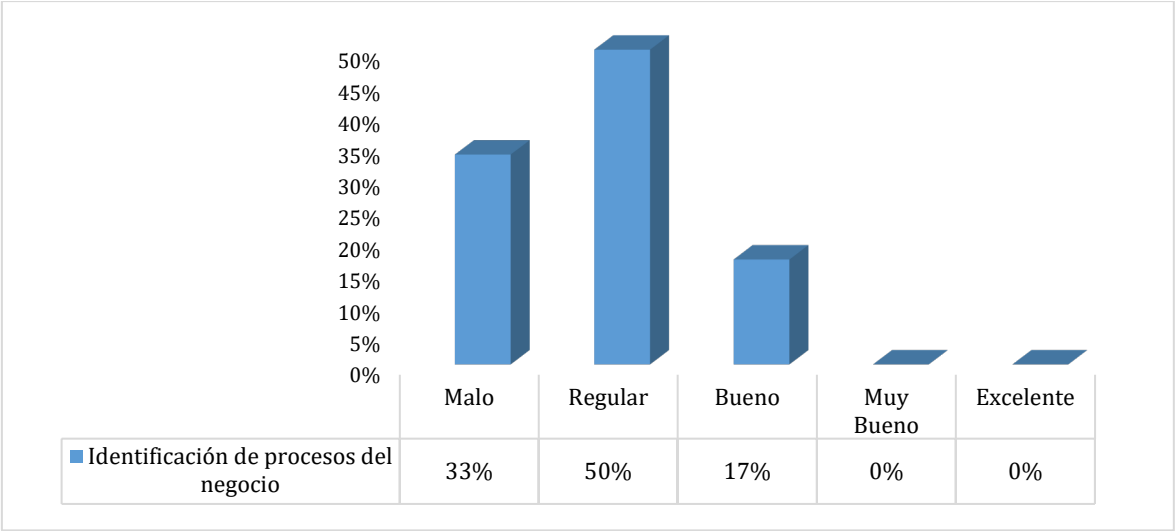
Bautista (2018) al tener un antecedente y comprobado la factibilidad del instrumento, es necesario la construcción de la lista de verificación y con ello su aplicación, tabulación y análisis respectivo.

El instrumento que se considera para la recopilación de la información en campo es la lista de verificación misma que consta de sinnúmero de factores a evaluar mediante la escala de Likert; como se lo puede identificar en el anexo No 2.

2.4. Procesamiento y análisis de la información

Aplicado la lista de verificación para el personal administrativo, jefes operativos de la EP-Empresa Municipal de Agua Potable y Alcantarillado de la ciudad de Ambato, misma que permite el levantamiento de datos se obtienen los siguientes resultados los mismos que son útiles para el siguiente análisis, que se muestra en la figura 9:

Figura N° 9. Identificación de procesos del servicio



Fuente: Elaboración Propia

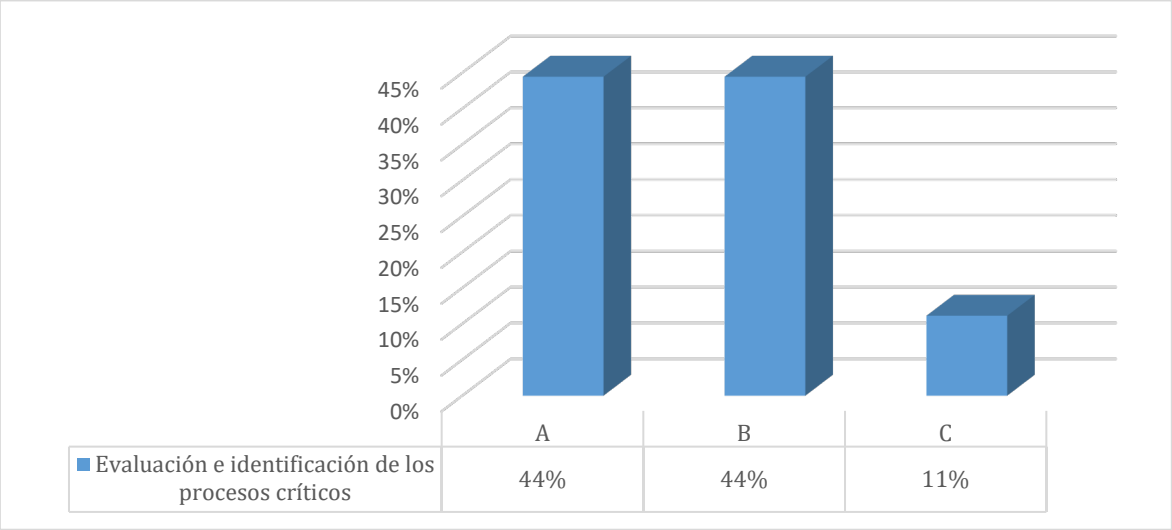
Análisis

Dentro del diagnóstico realizado, empleando el análisis del impacto del negocio (BIA), se tiene que el primer factor de identificación de procesos del negocio, como factores del sistema de control de documentos, Sitios web; servidor de datos, seguridad de la información, sistemas de almacenamientos y comunicación, cuadro de máquinas, proveedores y recursos humanos, en la que se indica que es regular en un grado

porcentual del 50%, así mismo es malo en un 33% y por último el 17% indica que es bueno, por ende se muestra que existen problemas para identificar los procesos organizacionales en la EP-EMAPA-A., mismos que constituyen un riesgo.

Para el sistema de gestión de seguridad de la información (2019), es necesario identificar todos los procesos y actividades que se encuentran relacionadas de forma directa con la misión y los objetivos de la empresa, su interacción con los activos de soporte, así como las dependencias y los insumos que resulten críticos en el caso de fallos inesperados.

Figura N° 9. Evaluación e identificación de los procesos críticos



Fuente: Elaboración Propia

Análisis

Dado la evaluación e identificación de los procesos críticos, señalados en la figura 10, se encuentra que los elementos que son críticos para la empresa, o que la función del negocio no puede realizarse (A), representa un 44% simbolizando un nivel de riesgo alto; por otra parte, los elementos que no son críticos para la empresa, pero que la operación es una parte integral de la misma (B), constituye un 44% también, e indica que tiene un riesgo medio; mientras que los elementos que hacen que la operación no sea parte integral de la empresa (C), dio un 11% con un riesgo bajo. Para una mejor comprensión del análisis y la gráfica se realiza la siguiente tabla, donde se identifica el nivel de riesgo según los procesos críticos (A, B, y C). Por lo tanto, para brindar una continuidad de negocio a los procesos críticos definidos dentro de la institución, es imprescindible contar con un plan

tecnológico que aumente la disponibilidad de dichos elementos a fin de dar cumplimiento con el tiempo de operación inactivo soportado por las instituciones (Jacome, 2013).

Se evalúa los procesos críticos mediante los siguientes riesgos de identificación tal como se observa en el siguiente cuadro N° 4:

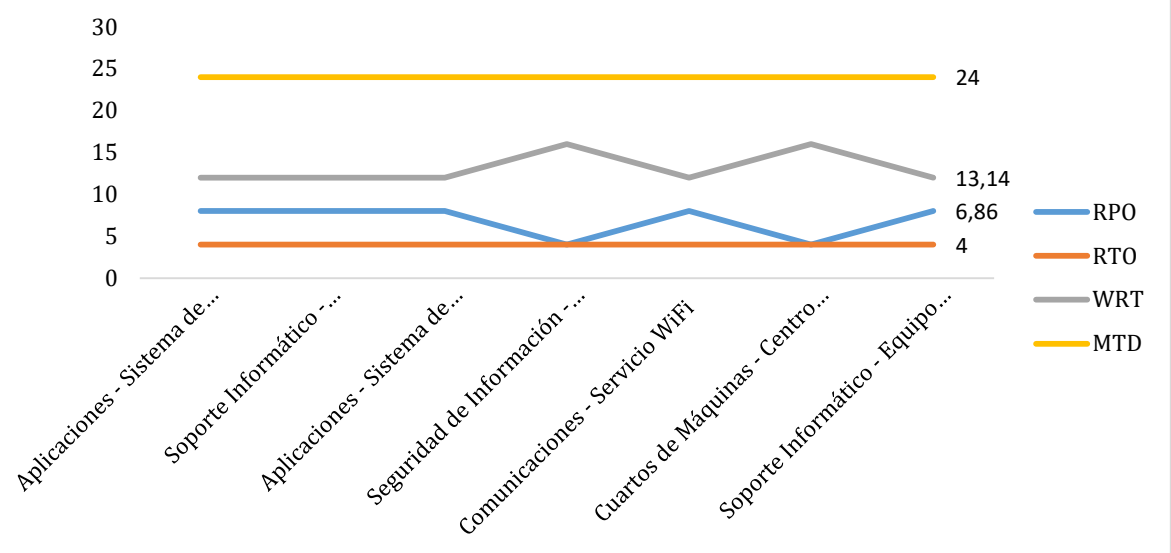
Cuadro N° 5. Riesgos en la evaluación e identificación de los procesos críticos

Evaluación e identificación de los procesos críticos	A	B	C
Aplicaciones - Sistema de Control de flujo de documentos			
Web - Sitio web Entidad			
Base de Datos - SQL			
Seguridad de Información - Firewall			
Sistemas de Almacenamiento - SAN (Storage Área Network)			
Comunicaciones - Acceso Local a Internet			
Cuartos de Máquinas - Centro de Datos			
Proveedores de Aplicaciones y/o comunicaciones - Interno/externo			
Recurso Humano - Internos/externos			

Fuente: Elaboración Propia

Jacome (2013) cita a Josep Micolau, Delivery Director de CA, indicando que la pérdida de datos críticos para el negocio de una entidad empresarial y el tiempo de inactividad de los sistemas clave de TI son dos de los mayores riesgos a los que se enfrentan los responsables de tecnologías de la información a la hora de aplicar un plan de continuidad del servicio, como se señala en la Figura 11.

Figura N° 10. Establecimiento de los tiempos de recuperación en número de horas

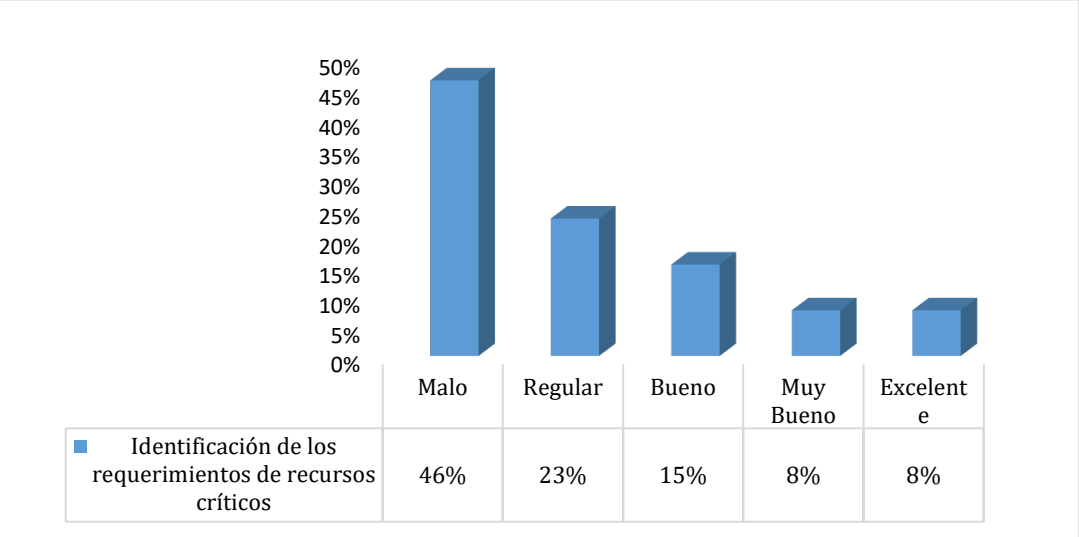


Fuente: Elaboración Propia

Análisis

En cuanto al establecimiento de tiempos de recuperación, este se trabajó en número de horas y en función de los promedios generales de recuperación de los procesos críticos identificados; es así que la magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio (RPO), tiene un promedio de recuperación de 6,86 horas; el tiempo disponible para recuperar sistemas y/o recursos que han sufrido una alteración (RTO), asume un promedio de 4 horas en su recuperación; el tiempo disponible para recuperar datos perdidos una vez que los sistemas están reparados, lo que se traduce como el tiempo de recuperación de trabajo (WRT), tiene un promedio de 13,14 horas; finalmente, el periodo máximo de tiempo de inactividad que puede tolerar la entidad sin entrar en colapso (MTD), tiene un promedio general de 24 horas. En general no sobrepasa de un día en recuperarse la parte de software y hardware, puesto que, si se sobrepasa estos promedios, la entidad entraría en un colapso.

Figura N° 11. Identificación de los requerimientos de recursos críticos



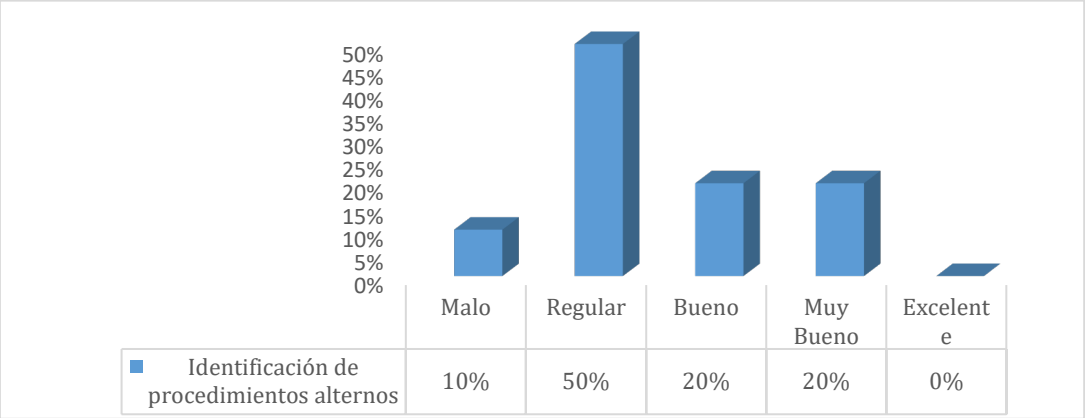
Fuente: Elaboración Propia

Análisis

Basado en los análisis de los elementos descritos dentro de la identificación de los requerimientos de recursos críticos; se observa en la figura 12, que es malo en un 46%, regular en un 23%; bueno en 15%; muy bueno en un 8% y excelente en un 8%; lo cual se traduce, en que EP-EMAPA-A no identifica los requerimientos de recursos críticos, no es una prioridad para la empresa, y esto en conjunto con los otros puntos, muestra una

total desatención y posibles colapsos en el caso fortuito u ocurrencia de catástrofes o riesgos no controlados.

Figura N° 12. Identificación de los procedimientos alternos



Fuente: Elaboración Propia

De la misma manera, como se observa en la figura 13, el Departamento TI de EP-EMAPA-A., no identifica procedimientos alternos, pues la valoración es mala en un 10%, regular en un 50%, bueno en 20%, y muy bueno en 20%; por lo cual, con el 60% existe una deficiente identificación de procesos alternos, y esto se complementa a los otros factores que de la misma manera son críticos y se encuentran con problemas, ante cualquier tipo de amenaza latente.

En conclusión, a los resultados obtenidos en la lista de verificación, del diagnóstico de la situación actual de la EP-EMAPA-A, en donde, los sistemas clave de TI son dos de los mayores riesgos a los que se enfrentan los responsables de tecnologías de la información a la hora de gestionar un plan de continuidad de servicios. Este Plan debe permitir minimizar el tiempo de recuperación e impacto que supone cualquier incidencia que afecte al nivel de servicio de los procesos críticos de los servicios para que afronte situaciones de riesgo en los procesos tecnológicos, es deficiente; no existe una clara identificación de los factores que intervienen en la metodología del análisis del impacto del negocio (BIA), lo cual a futuro, en el caso de eventualidades no deseadas, puede experimentar riesgos críticos y colapsos en su sistema, incluyendo en este punto la pérdida de información temporal y definitiva. Por ende, existe la oportunidad de diseñar un plan de continuidad del servicio que es un mecanismo de respuesta que asegura orden y control durante una interrupción operacional. Estos planes incluyen la identificación del

incidente, evaluación, escalamiento, declaración, activación del plan, desactivación del plan y procedimientos de restauración. Este plan está compuesto por el plan de continuidad del negocio (BCP), el cual ayuda a continuar y mantener los procesos críticos del negocio, y el plan de recupero de sistemas (DRP), mediante el cual se restauran los sistemas e infraestructura que soportan a los procesos críticos antes identificados. El resultado final del plan de continuidad de servicios de TI corresponde al mapeo de los procesos críticos de la empresa, con el plan de recuperación de desastres o plan de recuperación de sistemas.

2.5. Materiales y herramientas

Para el desarrollo y diseño de la propuesta no se requieren de materiales o herramientas que ameriten este punto; puesto que ya se cuenta con la información dada en el formato y archivo presentado en la lista de verificación, en base a esto y la guía para el diseño del plan de continuidad se elabora la propuesta.

Los materiales son básicamente la computadora, fichas para el levantamiento de información; y como herramientas, los programas para la escritura y para la tabulación de datos. Mencionar que, para el desarrollo de la propuesta queda en documentos, su aplicación es parcial y dependerá de la aprobación de la administración de la empresa, su ejecución total; para ello se contará con dicha documentación al final de la misma.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.2. Diseño de un plan de continuidad de servicios.

El diseño de un plan de continuidad de servicios en base a las TI, sirve para que la empresa EP-EMAPA-A requiera una adecuada planificación de actividades en base a factores de riesgo y problemas que se den en el departamento de tecnologías de información, para organizar, controlar y mitigar algún impacto negativo que se de en la operatividad del sistema de servicios de agua potable hacia la comunidad ambateña.

Para priorizar los productos o servicios que son esenciales en la generación de las estrategias a seguir para lograr continuidad de servicios. La primera prioridad que se debe ejecutar es proteger al talento humano; que labora en las instalaciones de la EP-Empresa Municipal de Agua Potable y Alcantarillado de la ciudad de Ambato, proveedores y clientes cumpliendo con las necesidades contractuales de clientes y usuarios, hacer frente a la responsabilidad social como empresa pública; así como, generar contribuciones con la sociedad y la economía locales. Cumpliendo con los múltiples requerimientos como la infraestructura TI, los recursos humanos, los mobiliarios e inmobiliario, el sistema de comunicación, la logística; entre otros. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico.

El plan de continuidad no se considerará válido hasta que no se haya superado satisfactoriamente el plan de pruebas que asegure la viabilidad de las soluciones adoptadas. El plan de pruebas diseñado tiene como objetivo:

Evaluar la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la empresa pública EP-EMAPA-A., probando su efectividad y los tiempos de respuesta del plan para comprobar que están alineados con la definición realizada en el diseño; como también la comprobación adecuada de los procedimientos desarrollados para soportar la recuperación de las operaciones en el servicio como la participación de los involucrados, por tanto, es importante para la situación de contingencia que presente la empresa; esto se lo deberá ejecutar con un simulacro donde se entrene y forme a los empleados y a los equipos que integran el comité de crisis.

3.3. Factores que integran un plan de continuidad de servicio de las TI

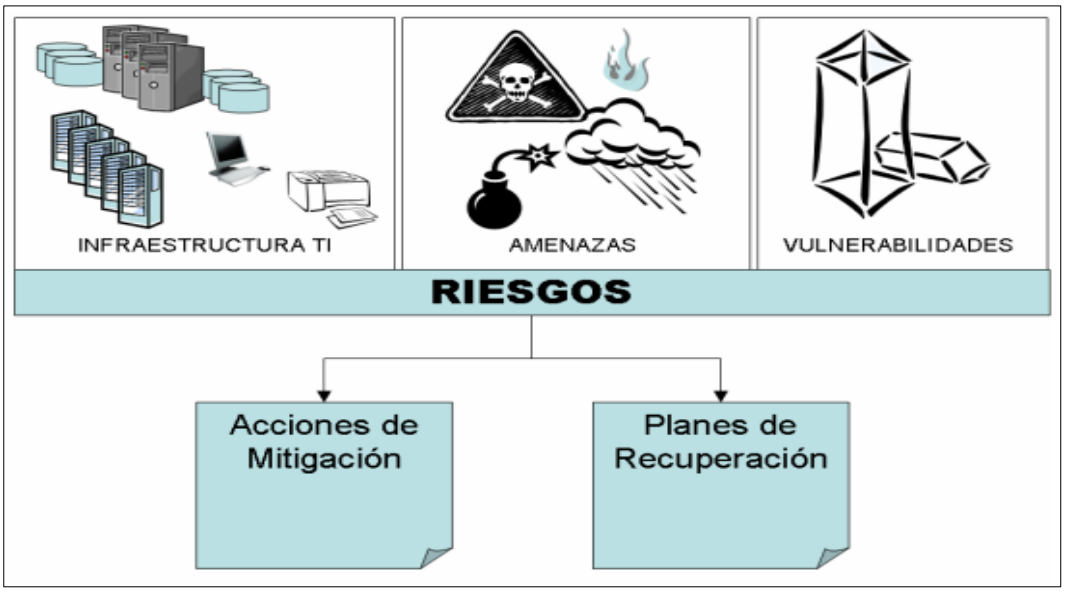
La empresa EMAPA, se ajusta a una planificación sobre la continuidad de servicio en las TI, aplican a un sistema informático denominado TI *Service Continuity Management*, que permite prevenir y proteger los efectos previstos por la interrupción de servicio de las TI, ocasionada por fallas técnicas, naturales o que hayan sido provocadas de forma involuntaria.

Por tanto, la administración sobre la continuidad de servicio en las tecnologías de la información crea un componente intrínseco para la empresa pública EP-EMAPA-A, cuya finalidad pretende mitigar un posible incidente, que impida el uso de los sistemas por pocas horas de duración y que puede tener un impacto en los equipos de la empresa. La dependencia que existe entre el servicio de institución pública y los sistemas de información exige que estén preparados para afrontar las múltiples amenazas que ponen en riesgo de operatividad y la continuidad de los servicios que presta. En base a los siguientes procedimientos:

- **Preventivos. -** Corresponden a las medidas y procedimientos que busca eliminar los riesgos de interrupción y los posibles efectos en el departamento de TI.
- **Reactivos. –** Reanudan el servicio tan pronto como sea posible después de cualquier disrupción.
- **Objetivos. –** Aseguran la pronta recuperación de los servicios críticos de las TI. Además, establece políticas, medidas y procedimientos para evitar desastres en base a terremotos, evento accidental, incendio, explosivos.
- **Costo. -** Es necesario que la empresa contrate un seguro en vista que se debe implementar en el sistema de continuidad de servicio.

Todos estos factores al integrase en el plan de continuidad de servicios ofrece una correcta coordinación en base, a las actividades que la empresa ofrece a un determinado grupo de personas en donde se requiere la toma de medidas asertivas para enfrentar los riesgos como se muestra en la figura 14.

Figura N° 13. Proceso de continuidad de servicios de TI

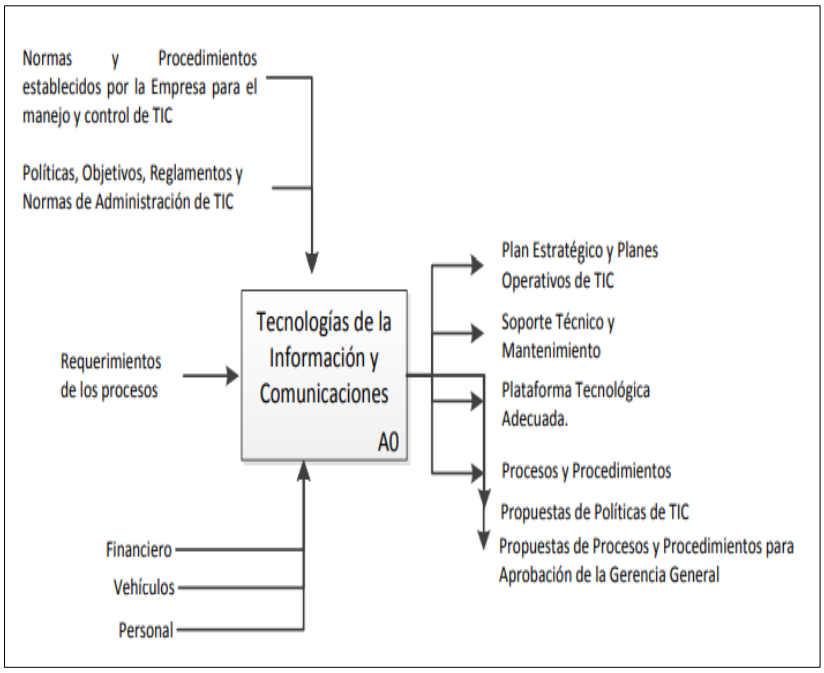


Fuente: (ISO Tools Excellence, 2019)

En la figura 14, es evidente al emplear un plan de continuidad de servicios para un departamento correspondiente a las TI, en donde implica que la infraestructura, amenazas y vulnerabilidades se relacionan entre si paralizando el funcionamiento del sistema y afectando al funcionamiento del servicio cuyo principal riesgo se basa en emplear acciones de mitigación y planes de recuperación.

Sin embargo, la tecnología de la información asiste con la responsabilidad de garantizar el uso adecuado y la correcta integración de la información en los procesos que usa la empresa, garantizando la efectividad, confidencialidad, integridad, disponibilidad y seguridad de la información. Además, es responsable de la administración de la infraestructura tecnológica de información y telecomunicaciones. Por ende, debe proveer de la instalación tecnológica adecuada relacionada con el manejo de la información para los procesos de la EP-EMAPA-A. Es necesario e indispensable tener un proceso de las actividades que deben ejecutarse en el departamento de TI, misma que se identifica en un proceso general y detallado para las jefaturas tal como se lo demuestra en las siguientes figuras No. 15.

Figura N° 14. Funcionalidad del departamento de tecnologías de información y comunicación



Fuente: (EP-EMAPA-A, 2019 – PRO - 018)

Como se puede apreciar en la figura 11, el departamento de tecnologías de la información y comunicación de la empresa EP- EMAPA- A, delega varias funciones y actividades que se vinculan con de los factores internos de un plan de continuidad, en instancia se identifica que la empresa aplica un conjunto de normas y procedimientos para el adecuado manejo de la TIC, mediante el cumplimiento de políticas, objetivos, reglamentos y normas correspondientes a la planificación y soporte técnico, para mitigar posibles daños o problemas.

Por otro lado, el manejo y soporte de los equipos requiere de un soporte técnico de Software y Hardware; considerando que los dos son de mucha importancia, para el análisis se generaliza los procesos por los componentes físicos y son componentes internos y manejados por técnicos de la empresa, el uso de las herramientas es utilizadas como mecanismo de control, formularios de aprobación y demás documentación mencionada en la estrategia de mantenimiento y se integra de dos formas:

1.- Soporte técnico mediante software

A continuación, se analiza los procesos que son utilizados con software, mismos que se encuentran enfocados a l descripción, tipo de sistemas, número de equipos y el responsable de su ejecución como se lo observa en la tabla No 2.

T**abla N° 2**. Soporte técnico mediante software

Nombre del proceso	**Nombre del sistema**	**Descripción**	**Tipo de Sistema (PC/Servidor/ Mainframe)**	**Nº de Equipos con la aplicación**	**Responsable**	**Contacto Técnicos**
Soporte técnico y mantenimiento	Correo electrónico	Soporte técnico de la empresa se debe ejecutarse siguiendo los lineamientos TI	Servidores de la empresa	**3**	Jefe del departamento de las TIC	------
Plataforma tecnológica (Edu2.0)		Aplicación para la Gestión	Conectividad de internet	**3**	Jefe del departamento de las TIC	-------

Fuente: Elaboración Propia

Tabla N° 3. Equipamiento del software

Equipamiento	**Detalles del Modelo/Configuración**	**Distribuidor**	**Cantidad**	**Localización**
Servidor de Correo	PowerEdgeTM 1900 Servidor en torre de núcleo cuádruple	Dell	**2**	Centro proceso datos EP-EMAPA-A.
PC's	Procesador Intel® CoreTM 2 Duo E6000 Chipset Q965 ICH8DO compatible con Active Management Technology (iAMT 2.1) de Intel® Solución LAN Gigabit Ethernet de Intel®	Dell	**3**	Centro proceso datos EP-EMAPA-A.
Servidor de Aplicaciones	PowerEdgeTM 2900 Servidor en torre de núcleo cuádruple con 2 sockets	Dell	**2**	Centro proceso datos EP-EMAPA-A.

Fuente: Elaboración Propia

2.- Soporte técnico mediante Hardware

Tabla N° 4. Soporte técnico mediante Hardware

Proceso	Sistema	Descripción	Tipo de Sistema (PC/Servidor/ Mainframe)	Nº de Equipos con la aplicación	Responsable	Contacto Técnicos
Plan estratégico y planes operativos TIC	Estrategias empresariales de la empresa Normativa ISO 9001:2015	Fomenta la optimización de recursos mediante la proyección de proyectos	Servidor / PC's	**3**	Jefe del departamento de las TIC Analista de las TI Asistente de las TI	Soporte Windows
Procesos y procedimientos	Normativa ISO 9001:2015	Se da seguimiento a los lineamientos normativos de norma	Servidor / PC's	**2**	Analista de las TI Asistente de las TI	Soporte Windows
Propuestas de las políticas de las TI	Normativa ISO 9001:2015	Se da seguimiento a los lineamientos normativos de norma	Servidor / PC's	**2**	Analista de las TI Asistente de las TI	Soporte Windows
Propuesta de procesos para la aprobación de la gerencia	Normativa ISO 9001:2015	Se da seguimiento a los lineamientos normativos de norma	Servidor / PC's	**1**	Jefe del departamento de las TIC	Soporte Windows

Fuente: Elaboración Propia

Tabla N° 5. Equipamiento del hardware

Equipamiento	Detalles del Modelo/Configuración	Distribuidor	Cantidad	Localización
Servidor de aplicaciones	PowerEdgeTM 1900 Servidor en torre de núcleo cuádruple	Dell	3	Centro proceso datos
PC's	Procesador Intel® CoreTM 2 Duo E6000 Chipset Q965 ICH8DO compatible con Active Management Technology (iAMT 2.1) de Intel® Solución LAN Gigabit Ethernet de Intel®	Dell	3	Centros de Valencia y Albacete

Elaboración: Propia

Tiempo máximo de recuperación de los procesos

N° 6. Tiempo máximo de recuperación de los procesos

Análisis de los procesos	Proceso	Necesidades de Recuperación	Cantidad
Software	Soporte técnico y mantenimiento	1 - 3 días	3
	Plataforma tecnológica adecuada	3- 5 días	1
Hardware	Plan estratégico y planes operativos TIC	15-30 días	2
	Procesos y procedimientos	3 meses	2
	Propuestas de las políticas de las TI	3 meses	2
	Propuesta de procesos para la aprobación de la gerencia	12 meses	1

Fuente: Elaboración Propia

Según el análisis de la tabla N° 5 y 6, los procesos y procedimientos como el mantenimiento de equipos son la clave para el control de las actividades en una organización, en vista que al no gestionar el Software y Hardware la empresa limita ofrecer un servicio, por lo tanto, incurrirá rápidamente en pérdidas. Por ello, es importante que este proceso se recupere lo antes posible.

Identificación e inventario de activos

Se realiza un análisis con un enfoque general, sin entrar en metodologías concretas ni valoraciones de los activos. Tomando como ejemplo el inventario de los procesos descritos y las premisas en la presentación de la empresa, se elaboró para cada proceso crítico un inventario de los activos involucrados en el proceso. Los activos se definen como los recursos de una compañía que son necesarios para la consecución de los objetivos en la empresa EP-EMAPA-A.

Cuadro N° 6. Identificación e inventario

Descripción	Tipo	Propietario	Localización	Valor
Servidor de aplicaciones	Hardware	EP-EMAPA-A.	Centro de Proceso de datos	Medio
Aplicación de normas digitalizadas	Aplicación	EP-EMAPA-A.	Servidores y PC's	Medio
Información clientes	Información	EP-EMAPA-A.	Base de datos	Alto
Impresoras	Hardware	EP-EMAPA-A.	Centros de Albacete y Valencia	Bajo
Redes de comunicaciones	Comunicaciones	EP-EMAPA-A.	Centros de Albacete y Valencia	Bajo
Infraestructura de las tecnologías informáticas	Aplicación	EP-EMAPA-A.	Telecomunicaciones, automatización y comunicación de negocios y servicios de Tecnología de la información	Medio

Fuente: Elaboración Propia

En el cuadro No 9, se describe el inventario de activos que posee la empresa EP-EMAPA-A, con el propósito de presentar la información de las diferentes actividades en base; a normas, procedimiento y aplicación del sistema informático del departamento de tecnologías de la información en donde, se observa que valor se obtiene para cada alternativa dentro del proceso.

Las alternativas existentes y dado que la opción de subcontratar espacios y soporte a terceros resultaría muy cara para EP-EMAPA-A., la solución más adecuada sería utilizar

el centro de Albacete con alternativa en caso de incidencia grave. De esta forma EP-EMAPA-A., podría seguir dando servicio a los clientes, sin que el impacto de un incidente tuviera consecuencias catastróficas para la empresa pública. Para ello, podrán utilizarse en primera instancia los equipos que se utilizan, de forma que se reaproveche la inversión. Para que estos equipos sean válidos será necesario equipar la infraestructura del centro de trabajo, con algunos elementos extras (incremento de memoria, capacidad de disco, etc.).

3.3.1. Desarrollo del plan continuidad de servicios

Una vez que se ha seleccionado la estrategia de continuidad, se puede comenzar a construir el plan de continuidad definiendo la estructura y composición de los equipos y las acciones de cada uno de ellos. Dado que EP-EMAPA-A., es una empresa de tamaño medio, reduciremos el número de equipos y la composición, que será necesaria en caso de activación del plan de continuidad de servicios.

Lista de distribución. - El documento es de uso interno de la empresa y se sujeta a los cambios del personal responsable para la asignación de datos correspondientes, que son controlados y registrados en la tabla de control de revisión.

Control de revisión	**Observaciones**
1	La empresa ha diseñado un plan de continuidad de servicio para el departamento de TI

Alcance.- El alcance de este documento es establecer un procedimiento que indique las directrices a seguir en caso de una contingencia en los servicios críticos de TI y los responsables de cada actividad.

Equipos. - Los equipos de trabajo, sus actividades e integrantes están conformados según el siguiente cuadro:

Cuadro N° 7. Equipo de integrantes de la empresa EMAPA

Equipos	Funciones	Integrantes
Equipo director	Análisis de la situación Activación o no del plan de continuidad de servicios de TI Seguimiento Evaluación	Gerente de sistemas (líder) Gerente comercial (suplente) Jefe de operaciones presidente ejecutivo
Equipo logístico	Transporte al centro alterno Proveer redes de agua y alcantarillado Contacto con los proveedores	Gerente de sistemas (líder) Gerente comercial (suplente) Jefe administrativo Jefe de desarrollo de software
Equipo de recuperación	Sistema de información SIS Sistema de información KREA Servidor de archivos compartidos	Jefe de operaciones (líder) Gerente de sistemas (suplente) Asistentes de operaciones Jefe de desarrollo de software Asistentes de desarrollo de Software
Equipos de pruebas	Realizarán las pruebas de verificación de operación de los servicios principales de TI	Asistente de calidad de software (líder) Asistente técnico Asistente de nómina Asistente de caja

Fuente: Elaboración Propia

Datos informativos. - A continuación, se coloca la información de contacto por cada miembro de equipos, líderes de área y proveedores de acuerdo al cuadro N° 15y 16

Tabla N° 7. Datos de los miembros de los equipos

Nombre del equipo: Logística

Datos	Líder	Suplente
Nombre	Esteban Sánchez	Daniel Ortiz
Cargo	Gerente en sistemas	Gerente comercial
Celular	0984234156	0999234785
Mail no corporativo	esteban@gmail12	dany@gmail34
Dirección domiciliaria	Ficoa calle limas y fresas	Nueva Ambato

Fuente: Elaboración Propia

Tabla N° 8. Listado de proveedores tecnológicos

Proveedores Tecnológicos	Características
DELL	Persona de Contacto: Teléfono Contacto: Mail:
XP	Persona de Contacto: Teléfono Contacto: Mail:
Toshiba / Sony	Persona de Contacto: Teléfono Contacto: Mail:

Fuente: Elaboración Propia

Lugar de Reunión. - Se llevarán a cabo en la sala de reuniones de la empresa pública EP-EMAPA-A. con el director general y los diferentes departamentos de la empresa pública para tomar las decisiones pertinentes sobre la aplicación del plan de continuidad previsto. Al suscitarse un incidente se debe activar el comité de crisis donde debe reunirse y tomar decisiones para afrontar la situación. En este caso, se comunicará a los responsables de los equipos del comienzo de las actividades que llevarán a restablecer los servicios en la empresa.

Una vez, estipulado las actividades a realizar se procede a aplicar en el plan de continuidad de servicios de TI, la prevención de riesgos futuros para la empresa descritos en la tabla N° 9, en donde, se establece los riesgos posibles y la aplicación de estrategias que ayudan a mitigar y a prevenir futuros problemas.

Tabla N° 9. Prevención de riesgos de la empresa

N°	Riesgo	Estrategia de mitigación	Estrategia de prevención
1	Mantenimiento no planificado de servidores de la empresa EP-EMAPA-A	Reagendar los despliegues programados en la fecha del incidente. Comunicar a los jefes de los proyectos de la suspensión de los servicios.	Agendar el mantenimiento de los servidores e informar a los proyectos las fechas en las cuales se llevarán a cabo. Esta medida prevendrá que consideren las fechas para despliegues y no impacten a los proyectos
2	Indisponibilidad del back up	Analizar la línea base a los jefes de proyecto. Almacenar los back-up recibidos por los jefes de proyecto en el *file serve*	Almacenar las fechas de caducidad del servidor *file serve*
3	Falta de una unidad de sistema de alimentación ininterrumpida	Suspensión de la información en base de los servicios de la TI, en el área de sistemas	Solicitar unidades UPS para los servidores
4	Accidentes ocasionados en los equipos de cómputo	Contar con garantía para los servidores que considere daños por catástrofes.	Cambiar el Sistema contra incendios de rociadores para la sala de servidores a un sistema de supresión de incendios mediante gas inerte
5	Incumplimiento de las políticas de seguridad en la empresa.	Establecer un sistema de penalización por reglas incumplidas. Dicho sistema de penalización podrá definir la nota de los recursos en la página web	Mantener informado a los usuarios del acontecimiento, para evitar problemas en los servicios de agua potable y alcantarillado

Fuente: Elaboración propia

s

3.2.2. Desarrollo de procedimientos en un plan de continuidad de servicios

Una vez que se ha definido los equipos y se han establecido las funciones que debe desempeñar cada equipo, debe desarrollar los procedimientos que van a seguir, como la actuación en cada una de las fases de activación del plan de continuidad identificando el evento que se vaya a suscitar, la actividad y los responsables. Como se describe en el cuadro N°17.

Tabla N° 10. Desarrollo del plan de continuidad de servicios

Fase	Evento	Actividad	Responsable
Alerta	Notificación	Se notifica al área de TI mediante los canales de comunicación definidos por la empresa y correo electrónico en horario laboral y vía celular fuera del horario laboral.	Usuario de instancia de incidencia
Alerta	Análisis de incidente	Se analiza el incidente en el área de TI si no es grave se resuelve según procesos habituales. Si es grave se notifica al líder del equipo director (Gerente de Sistemas).	Asistente de operaciones
Alerta	Reunión del equipo	El líder convocara a una reunión con todos los integrantes del área	Equipo de director
Alerta	Evaluación del incidente	Se decidirán si el centro de operaciones principal está operable o se debe levantar operaciones desde el centro alterno	

Fase	Evento	Actividad	Responsable
Alerta	Activación del plan de continuidad	Se realizan llamadas a los líderes de cada equipo indicando la activación del plan y el sitio desde el cual se levantarán las operaciones.	Equipo del director
Transición	Coordinación del traslado de los equipos	Cada jefe departamental deberá trasladarse al lugar de reunión propiciado por el director general.	Jefe administrativo

Transición	Solicitud de equipos de cómputo	Si el sitio de operación será el COQ, se solicitará al proveedor de TI los equipos de cómputo necesarios para el procedimiento de restauración las operaciones	Jefe de desarrollo y gerente de sistemas
Transición	Notificación personal	Se notificará al líder de cada área la indisponibilidad de servicios para que procedan a informar a los equipos cual es el centro de operaciones vigente, y si es posible continuar con el resto de operaciones o las directrices a seguir según el impacto de la incidencia	Gerente en sistemas
Recuperación	Obtención de claves	Solicitar al asistente administrativo que entregue la clave en base al uso de los usuarios	Jefe de operaciones
Recuperación	Verificar y garantizar la disponibilidad de los recursos de red	Verificar que exista red en el centro de datos ´principal para garantizar hacia los servidores en el centro de datos principal o en el centro de datos EMAPA de Ambato.	Asistentes de operaciones

Fase	Evento	Actividad	Responsable
Verificación	Verificar y garantizar la disponibilidad de sistemas de información	Verificar la disponibilidad de los sistemas de información que han sido afectados, para esto se ingresará al sistema correspondiente para verificar que esté operativo, el registro de operación RO04	Asistente de operación 1
Verificación	Consolidación de los registros de operación	Se consolidarán los registros de operación y se notificará al equipo de pruebas que pueden arrancar con la verificación	Jefe de operaciones
Verificación	Pruebas de verificación	El equipo de pruebas realizará la verificación de la disponibilidad de los servicios que fueron afectados: Sistema de información los perfiles de pruebas serán asistentas técnicas, indemnizaciones y caja. Sistema de información los perfiles de pruebas serán asistentes contables y de nómina Servidor de archivos el perfil de pruebas será al asistente de calidad de software	Asistente de calidad de software
Normalidad	Análisis de impacto	El equipo director se reunirá para realizar una valoración de los daños y llenarán el registro de evaluación RE01 colocando adicionalmente si el servicio está operativo o no el centro de operaciones en el cual está disponible.	Equipo director

Fuente: Elaboración Propia

3.3.3. Ejecución del plan de continuidad de servicios

Para la ejecución del plan de continuidad el comité de evaluación de la empresa EP-EMAPA- A, socializa la información de acuerdo si se va activar el plan de continuidad de servicios de TI, para poner en marcha todo tipo de incertidumbres que se haya generado durante los diferentes procedimientos de riesgos que se han encontrado durante el procedimiento y actividades. Como se muestra en el cuadro N° 18.

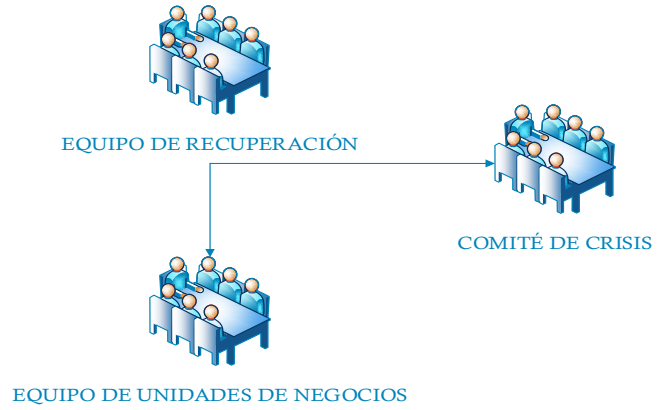
Cuadro N° 18. Registro de avaluación del plan de continuidad de servicios de TI

Servicio	Ejecución	Disponibilidad SI/NO
Solicitud de información de aplicaciones de gestión de sistemas de información	Generación y entrega de información de las aplicaciones de gestión (reportes) que no se pueden generar a través de herramientas de usuario disponibles.	
Instalación, configuración y acceso a software de gestión datamart	Instalación para el correcto uso y sistematización de la información bajo el software datamart	
Eventualidades con el software de KREA	Eventualidades para el proceso y control del sistema	
Servidor de archivos	Acceso y configuración al servidor de archivos de la organización (carpetas compartidas N, M y T)	

Fuente: Elaboración Propia

El cuadro N° 18, describe la ejecución del plan de continuidad de servicios de TI para establecer las actividades que se pusieron en práctica, con el propósito de evaluar posibles riesgos y mitigación en base de la aplicación del instrumento denominado lista de cotejo, en donde identifica las incertidumbres referentes al sistema de información de la empresa de agua potable y alcantarillado de la ciudad de Ambato.

Figura N° 15. Procedimientos de comunicación de soporte y gestión



Fuente: Elaboración Propia

Procedimiento de traslado de materiales - Se debe trasladar todo el material necesario para poner en marcha el centro de recuperación (cintas de *backup*, material de oficina, documentación,) Esta labor queda en manos del equipo logístico.

Procedimiento de puesta en marcha del centro de recuperación. - Una vez que el equipo de recuperación llegue al punto de encuentro y que los materiales empiecen a llegar, pueden comenzar a instalar las aplicaciones en los equipos que se encuentran en esta oficina. El equipo de recuperación solicitará al equipo de logística cualquier tipo de material extra que fuera necesario para la recuperación.

Procedimiento de restauración. - El orden de recuperación de las funciones se realizará según la criticidad los sistemas: Pedidos, Facturación, Correo, Nóminas. Los dos primeros sistemas deben recuperarse lo antes posible, en las 48 horas siguientes. Los demás sistemas pueden esperar a recuperarse después de pedidos y facturación.

Procedimiento de soporte y gestión. - Una vez recuperados los sistemas, se avisará a los equipos de los departamentos que gestionan los sistemas para que realicen las comprobaciones necesarias que certifiquen que funcionen de manera correcta y pueda continuarse dando el servicio. Además, el equipo de seguridad deberá comprobar que existen las garantías de seguridad necesarias (confidencialidad, integridad, disponibilidad) antes de dar por terminada la etapa de recuperación.

Análisis del impacto. – Se realiza de una valoración detallada de los equipos e instalaciones defectuosas para luego procederá a definir las estrategias para normalizar el equipamiento y las instalaciones. Para ello, el equipo de recuperación junto con el equipo de seguridad, realizarán un listado de los elementos que han sido dañados gravemente y son irrecuperables, así como de todo el material que se puede volver a utilizar. Esta evaluación deberá ser comunicada lo antes posible al equipo director para que determinen las acciones necesarias que lleven a la operación habitual lo más pronto posible.

Adquisición de nuevo material. - Una vez realizada la evaluación del impacto, se determinará la necesidad de nuevo material. El comité de crisis contactará con el seguro de la compañía para conocer qué parte cubre el seguro dependiendo del tipo de póliza contratada por EP-EMAPA-A. sobre qué inversión tendrá que hacer la compañía en el material que no se pueda recuperar. Contactar con los aseguradores o proveedores para que en el menor tiempo posible reponga todos los elementos dañados.

Etapa de regreso a la normalidad. - Con los procesos críticos en definidos, hay que plantearse las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento.

Mantenimiento del plan de continuidad. - Debe ser propia dinámica de la empresa pública EP-EMAPA-A., y con el grupo administrativo que lo involucra, tomando decisiones acertadas a las nuevas soluciones a los Sistemas de Información y los activos informáticos van evolucionando para dar respuesta a las necesidades planteadas. La correcta planificación del mantenimiento del Plan de Continuidad evitará que quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades.

3.3.4. Conclusión del plan de continuidad propuesto

La diferencia para la empresa pública EP-EMAPA-A., entre tener y no tener un plan de continuidad, puede suponer que la empresa pública pueda desaparecer en caso de un incidente grave que perjudique sus principales procesos. Por ello, como parte de la gestión de seguridad, EP-EMAPA-A., ha considerado como prioritario desarrollar un Plan de Continuidad para estar preparados ante cualquier incidente.

3.4. Legislación del plan de continuidad

El gerente general de la empresa pública EP-EMAPA-A., conjuntamente con las áreas administrativas y los responsables de las TI, socializarán el programa para su ejecución, ellos mismos serán los responsables de ejecutar la legalización del plan de continuidad de servicios del Departamento de Tecnología de la información de la EP-EMAPA-A., en casos excepcionales.

El proceso de la legalización podría llevar meses ya que necesita la conformación del comité de crisis y sus equipos de trabajo. Debido a lo anterior se desarrolla un documento para la aprobación desde el punto de vista estructural y técnica de la propuesta por parte del Departamento de TI de la EP-EMAPA-A.

CONCLUSIONES

En base a la información obtenida, sobre el diseño de un plan de continuidad de servicios del departamento de tecnología de la información de la empresa EP- EMAPA- A, se emiten las siguientes conclusiones:

- Un plan de continuidad de servicios, es una herramienta guía que provee información para asistir en los equipos de recuperación del departamento de tecnología de información, con el propósito de responder a la disrupción de los sistemas críticos, por tanto, la investigación esta direccionada al diseño para mejorar los tiempos de recuperación y restauración que se susciten frente a fallas o problemas que generen incertidumbre en la empresa, identificando que actividades de continuidad son las más adecuadas y plantean alternativas de solución con el fin de obtener mejoras y ahorro en la operación como en la administración de los servicios críticos de la TI.

- Para, el diagnóstico situacional de la empresa EP- EMAPA- A, se trabajó bajo la línea base en relación a la estructura organizacional de las áreas tomando en cuenta el departamento de tecnologías de información, en donde se a previsto llevar un control en el aspecto sistémico del servicio en función de la comunidad ambateña, cuyo propósito es llevar un plan de continuidad, que ayude a mitigar posibles riesgos como puntos críticos para saber cómo pueden continuar los procesos en caso se presente un caída parcial o total de los servicios que utilizan según la labor que desempeñan. Con la mejora continua del plan, en un futuro se seguirán optimizando estos resultados.} A través, de la aplicación de la metodología “Business Impact Analysis” (BIA), se establece el proceso de análisis de impacto que pueda tener en el tiempo de interrupción dentro del servicio de TI, de la empresa de tal manera que se aplicó una metodología de corte descriptivo, que detalla las características sobre la importancia y estructura de un plan de continuidad en los procesos, gestión de calidad, e información sobre el adecuado procedimiento de la información mediante el uso de un sistema informático para optimizar y flexibilizar los recursos frente a los riesgos y amenazas que se den en la empresa, en instancia también se aplicó el método general cuya técnica de estudio es la observación directa la misma que permite obtener información en base a un checklist,

para identificar las principales actividades que se han realizado en la empresa cuyo aspecto radica en relacionar el uso de un sistema informático para mejorar la continuidad de mejora en el servicio del departamento de TI.

- Como técnica se aplicó una encuesta dirigida al área departamental de sistemas en donde, se obtuvo que la mejora continua del plan de continuidad, en un futuro se seguirán optimizando los puntos críticos y de operación representando un 44%; correspondiente a la parte integral del funcionamiento de servicios presentó un 11% con un riesgo bajo.

- Finalmente, la empresa EP- EMAPA- A, requiere de una actualización y redirección de un proceso que ayude a mitigar, evaluar los puntos críticos mediante la aplicación del plan de continuidad siendo muy importante importante que la gerencia general y la alta dirección se involucre en el proyecto ya que la implementación de un plan de continuidad de servicios críticos de TI, con el propósito de llevar una mejora continua en las actividades inmersas en el servicio.

RECOMENDACIONES

De acuerdo a los resultados obtenidos en el desarrollo de la investigación se establece que:

- Para diseñar un plan de continuidad de servicios, se debe seleccionar adecuadamente la infraestructura de hardware y software para soportar la continuidad de servicios de TI, bajo ese concepto siempre será necesario realizar un cuadro comparativo con un análisis costo beneficio para seleccionar la infraestructura correcta con alta disponibilidad y a la correcta gestión de aplicación que se realice en el departamento de TI.

- Es necesario documentar, todas las fases de pruebas del plan con las observaciones, correcciones y mejoras de todas las novedades encontradas con el fin de aprovechar las lecciones aprendidas para incorporarlas en el plan de continuidad y que cumpla con el propósito de alcance de todos los resultados esperados.

- Es importante realizar pruebas periódicas para asegurarse del buen funcionamiento del plan de continuidad de servicios críticos de TI, en base de la información para prevenir futuros problemas o riesgos.

- La empresa debe trabajar en función de las necesidades reales, diseñe, mantenga actualizado, probado un plan de continuidad de servicios críticos de TI, para que en caso de producirse uno o más escenarios de paralización tengan una ventaja competitiva al convertir las pérdidas en ganancias, utilizando la mejora continua del plan mediante opciones de inversión que aseguren la continuidad de dichos servicios y que además incrementen la capacidad, disponibilidad y rendimiento de los recursos sistémicos y tecnológicos..

- Finalmente; dado una respuesta del departamento TI, sobre la legalización del plan de continuidad de servicios de la empresa EP-EMAPA-A., se deberá mantener comunicaciones y conversaciones continuas, para su futura ejecución. Con el visto bueno queda pendiente su tramitación para ejecución, actividad, que no está

contemplado dentro de la planificación o término del presente documento, pero que se hará el seguimiento para saber los avances y mejoras previstas.

BIBLIOGRAFÍA

Arévalo, C. L. (2016). PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN. BOGOTÁ D.C: https://re pository.uca tolic a.edu.co/bi tstream/10983/13914/4/TRABAJO %20DE%20GRADO.pdf.

Arteaga, Y. (2017). INICIO NOSOTROS MATERIAL PREMIUM SERVICIOS BLOG CONTACTO Plan de Continuidad de Operaciones: todo lo que debes saber. https://www.atalait.com/blog/plan-de-continuidad-de-operaciones.

Atalait. (2017, noviembre 27). *Ejecutar pruebas, dar mantenimiento y revisar la continuidad del negocio*. Obtenido de https://www.atalait.com/blog/ejecutar-pruebas-dar-mantenimiento-y-revisar-la-continuidad-del-negocio

Balladares, E. M. (2018). El Plan de Continuidad del Negocio . http://accuratioratings.com/portalnew/wp-content/uploads/2018/01/PCN1217.pdf.

Bautista, M. (2018). marco de Referencia para la Formulación de un Plan de Continuidad de Negocio para TI, un caso de estudio. *Seguridad y Privacidad de la Información*, 8-24. doi:http://revistaenergia.cenace.gob.ec/index.php/cenace/article/view/116

Carrizo, D., Alfaro, A. A., & Loyola, R. (2016). PROPUESTA DE UN MODELO DE PLAN DE CONTINUIDAD: UN ESTUDIO DE CASO. http://www.iiis.org/CDs2016/CD 2016Summer/papers/CA539WU.pdf.

Córdoba, A. (2008). El Plan de Continuidad de Negocio debe ser una prioridad . http://www.itcio.es/planes-contingencia/analisis/1004786016902/plan-continuidad-negocio-debe-prioridad.1.html.

Correa, R. (2018, Abil 26). *Diseño de un plan de continuidad para los servicios críticos del área de Tecnología de la Información de la empresa JJC Contratistas Generales S.A. basado principalmente en la norma ISO/IEC 27031:2011.* Obtenido de

https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625692/correa_sr.pdf?sequence=1&isAllowed=y

Council, R. (2014). Concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. https://eur-lex.europa.eu/LexUriServ/LexUriSe rv.do?uri=OJ:L:2014:078:0006:0015:EN:PDF.

Cruz, M., Pozo, M., & Andino, A. (2018). Las tecnologías de la información y comunicación como forma investigactiva. *Dialnet*, 20. Obtenido de file:///C:/Users/Usuario1/Downloads/Dialnet-LasTecnologiasDeLaInformacionYLaComunicacionTICCom-6840740.pdf

Ferrer, V. R. (2014). Plan de Continuidad para el Negocio. https://www.sisteseg.com/files/Microsoft_PowerPoint_-_PLANES_DE_CONTI NUIDAD_NEGOCIO_V_3.0.pdf.

García, J. (2005). Métodos de Administración y Evaluación de Riesgos. La Habana : Universidad de Chile . Obtenido de http://repositorio.uchile.cl/tesis/uchile/2005/garcia_j2/sources/garcia_j2.pdf

Gilart, I. I. (2016). Las 6 principales causas de un Desastre de IT. https://www.whitebearsolutions.com/las-6-principales-causas-de-un-desastre-de-it/.

Hernandez, A. T. (2006). LOS SISTEMAS DE INFORMACIÓN: EVOLUCIÓN Y. https://revistas.uexternado.edu.co › index.php › derpen › article › download.

Hernández, L., & Galeano, R. (2016). ANALISIS DE IMPACTO AL NEGOCIO. En U. P. Colombia. Colombia: http://polux.unipiloto.edu.co:8080/00000815.pdf.

ISO Tools Excellence. (2019). Sistema de Seguridad de Gestion en la Informacion . PMGSSi. Obtenido de https://www.pmg-ssi.com/norma-22301/8-2-negocios-y-evaluacion-de-riesgos/

Jacome, C. W. (2013). ADMINISTRACIÓN DE CONTINUIDAD DEL NEGOCIO EN EL DEPARTAMENTO DE TI. http://repositorio.puce.edu.ec/bitstream/h andle/22000/12656/Tesis_Jaco meWilsonMGTI.pdf?sequence=1&isAllowed=y.

Marroquín, R. A. (2015). Un método de evalución de Sitemas de Getión de Procesos de Negocios . https://riunet.upv.es/bitstre am/handle/10251/62760/Un%20m%C3%A9todo%20de%20evaluaci%C3%B3n%20de%20sistemas%20de%20gesti%C3%B3n%20de%20procesos%20de%20negocio.pdf?sequence=1.

Méndez, P. (2019). *La teoría y evolución de la tecnología de la información aplicado en las organizaciones como medio de planificación de contingencias.* Madrid: Trillas.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). Esquema Gubernamental de Seguridad de la Información – EGSI. https://www.gobiernoelectronico.gob.ec/esquema-gubernamental-de-seguridad-de-la-informacion-egsi/.

MINTIC. (2015). Guía para realizar el Análisis de Impacto de Negocios BIA. https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf.

Morales, M. H. (2013). Continuidad del negocio . Bógota-Colombia : http://polux.unipiloto.edu.co:8080/00001618.pdf.

Nippon, K. (2017). PLAN DE CONTINGENCIAS. Chillon - Lima: http://www.sedapal.com.pe/Contenido/ambiental/ambiental/disco1/018%20CAPITULO%2017%20Plan%20de%20Contingencias.pdf.

Ochoa, M. (2019). *Plan de continuidad de los servicios críticos de red de la empresa Actuaria Consultores cía. ltda.* . Quito: Pontificia Universidad Católica del Ecuador.

Ochoa, M. J. (2013). Guía de Desarrollo de un Plan de Continuidad de Negocio. https://vochoa84.files.wordpress.com/2012/03/guia-para-la-elaboracion-plan-de-contingencia.pdf#page=51&zoom=100,0,0.

Oficina de Sistemas e Informática . (2018). La planeación de la continuidad del negocio BCP. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-continuidad-del-negocio-v1.pdf.

Ortega, A. (2017). *Revisión del control del proceso DS4; Garantizar la continuidad del servcio de las TICS.* Puerto Rico: Universidad de Costa Rica. Obtenido de https://www.kerwa.ucr.ac.cr/bitstream/handle/10669/27897/Proyecto%20Final%20Garantizar%20la%20Continuidad%20del%20Servicio%20de%20las%20TICs.pdf?sequence=1&isAllowed=y

Pacheco, Apostólico y Asociados. (2017). Evaluación de Riesgos de Negocio para la preparación del Plan anual de Auditoría. Venezuela: PricewaterhouseCoopers. Obtenido de https://www.pwc.com/ve/es/servicios/auditoria/auditoria-interna/evaluacion-de-riesgos-de-negocio-para-la-preparacion-del-plan-anual-de-auditoria.html

Partinez, F. (2014). Call for Code: el llamado de IBM a desarrolladores para utilizar Cloud, IA, Blockchain y mitigar el impacto de los desastres naturales. https://movimientostem.org/blog/call-for-code-el-llamado-de-ibm-a-desarrolladores-para-utilizar-cloud-ia-blockchain-y-mitigar-el-impacto-de-los-desastres-naturales/.

Pérez, J. (2013). Mexico . Obtenido de https://definicion.de/plan-de-desarrollo/

Portillo, A., & Martínez, J. (2019). *La adopción tecnológica en sistemas de gestión sobre planes de continuidad.* México: Perason.

Recovery Labs, M. (2016). Principales factores que causan una pérdida de información. https://www.recoverylabs.com/ayuda-y-soporte/data-recovery-white-papers/informes/princ ipales-factores-que-causan-una-perdida-de-informacion/.

Rodriguez, J. M. (2016). Sistemas de tolerancia a fallos de discos duros. https://www.adrformacion.com/knowledge/administracion-de-sistemas/sistemas_de_tolera ncia_a_fallos_de_discos_duros.html.

Sauveur, L. (2016). Chief of External Relations at United Nations Human Rights. Organización Naciones Unidad .

Serrano, B. R. (2013). La importancia de implementar un Plan de Continuidad de Negocios. México : https://www.dineroenimagen.com/2013-07-01/22403.

Sistemas de Gestión de Seguridad de la Información. (2019). Análisis BIA. Importancia, características y consideraciones. https://www.pmg-ssi.com/2019/06/analisis-bia-importancia-caracteristicas-y-consideraciones/.

Soto, L. (2004). Ventaja Competitiva. En M. E. PORTER. México,: Patria Cultural, S.A.

Torres, J. E., & Velasco, H. (2014). DISEÑO Y PROPUESTA DE IMPLEMENTACIÓN DE UN PLAN DE CONTINUIDAD DEL NEGOCIO APLICABLE A LOS HOSPITALES EN LA CIUDAD DE BOGOTA. https://repository.u catolica.edu.co/bitstream/10983/1706/1/Trabajo%20de%20Investigacion%20BCP%20Hospitales%20de%20la%20Ciudad%20de%20Bogota.pdf.

UNESCO. (2013). Planteamientos teóricos y aplicaciones pedagógicas. http://unesdoc.unesco.org/images/0013/001340/134047so.pdf.

ANEXOS

Anexo N° 1. Checklist para el plan de continuidad de servicios de TI.

Riesgo/Actividad	Categoría	Intensidad
Los mantenimientos no planificados a los servidores IT, podría ocasionar el cese repentino en la atención de servicios, generando inconvenientes en el sistema y procesamiento de la información	Hardware	Logística
No cumplimiento de las políticas de seguridad en la empresa.	Seguridad	Sistemas y tecnologías de información
Falta de una unidad de sistema de alimentación ininterrumpida (UPS)	Hardware/Tiempo	Sistemas y tecnologías de información
Prevención de incidentes, ataques informáticos, desastres naturales	Seguridad	Sistemas y tecnologías de información
Planificación de actividades sobre el proceso de control, evaluación y seguimiento	Software	Sistemas
El gestor de continuidad de servicios de TI deberá comunicar siempre al gerente de servicios de TI si un incidente afectó la continuidad de los servicios	Software	Restricción operacional

Fuente: Elaboración propia

Anexo 2. Lista de verificación para el departamento de TI, EM-EMAPA-A

Pontificia Universidad Católica del Ecuador

Magister en Gerencia Informática

Lista de verificación para el Departamento TI de EP-EMAPA-A

Objetivo: Implementar un plan de continuidad de Servicios para el Departamento de Tecnologías de la Información de la EP-Empresa Municipal de Agua Potable y Alcantarillado de la ciudad de Ambato.
Instrucciones: Considerar para los niveles; 1=Malo; 2=Regular; 3=Bueno; 4=Muy Bueno y 5=Excelente; además de leer detalladamente y aplicar según corresponda a las instrucciones detalladas dentro del mismo.

Tabla N° 11. Instrumentos para recolección de la información

	Cuestionamientos / Elementos BIA	Nivel				
		1	**2**	**3**	**4**	**5**
No.	**Identificación de procesos del negocio**					
1	La estructura organizacional considera como nivel principal al departamento TI					
2	La empresa cuenta con el personal apropiado para el desarrollo de actividades de evaluación de puntos críticos dentro del departamento TI					
3	La empresa cuenta con un Sistema de Gestión de Seguridad de Información					
4	Existen normativas de seguridad dentro del departamento TI					
5	Cuentan con procesos actualizados para la prevención de riesgos dentro del departamento TI					
6	Los respaldos de información y documentación en qué nivel se encuentra					
7	Consideran evaluación de los impactos operacionales y financieros					
8	Identifican los procesos críticos de toda la empresa					
9	Establecen tiempos de recuperación del sistema informático					
10	Cuentan con respaldos en la nube u otros de similares características					
11	Identifican los requerimientos de recursos críticos necesarios					
12	Identifican procedimientos alternos dentro y fuera del departamento TI					
	Resultados					
	Interpretación del proceso crítico	**A**	Crítico para el Negocio, la función del negocio no puede realizarse			
		B	No es crítico para el negocio, pero la			

			operación es una parte integral del mismo.		
		C	La operación no es parte integral del negocio.		
No.	**Evaluación e identificación de los procesos críticos**	A	B	C	NO APLICA
1	Aplicaciones - Sistema de Control de flujo de documentos				
2	Web - Sitio web Entidad				
3	Base de Datos - SQL nómina				
4	Seguridad de Información - Firewall				
5	Sistemas de Almacenamiento - SAN (Storage Área Network)				
6	Comunicaciones - Acceso Local a Internet				
7	Cuartos de Máquinas - Centro de Datos				
8	Proveedores de Aplicaciones y/o comunicaciones - Interno/externo				
9	Recurso Humano - Internos/externos				
	Resultados				
	Tiempo de Recuperación	RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio		
		RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración		
		WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.		
		MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.		
			En horas		
No.	**Establecimiento de los tiempos de recuperación**	**RPO**	**RTO**	**WRT**	**MTD**
1	Aplicaciones - Sistema de Control de flujo de documentos				
2	Soporte Informático - Dispositivos Móviles				
3	Aplicaciones - Sistema de Nómina				
4	Seguridad de Información - Firewall				
5	Comunicaciones - Servicio WiFi				
6	Cuartos de Máquinas - Centro de Datos				
7	Soporte Informático - Equipo PC de usuario				
	Resultados				

	Identificación de los requerimientos de recursos críticos	**Nivel**				
No.		**1**	**2**	**3**	**4**	**5**
1	Sistema de entrada de novedades administrativas.					
2	Interfaces con el Sistema Financiero					
3	Reglas de entrada y salida de puertos.					
4	Reglas NAT/PAT.					
5	Direccionamiento IP público.					
6	Control de identificación usuarios con Portal Cautivo.					
7	Control de usuarios locales Vs Invitados.					
8	Control de operaciones de Servidores					
9	Equipos de Comunicaciones					
10	Sistemas de Almacenamiento					
11	Sistemas de Backups					
12	Aire Acondicionado					
13	Acometida Eléctrica.					
	Resultados					
	Identificación de procedimientos alternos	**Nivel**				
No.		**1**	**2**	**3**	**4**	**5**
1	Se identifican procesos alternos en caso de interrupciones					
2	En el caso de una interrupción la empresa puede seguir operando					
3	Existen manuales o políticas para casos de crisis en el departamento de TI					
4	Dado la evaluación de los procesos críticos cual es el nivel de los procedimientos alternos					
5	Existen controles correctivos					
6	Identifican la causa de los problemas con el objeto de corregir errores producidos.					
7	Modifican los procedimientos para minimizar futuras ocurrencias del problema.					
8	Existen parches de seguridad.					
9	Se da corrección de daños por virus					
10	Nivel de recuperación de datos perdidos					
	Resultados					

Elaboración: Propia

Anexo N° 3.- Solicitud de información para la aprobación en la empresa EP-EMAPA-A

Ambato, 24 de julio de 2019

De nuestra consideración

A quien corresponda;

Saludos cordiales, por solicitud del Ing. Jorge Alfonso Jaramillo Camacho con C.I. 1802272508, estudiante del Magister en Gerencia Informática de la Universidad PUCE-SA, y presentado la propuesta del trabajo de fin de magister, hemos acordado y revisado los siguientes puntos:

- El estudiante se acercado y ha estado en contacto durante el desarrollo investigativo y de su propuesta.
- La propuesta consta de cuatro fases, con una estructuración técnica que guarda conformidad a lo solicitado y a los estándares de los sistemas de seguridad de la información.
- La aplicación técnica está basada en una metodología ya aplicada, por lo cual su seguimiento y control correspondería a la gerencia u administración de la empresa EP-EMAPA-A o a quien por defecto se asigne estas funciones.
- Su legalización llevaría tiempo por los procesos administrativos, además qué por la reciente transición y rotación de personal, por lo que se menciona que este punto se lo haría mediante tramitación y oficio; posterior a la aprobación del proyecto de grado y sea subido al repositorio de la universidad.

En conclusión, el trabajo guarda conformidad en estructuración y técnicamente se trabajan todos los puntos que son necesarios en esta institución; por lo que al tener y solicitar la asignación de un puntaje; se le asigna a la propuesta 9,8/10 puntos, siendo excelente; y recomendando, tener cuidado en la redacción y faltas ortográficas. Es todo en cuanto a nuestra pronunciación.

Atentamente;

Ing.

Jefe departamental TI–EP–EMAPA-A